IIWXXXII

INTERNET IDENTITY WORKSHOP 32

APRIL 20 - 22, 2021

Book of Proceedings

www.internetidentityworkshop.com

Collected & Compiled by
LISA R. HORWITCH, DOUNIA SAEME, HEIDI N. SAUL

April 20, 21 & 22, 2021
On Line, Near You ~ via QiqoChat

The Internet Identity Workshop Global Community

IIW founded by Kaliya Young, Phil Windley and Doc Searls
Co-produced by Heidi Nobantu Saul, Phil Windley and Kaliya Young
Facilitated by Heidi Nobantu Saul, Kaliya Young, Lisa R Horwitch

IIWXXXIII Online or In Person in Mountain View, CA
October 12 - 14, 2021

Thank You! Documentation Center & Book of Proceedings Sponsors: JOLOCOM – AyanWorks – ADI Association

@GETJolocom **@ayanworkstech** **@ADIAssociation**

Contents

About IIW

The Internet Identity Workshop (IIW) was founded in the fall of 2005 by Phil Windley, Doc Searls and Kaliya Young. It has been a leading space of innovation and collaboration amongst the diverse community working on user-centric identity.

It has been one of the most effective venues for promoting and developing Web-site independent identity systems like OpenID, OAuth, and Information Cards. Past IIW events have proven to be an effective tool for building community in the Internet identity space as well as to get actual work accomplished.

The event has a unique format – the agenda is created live each day of the event. This allows for the discussion of key issues, projects and a lot of interactive opportunities with key industry leaders that are in step with this fast-paced arena.

Watch this short documentary film: ***"Not Just Who They Say We Are: Claiming our Identity on the Internet"*** http://bit.ly/IIWMovie to learn about the work that has happened over the first 12 years at IIW.

The event is now in its 17th year and is Co-produced by Phil Windley, Heidi Nobantu Saul and Kaliya Young. IIWXXXIII (#33) will be October 12, 13,14, 2021, registration will open in mid-June.

Thank You to our Sponsors!

IIW Events would not be possible without the community that gathers or the Sponsors that make the gathering feasible. If you are interested in becoming a sponsor or know of anyone who might be please contact Phil Windley at Phil@windley.org for Event Sponsorship information.

Upcoming IIW Events

IIWXXXIII #33
October 12 - 14, 2021
Location TBA by mid-June
https://internetidentityworkshop.com/

IIWXXXII Registrants

IIWXXXII 3 Day Global Schedule

Sessions are set for 75min each with a 15min break	West Coast USA	East Coast USA	Central Europe	India	Indochina (Thailand)	Japan	New Zealand
	PDT	ET	CET	IST	ICT	JSP	NZST
Grand Opening Agenda Creation	7:00am April 20	10:00am April 20	4:00pm April 20	7:30pm April 20	9:00pm April 20	11:00pm April 20	2:00am April 21
Session 1	8:30am	11:30am	5:30pm	9:00pm	10:30pm	12:30am	3:30am
Session 2	10:00am	1:00pm	7:00pm	10:30pm	12:00am	2:00am	5:00am
Session 3	11:30am	2:30pm	8:30pm	12:00am	1:30am	3:30am	6:30am
Session 4	1:00pm	4:00pm	10:00pm	1:30am	3:00am	5:00am	8:00am
Demo Hour	2:30pm	5:30pm	11:30pm	3:00am	4:30am	6:30am	9:30am
Closing / Open Gifting Agenda Announcement	3:30pm April 20	6:30pm April 20	12:30am April 21	4:00am April 21	5:30am April 21	7:30am April 21	10:30am April 21
Session 5	4:30pm	7:30pm	1:30am	5:00am	6:30am	8:30am	11:30am
New Day	April 21	April 21	April 21	April 21	April 21	April 21	April 21/22
Session 6	1:00am	4:00am	10:00am	1:30pm	3:00pm	5:00pm	8:00pm
Session 7	2:30am	5:30am	11:30am	3:00pm	4:30pm	6:30pm	9:30pm
Session 8	4:00am	7:00am	1:00pm	4:30pm	6:00pm	8:00pm	11:00pm
Session 9	5:30am	8:30am	2:30pm	6:00pm	7:30pm	9:30pm	12:30am
Opening Circle Agenda Creation	7:00am April 21	10:00am April 21	4:00pm April 21	7:30pm April 21	9:00pm April 21	11:00pm April 21	2:00am April 22
Session 10	7:30am	10:30am	4:30pm	8:00pm	9:30pm	11:30pm	2:30am
Demo Hour	9:00am	12:00pm	6:00pm	9:30pm	11:00pm	1:00am	4:00am
Session 11	10:00am	1:00pm	7:00pm	10:30pm	12:00am	2:00am	5:00am
Session 12	11:30am	2:30pm	8:30pm	12:00am	1:30am	3:30am	6:30am
Session 13	1:00pm	4:00pm	10:00pm	1:30am	3:00am	5:00am	8:00am
Session 14	2:30pm	5:30pm	11:30pm	3:00am	4:30am	6:30am	9:30am
Closing / Open Gifting Agenda Announcement	4:00pm April 21	7:00pm April 21	1:00am April 22	4:30am April 22	6:00am April 22	8:00am April 22	11:00am April 22
Session 15	5:00pm	8:00pm	2:00am	5:30am	7:00am	9:00am	12:00pm
New Day	April 22	April 22	April 22	April 22	April 22	April 22	April 22/23
Session 16	1:00am	4:00am	10:00am	1:30pm	3:00pm	5:00pm	8:00pm
Session 17	2:30am	5:30am	11:30am	3:00pm	4:30pm	6:30pm	9:30pm
Session 18	4:00am	7:00am	1:00pm	4:30pm	6:00pm	8:00pm	11:00pm
Session 19	5:30am	8:30am	2:30pm	6:00pm	7:30pm	9:30pm	12:30am
Opening Circle Agenda Creation	7:00am April 22	10:00am April 22	4:00pm April 22	7:30pm April 22	9:00pm April 22	11:00pm April 22	2:00am April 23
Session 20	7:30am	10:30am	4:30pm	8:00pm	9:30pm	11:30pm	2:30am
Session 21	9:00am	12:00pm	6:00pm	9:30pm	11:00pm	1:00am	4:00am
Session 22	10:30am	1:30pm	7:30pm	11:00pm	12:30am	2:30am	5:30am
Session 23	12:00pm	3:00pm	9:00pm	12:30am	2:00am	4:00am	7:00am
Session 24	1:30pm	4:30pm	10:30pm	2:00am	3:30am	5:30am	8:30am
Closing Circle	3:00pm	6:00pm	12:00am	3:30am	5:00am	7:00am	10:00am

IIW 32 Opening Exercise in Small Groups

Each IIW begins with a round table exercise designed to both start the current identity conversations and connect new with long time attendees. At IIW 31 the prompt questions were focused on the following questions. When groups returned to the main room, they were asked to share what was discussed in the Zoom Chat.

What's exciting and inspiring right now for you relative to your work in the industry?
What are you keen on learning about?
What is worrying you?

From Kaliya Identity Woman to Everyone : As you are returning please share in chat highlights from your conversation we would like to know how How is the current crisis shaping how you think about identity differently and the any new opportunities you are seeing?

Drummond Reed to Everyone : The last comment in our breakout room was from Dave Crocker who said, "Interop testing creates community". Well said!!

Paul Knowles to Everyone : Lots of Europeans in our breakout room. The pandemic has turned IIW into a truly international event!

Jemima Gibbons to Everyone : As a first timer it was great to meet Kaliya and some other friendly faces. Thanks for the encouragement Kaliya I will definitely post a session!

schmudde to Everyone : Already talking about identity + vaccines - differences between USA, UK, EU - people couldn't wait to dive into the real issues.

Stephen Curran to Everyone : Collaborating on wallets -- not everyone creating their own. Building on the shoulders.

dsearls to Everyone : We're from everywhere. A live demonstration of a world absent of distance and gravity. The only preposition that applies is *with*.

Kimberly Linson to Everyone : I'm grateful to the Zoom gods for sending me into the cool kids room! I'm really looking forward to some more friendly contentious discussions!!!

dcrocker to Everyone : To get working interoperability, 'test suites' are only a beginning; they help find the easy problem. What is really needed is interoperability events, between working systems. Besides the benefit of the testing, it usually helps jumpstart the /community/ of implementors.

ken.ebert to Everyone : We had an interesting discussion about censorship.

Cam Geer to Everyone : looking to push passed current state and get to wider adoption, scalability and monetization

Anil John to Everyone : I was informed that I was their personal nemesis due to who I work for and what I do :-)

Drummond Reed to Everyone : @DSearls: this is what Craig Burton meant by the Internet bringing us all “zero distance from one another” ;-)

From Leah Houston to Everyone : I tweeted a highlight:
https://twitter.com/LeahHoustonMD/status/1384515192822849542?s=20

08:34:38 From Grace Rachmany to Everyone : Interoperability concerns were big in our breakout room.

From Dave Huseby to Everyone : IIW is the best community and conference in tech and you’ve been such a huge part of it John. Thanks for coming back to us.

From Riley Hughes to Everyone : The coolest thing about IIW is the community. Identity is great, but these connections are incredible. Thanks John & Manjit

Session Topics / Agenda Creation

153 distinct sessions were called and held over 3 Days.

We received notes, slide decks, and/or Zoom Chats for 141 of these sessions.

Tuesday April 20, 2021 ~ Day 1

Session 1
1A/ Biometric COVID Verifiable Credential
1B/ **101 Session:** OpenID Connect
1D/ Better and more secure methods for API authentication
1C/ COVID Credentials Initiative Update/Overview
1F/ Dynamic Disambiguation and Deconfliction of Complex Access Controls from Multiple Verifiable Sources –
1H/ Building a Hyperledger Indy Network - Questions, discussion, etc.
1K/ GLEIF and KERI (Global Legal Entity Identifier Foundation)
1L/ Mobile Agent Development **FAQ**
1P/ 9am PT: W3C CCG weekly call about VC HTTP APIs

Session 2
2A/ The Principles of User Sovereignty and A Unified Theory of Decentralization
2B/ **101 Session:** OAuth2
2C/ godiddy.com - Universal DID Services
2D/ Why the Internet Needs DIDComm
2E/ Decentralized Semantics 101
2F/ OpenID Connect for W3C Verifiable Credential Objects
2K/ Security Considerations of KERI. Why and how KERI provides secure portability

Session 3
3A/ ION 101-401: what is ION (the public, permissionless DID network), how can you use it today, and what comes next
3B/ **101 Session:** UMA - User Managed Access
3C/ Standard Interfaces for DID Create/Update/Deactivate
3D/ Data Unions, Banks, Coops, Fiduciaries etc -- has their time come?
3E/ Making **The Intention Economy** happen
3G/ Revocation: Introduction & Overview - goal is to connect
3H/ Biometric and digital identity
3I/ US Dept of Ed and Universal Wallet: Bring your wallet!
3K/ KERI Q&A basic introduction
3M/ Is the verifiable credential trust triangle incomplete?

Session 4
4A/ Overlays Capture Architecture (OCA): A global solution for data capture and semantic harmonization
4B/ **101 Session:** Self Sovereign & Decentralized Identity
4C/ Introduction to Picos
4D/ Managing Authorization: Who Has What?
4E/ An introduction to The Authentic Data Economy
4G/ Guardianship Showcase - The Sovrin Working Group Tech Requirements and Implementation Guidelines
4I/ The did:indy DID Method - Future Indy Ledgers
4K/ Introducing: WACI (Wallet And Credential Interaction)

Closing Circle – Open Gifting & Opening for next 5 Sessions
Session 5
5B/ OpenID Connect Claims Aggregation

Wednesday April 21, 2021 ~ Day 2

Session 6 / Session 7 / Session 8 (no sessions called)

Session 9
9A/ Secure Scuttlebutt Intro

Closing for 5 Sessions that were held & Opening / Agenda Creation for Upcoming Sessions

Session 10
10A/ Don't use DIDs, DIDs, nor DIDs: Change My Mind (a.k.a. Oh no he DIDn't)
10B/ Making The Intention Economy Happen, Part 2
10C/ Covid Credentials Initiative: Challenges & Learning
10D/ Directories in Distributed Identity
10E/ Integrating FIDO with Verifiable Credentials (8.30 am start)
10G/ Verifiable Credentials for Authentic Data in the Supply Chain
10H/ Self-Sovereign Communities of Self-Sovereign Agents
10I/ Internet Governance – UDDI – Universal Declaration of Digital Identity
10J/ OpenID Connect 4 Identity Assurance

10L/ Dynamic Data Economy: Digital Identity, Authentic Data Flows, Data Mesh and other dragons

Demo Hour

Session 11
11A/ **IIW verifiable credentials** - Decentralized VC integration with Eventbrite and Qiqo chat. This session will review the implementation process, lessons learned, and community discussion on related use cases.
11B/ Group Credentials/Multi-Issuer Credentials
11C/ **Rugged Identity:** resilience for Identity of Things to bad latency, signal, power, physical integrity.
11D/ **DIDComm V2**: Implementation and integration [technical] (did:key and did:keri resolvers, seamless and partial integrations)
11E/ BBS+ Credential Exchange in Hyperledger Aries
11F/ State of SSI in Europe and Necessity for Network-of-Networks (convened by Sovrin)
11H/ Semantic interoperability with layered schemas and linked data
11I/ Identity Escrow - Accountability AND Privacy
11K/ KERI: Centralized registry with decentralized control (KEL & TEL) + DEMO
11M/ OpenID Connect: Session Management vs Privacy
11P/ Credential-based login to a Pico-based application

Session 12
12A/ Git as Authentic Data Creation Tool (a.k.a. what happened to did:git? a.k.a. independently verifiable, secure, developer sovereign, open source software supply chain)
12B/ Veres One (did:v1) Rubric Evaluation
~~12C/ Maturity Models for enterprise and ecosystem identity.~~
12D/ IDunion Introduction and AMA (there will be another one tomorrow!)
12E/ IoT Swarms + SSI in constrained networks
12F/ Credentials Exchange - figuring it out - (Jello Bowl Death Match?) –
12G/ Use-cases: OIDC for Verifiable Credentials – How do you want to use Identity Provider you control?
12H/ Mapping FHIR JSON resource to W3C Vaccination vocabulary : A semantic data pipeline
12J/ Kepler: Permissioned Replicated Storage for Decentralized Applications
12K/ Credential Marketplaces
12L/ Managing VCs at Scale & the VC Stack
12M/ Sovrin Update: Supporting Commercial Development of SSI
12O/ Global Survey Findings: Current state of SSI

Session 13
13A/ Security Event Tokens, Subject Identifiers, and SSE/CAEP/RISC Java implementation
13B/ What's next for BBS+ LD-Proofs?
13C/ John Jordan AMA - ToIP, BC Gov, Spinal Cord Injuries
13D/ We evaluated 7 DID methods with the W3C DID Rubric! did:btcr, did:sov, did:ion, did:web, did:key, did:peer, did:ethr
13E/ VC-HTTP-API discussion (FAQ, vs other APIs, etc)

13F/ MOVE 78 - Human Deep Mind vs. Google Deep Mind (AlphaGo) How can Human Intention ever win??
13G/ Trust Registries - Good Health Pass - DIDs and X.509
13H/ GS1 2021 VC/DID Prototype Review: The Hero's Journey
13I/ State of the DAO: Decentralized Governance
13J/ Dynamic Data Sharing Hub: A target component for criteria searches on distributed structured data
13K/ KERI Security #2 (Why Secure Portability is Hard and How KERI Solves it)
13L/ Browser APIs to enable OpenID Session Management and Privacy

Session 14
14A/ Identity Hub data storage and relay: unlocking the 99.99% of decentralized identity use cases
14B/ SNARK-based anonymous credentials
14C/ COVID Credentials Open Source Proposals at LFPH:CCI
14E/ DHS SVIP group: What we've done and how to participate
14F/ Trust Assurance in SSI / Verifiable Credential Ecosystems
14G/ SSI for Organizations: Who's behind this DID?
14H/ Realistically speaking: Identity reclamation/solutions for normies
14K/ Supply chain – ACDC and KERI + DEMO
14M/ Ceramic, SkyNet, LoRa, IoT. low bandwidth & memory, distributed network. Managing schemas, DIDComm, and V.C. in context

Closing Circle – Open Gifting & Session Announcements for next 5 Sessions

Session 15
15A/ Presentation Tech - Lights, Camera, backgrounds, AMA, Happy hour?

Thursday April 22, 2021 - Day 3

Session 16
Session 17
Session 18

Session 19
19A/ Governance: Clarifying or confusing the marketplace?

Closing for 5 Sessions that were held & Opening / Agenda Creation for Upcoming Sessions

Session 20
20A/ DID chooser for SIOP
20B/ Agency By Design (Privacy is not Enough)
20C/ Digital COVID Vaccine Passports- Is there really a need or are we creating a false certainty in uncertain times?
20D/ UDDI & UDDR - Common language once and for all?
20E/ WHiSSPRr Risk for People
20F/ Wallet Security & Hardware-backed VCs - privacy challenges & new DIF WG incoming
20H/ What if the Credential Subject cannot be the Holder?

20I/ Could an NFT be a VC?
20J/ Device-free SSI: Ideas, Potentials and Challenges
20K/ GLEIF vLEI with KERI
20L/ Why you know less about Guardianship than you think (because we ALL know less about Guardianship than we think)
20P/ GS1 2021 VC Prototype Journey

Session 21
21A/ DIDComm and the Self-Sovereign Internet
21B/ (California) Verifiable Credentials Policy Committeee - Come learn about how participate in passing legislation to crete a California Trust Framework!
21C/ Solving Identity Challenges at the Intersection of Education and Healthcare
21D/ The world between public and private DIDs - Or how to make use of SSI without the subjects
21E/ Verifiable Credentials for Assets <30 min
21F/ Universal NFTs as authentic data without tokens/blockchains. How to eliminate minting/mining fees and break the NFT silos.
21G/ Build an SSI proof of concept in <30 minutes
21H/ Accumulators and Credential Signatures AMA (You don't need to know crypto)
21I/ Creating a positive vision for the future - decentralised web + SSI
21J/ UX for AR, ambient identity, IoT? Human disclosure, consent, auth with devices.
21K/ Can Kids Use D.I.D.s? What's your tech for kids online?
21L/ International Semantic Infrastructure: Requirements for a distributed data economy
21M/ Humanizing PoSSI- Human-centric structure of the Principles of SSI
21O/ DHS SVIP - Program Overview + AMA
21P/ Universal Resolver Driver Policy Discussion

Session 22
22A/ App Framework for Mobile Agent Dev - "No more forking"
22C/ NHS Staffpassport; Based on Evernym Verity built by Sitekit/Condatis; A 12 month experience
22D/ Career Advice for New Professionals in Identity
22E/ Auto-Generating Language-Specific Wrappers for Rust Libraries
22F/ OPN-R (Open Public Notice - Rights) - starting Notice & Control Language - for people to use rights and govern identity (govinterop) with @ Kantara, ToiP and W3C Data Privacy Vocabulary using international vocab - from ISO/IEC 29100 Legal Framework Vocabulary
22H/ Figuring out Verifiable Credentials Exchange - combining Bloom, Aires Protocols, Presentation Exchange into a unified - *Killer Whale Jello Salad*
22I/ Practical Perspectives on the collapse of zero-sum civilizations and the emergence of computational sovereigns and a pattern approach to digital equity governance: The source of the problems is the source of the solutions.
22K/ Implementing Interop with technology across ecosystems (did:ion, did:key, did:ethr, did:web, did:nft and JWT, LD + DIDComm v1 and Chapi)
22L/ KERI Security Considerations #3 (Detailed walkthrough of how KERI achieves secure portability)
22M/ Open-Source Sovrin SSI Wallet - Functionality Design Session
22N/ Mapping FHIR JSON-LD to OCA

Session 23
23A/ What is an Aries Interop Profile (AIP), and Status of AIP 2.0
23B/ TMI BFF: OAuth Token Mediating and session Information Backend For Frontend
23C/ Trinsic Open Source - BBS+ VCs over DIDComm v2 - End-to-end vaccination credential example
23D/ An Identity Through Time
23E/ WHiSSPR- Human transparency over identity and surveillance risk
23F/ Good Health Pass Ecosystem Trust Architecture: DIDs and X.509 Trust Registries with Ecosystem Governance Frameworks
23G/ Self Attested vs Chain of Custody - assurance levels in data provenance in VCs
23I/ Talking on Aries Bifold, building a community effort around an open-source mobile wallet in React Native
23J/ Self-Sovereign E-Commerce
23K/ KERI Composable Event Streaming Representation
23M/ AMA: Sovrin + ToIP Core Purposes and Cooperation
23P/ 12pm PT: W3C CCG VC HTTP API Special Topic Call:

Session 24
24A/ BC Gov Collaboration on the Business Partner Agent, sharing our Roadmap (Create Creds, Issue them, Verify them, Hold them, publish them, ZKPs, Selective Disclosure)
24B/ More Killer Whale Jello Salad...figuring out how credential exchange can harmonize.
24C/ WHiSSPRr Risk for People
24D/ IDunion Introduction and AMA (same as on day 2!)
24E/ Decentralized publication, micro-publication and moderation-- what the real pitfalls would be.
24F/ Making ACA-Py (Almost) Ledger Agnostic: DID resolution over DIDComm (instead of HTTP) to a Universal Resolver.
24H/ KERI and ADS Key State Provenance Logs Kumbaya (KEL and ADPL)
24K/ Dissertation Study on Adoption of SSI Digital Wallet
24L/ Decentralized publication, micro-publication and moderation-- what the real pitfalls would be.
24N/ A Decentralized Autonomous Organization (DAO) for Public Health (Why/What/How)
24P/ Secure Scuttlebutt Outro

Closing Circle – Open Gifting

Session Topic Breakdown

Breakdown of 153 Sessions Convened by Broad Topic Categories The numbers do not Add UP as some covered more than 1 Topic Category					
Verifiable Credentials	41	DID = Dectralized Identifier	19	Governance	12
KERI = Key Event Receipt Infrastructure	10	Wallets	10	Decentralization	9
Ecosystem	9	OICD = Open ID Connect	7	Agent	6
Cryptography	6	DIDComm	6	Interop	6
IoT = Internet of Things	5	Use Cases	5	Covid Related	5
ADS	4	Autonomy	4	Guardianship	4
Semantics	4	Misc	4	MyData	3
Privacy	3	Registries	3	VRM = Vendor Relationship Management	3
AUTHZ	2	Biometrics	2	Consent	2
Data Formats	2	OAUTH	2	Policy	2
Principles	2	Scuttlebutt	2	ZKP	2
And 28 Sessions on a Wide Variety of Topics					
AI		Blockchain		Development	
API		Career		Digital Rights	
AuthN		demo		Directories	
education		Human Rights		iot	
Exchange		Identifiers		Market Model	
FIDO		ION		Networks	
Networks		Presentation Tips		Security	
NFT		Public Policy		Social Network	
Overlay		Revocation		SSI	
UMA		Usability			

Notes Day 1 Tuesday April 20 / Sessions 1 - 5

Biometric COVID Verifiable Credential

Tuesday 1A
Convener: Adrian Gropper / Eric Welton
Notes-taker(s): sankarshan, Neil Thomson (edits, additions)

Tags for the session - technology discussed/ideas considered:

COVID, Verifiable Credentials, Biometrics, Privacy

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

Biometric Health Card (Adrian Gropper)

1. [Eric] Continuing updates from the Thoughtful Biometrics workshop (Biometrics and DIDs - where next?)
    1. Vocabulary for understanding the last diagram in the above link
        1. IBV = initial biometric vector (stored during enrollment - raw or processed)
        2. CBV = candidate biometric vector (ephemeral material used during verification session for matching against IBV)

b. Historical occurrence of the term 'biometric' in DID-Core specification (initially added in 05Nov2017 - about a way to authenticate to a DID); subsequently removed 01Dec2020 (PR#459)

c. DIDs are effectively key centric (biometric control, biometric authentication are no longer part of the specification/code)

d. 'I am not a key, I am a person' does not map well to a key based mapping and management
    1. Self-sovereignty based on who I choose to be

e. Illusion of biometric control - originating from habit based trust around the everyday usage experience
    1. Biometrics as credentials? Can mathematical techniques be used safely to authenticate (instead of just limited to unlock a secured enclave)
    2. Alternatives (see slide) ; possible presentation from Finema (get rid of keys)

[Adrian] Successfully recovered from a computer crash and joined the session :)

. The novel concept of how to deal with the severe privacy issues with any kind of COVID-19 credentials - purely about how the fraud and privacy issues can be dealt with.

a. The approach is simple and based on the fact that people can recognize a face that might be put into the center of a QR code (as an example). Reliably hash the photo on the credential - and you don't have to go back to any datastore. (see Biometric Health Card link above)

1. [Robert M] is this about overall biometrics or limited to facial recognition?
    1. [Adrian] this would only apply to things which are human recognizable; but not for say, a signature
2. [Dan Bachenheimer] Global Entry is fingerprint based transitioning to face recognition - face on receipt is for administrative purposes not for automated facial recognition
3. [Michael Shea] https://www.researchgate.net/publication/283473746 : about constructed image that can potentially pass human and automated recognition [Dan B] photo morphing is a real and known problem in passports. Photo morphing is a KNOWN, REAL problem with passports today; specifically those where photos are sent to the passport agency (i.e., non live capture). NIST has proven that modern Face Recognition Technology (FRT) is more accurate at recognizing unfamiliar faces

b. For the QR code to stand-alone without phone-home, you'll need to embed the hash rather than the actual photograph

c. 3 unique use cases to understand the rights and privacy aspect of this proposal (see document at the Biometric Health Card link above)

1. Please add comments directly to the document
2. [Robert] Eric mentioned that digital identity controlled by public/private key instead of biometrics is a friction around how individuals would prefer to manage their identities
3. [Dan B] the photo is for a human to say that it 'looks like the person' while the hash provides the tamper-evident nature of the credential
    1. Is the photo sufficient for a human to be able to conclude definitively that the photo and the actual human are the same.
4. This approach could address the topics arising from hesitancy around digital vaccination credentials
5. [Hunter Cain] Should not the aim be taking out human verification altogether?
    1. [Adrian] Not ideal to move towards the direction such as CLEAR. It is needed to be very careful not to introduce a system of ambient surveillance (there is no law/regulation which prevents this in US and EU). A system that is 'good enough for machine readability' is going into FRT and is very likely to be prohibited by law.
    2. [Dan B] it is possible to have a handheld device that is not connected to the internet that can read and match with software installed on a kiosk
    3. [Adrian] This approach could be a way to bring the SSI and decentralized identity together to limit forgery in a privacy preserving way.
        1. [Dan B] for instance the presentation of a vaccination record does not need first name, last name or DoB etc. Having a photograph and the record is sufficient to establish the proof of vaccination
        2. [Adrian] will be running a session on HI of One on Day2
        3. [John C] solving a binding problem between the photo and the credentials. How do we also establish that the integrity of the credentials?

d. [Mahesh Balan] use a accredited 3rd party (e.g., equivalent of a civil law notary (France, Quebec)) to create biometric (including photo, finger prints, retinal scan...) from capture to Verifiable Credential. This provides control of the VC process to the owner.

.[Adrian] this would apply if the issuer (lab) has used a separate VC (e.g., driver's license) to validate you prior to a vaccination (certificate) being issued by the lab (which would be provided to the notary -> Verif Cred). This would preserve the chain of trust (in the VC)

i. Could have an issuer who checks VCs, but doesn't apply identifying information on the vaccination certificate
ii. Could use a separate DID for each certificate/VC
iii. Call for discussion on Policy with regards to this proposal (outside scope of this session)
iv. [Adrian] - Lots of people pushing business interests onto Good Health Pass (GHP) and other COVID related VCs, identity which is politicizing the issue
v. [Robert Mitwicki] - can we talk about a VC (including biometric based) without being associated with a Holder (and their wallet)? A VC independent of any DID
vi. [Adrian] Not sufficient. The problem with more than low fidelity biometric information (as per the 512 byte image in QR code_ is adapting that to a VC using a QR code - size of data limitation.
Industry looking for "do not need to call home" verification standard. What the Health Card industry (and GHP WG) is struggling to figure out
vii. Many organizations and public groups (incl. MIT) are unwilling to violate what they see as privacy issues
viii. [Terry Hayes] - concern with verifiability of pixelated images being shown as examples.
ix. [Notetaker addition]: there is an inherent problem with face colouration and lighting that either geometry or facial feature (human recognition) does not work well unless there is high contrast in the photo to pick out differentiating facial features.

More to follow in coming sessions

101 Session - OpenID Connect

Tuesday 1B
Convener: Michael Jones
Notes-taker(s): Michael Jones

Tags for the session - technology discussed/ideas considered:

OpenID Connect; OAuth 2.0; Claims; Login; Logout; OpenID Certification; Digital Identity

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

Session Described at: https://openid.net/connect/

Built on standards: OAuth 2.0 and JWT

See the presentation at https://self-issued.info/?p=2167. (this link is OK - 101 Session + shared by Mike)

COVID Credentials Initiative (CCI) Update/Overview

Tuesday 1C
Convener: Lucy Yang (lucyy.cci@lfph.io)
Notes-taker(s): Kaliya Young (kaliyay.cci@lfph.io) & John Walker (johnw.cci@lfph.io)

Tags for the session - technology discussed/ideas considered:

Current Open Proposals: We will host another session (Day 2 Session 14 2:30 pm PT) to talk about these proposals

- **Proofmarket (Medcreds):** https://docs.google.com/document/d/1hlR_2yp7EJQqYvxm8mNY-KNgwScTsClKDp6W6yw33Ic/edit?usp=sharing
- **Indicio:** https://docs.google.com/document/d/1Vl9IKRg6ygHD1njc8GfnjsQglDOVglBKbuXHSuqQ7T4/edit?usp=sharing

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

Session Slides:
https://docs.google.com/presentation/d/11K027LlitWljJu_XNTztqc6BGvhsD8JBX5OkavLEEMA/edit?usp=sharing

Questions about Government
Obstacles:
Paper as the basis of proof
What Vaccine you take

John Jordan - talking about the perspective they have governments. They are very concerned about how governments are concerned that people might ask them for information. Aligning with the mental models

Anil John - we are interested in the technology US immigration and citizenship suervices - to issue immigration credentials, Green Cards, US Naturalization, Work Permits
We funded the development of Decentralized ID and Verifiable Credentials. Decentralized Identifiers - meaningless but unique identifier. VC model - breaks phone home paradigm that is in the traditional PKI

The starting point for talking to a government.
Equity and Access. Government entity not only opportunity - bridge to paper. Meet people where they are.
Technology and verifiable credentials.
Credentials used in combination.
People should not be put in position where they need 5 different wallets, infrastructures to share 6 credentials.
Clear path bridge to paper -

Lucy - sharing the workstreams
Use-Case Implementation Workstream

- EU approach was discussed last time.

Rules and Governance Workstream - technical part is challenging - a lot of moving pieces. Challenges - interoperability at policy level - from state health agencies. Identify key principles to follow -
Vaccine Credentials Focus Group

Responses to various entities asking for input [put in links]

Summit Series
Paper Based Verifiable Credentials
From Closed-Loop Systems and Open World Credentials Exchange

Open Standards
Schema's - community led
Credential Format and Signing protocols
Credential Exchange Protocols

QR codes that encode data - contain uniques identifiers and personal information in them. Really dangerous - digital credentials using paper as a transport mechanisms. It is permanent - and it can be scanned and the control is lost.
The name is a little akward - they are digital credentials - QR codes are machine readable.
As a person who advises government decision makers. Privacy rules would be violated.

RE: Paper credentials… Is the solution required, a cheap accessible device that can securely verify the holder? E.g. a usb key that has a finger print reader or something like that. If it was under $20 or something then it could be in reach for nearly all.

Check out Tangem NFC cards.

Manny - healthcare and technologists.
This is about health information
A lot of considerations here - that are well intentioned being trained in outbreak medicine and pandemic response. All biomedical
Medical Ethics - Autonomy, Justice,
Stick to medical ethics.

Different diseases - need to be thought of differently

Started personal health information and infrastructure around it right.
Trying to let people whole it.
Hard to engage with policy makers - who don't understand the disease are making decisions.

Karn - question slide - venn diagram with VCI, GHP, CCI - software implementation - do we have open source code bases right now?
What is thought process behind having open source code base - many implementors.
> > > > >
Ontario with paper AB2004 barriers was equity - needs to be a paper option or won't fly in California.

Here is a project that BC Gov digital trust services is collaborating on that has capabilities in line with what is needed to do the VC issuer, verifier, and holder. Issuing to individual wallets is being implemented this month.
https://github.com/hyperledger-labs/business-partner-agent/

Demo: https://www.youtube.com/watch?v=09-LOHPTHWs

Better and More Secure Methods for API Authentication

Tuesday 1D
Convener: Michael Lodder
Notes-taker(s): Jan Christoph Ebersbach

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

Presentation slides:
https://docs.google.com/presentation/d/1UO25DzVmq25ya2S4_tV5UKTSP6NtBggln9vP1TEXSzE/edit

Goal of the Oberon protocol when building an API:

- Super effective: no separate session token to required for accessing the API; very fast to issue and verify tokens; 128 bytes required per message
- Privacy preserving
- No new crypto, uses BLS signature keys and Pointecheval saunders Construction

Questions:

- Can multiple tokens can be combined: Michael: yes, that's possible.
- Will the implementation become open source software: Michael: yes, that's planned.
- Can a proof be reused for API requests? Michael: yes, within a certain time frame it might make sense. However, the idea is to generate a new proof for every request. Proof generation is very simple so that even low powered devices can do it without much effort. Verification of the proof takes longer than proof generation.
- Use cases? Michael: HTTP API authentication and potentially even did:peer; 2 IoT devices that have never talked to each other before shall be able to authenticate each others tokens and establish a secure connection.
- Quantum resistant? Michael: no, it's not. Post-quantum resistance would require very large keys in the range of kilobytes.
- What's the performance of the solution? Tobias Looker points out that the performance varies greatly depending on the environment the code is executed in. Mattr did performance comparisons between native node modules, WASM and ASM.js, more at: https://github.com/mattrglobal/bbs-signatures
- Differences to OAuth? Phil: People today use long lived tokens for OAuth. These tokens/secrets are known to both parties, the developer and the server. Whoever gets their hands on the tokens will have full access to the API. With Oberon, the secret is only known to the developer which protects them more.

Dynamic Disambiguation & Deconfliction of Complex Access Controls from Multiple Verifiable Sources

Tuesday 1F
Convener: Chris Buchanan
Notes-taker(s): Chris Buchanan

Tags for the session - technology discussed/ideas considered:

COVID-19, Good Health Pass Collaborative, Rules Engines, Verifiable Presentation Requests

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

The transition from contemporary access controls to SSI will need a metalanguage for access control rules in order to allow verifiers and holders to trust the transaction. Not everyone will know how to write the complex branching and contextual rules logic that make up real life access controls.

Outsourced rules could also have the properties of verifiability for both the verifier and the holder. Implementing verifiable Verifiable Presentation Requests will be safer for users and verifiers.

This discussion centered around Clinical Quality Language (CQL) as an exemplar of this type of integrative technology. The general consensus was that the idea was sound and would expedite the transition to Verifiable Presentations.

Link to Presentation:
https://docs.google.com/presentation/d/1R_JfLc9kLqAmoqfTDCtVbZZ99gAktavtJJNGlKwXdQQ/edit?usp=sharing

The Problem with the Current Solution

Rules Engine ==> ~~Dynamic~~ Disambiguation and Deconfliction of Complex Access Controls from Multiple Verifiable Sources

As dynamism grows, Rules Engine efficacy decreases.

Answer: Move disambiguation to the edge and automate the deconfliction process?

Requirement: A machine readable way to express complex access control decisions.

Solution: Something like Clinical Quality Language (CQL)

MITRE

What is Clinical Decision Support (CDS)?

Clinical Decision Support systems link health observations with health knowledge to influence health choices by clinicians for improved health care.

Robert Hayward, Centre for Health Evidence

Five "Rights" Framework

Clinical Decision Support delivers:

1. The right **information**
2. To the right **person**
3. In the right **format**
4. Through the right **channel**
5. At the right **time**

Osheroff J.A., Pifer E.A. Teich J.M. et. al. *Improving Outcomes with Clinical Decision Support: An Implementer's Guide*, 2 Ed. Danvers, MA: HIMSS Publishing, Taylor & Francis Group/CRC Press, 2012.

MITRE

CDS-related Standards*

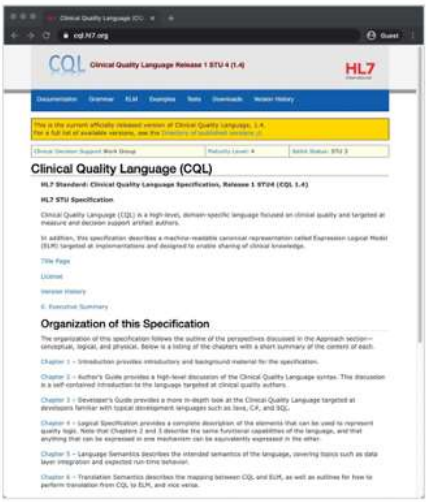
- **Health Level Seven (HL7®) Clinical Quality Language (CQL)**
- **HL7® Fast Health Interoperability Resources (FHIR®)**
- HL7® FHIR® Clinical Reasoning
- HL7® FHIR® Clinical Guidelines
- HL7® CDS Hooks™
- HL7® Substitutable Medical Apps, Reusable Technology (SMART®) App Launch Framework
- Object Management Group (OMG®) Business Process Management Plus (BPM+) Health™

** An incomplete list*

HL7® Clinical Quality Language (CQL)

"Clinical Quality Language (CQL) is a high-level, domain-specific language focused on clinical quality and targeted at measure and decision support artifact authors."

HL7 Standard: Clinical Quality Language Specification, Release 1 STU4 (CQL 1.4)
http://cql.hl7.org/



CQL Key Points

The CQL specification defines two components:

- **Clinical Quality Language**: Author-friendly domain specific language
- **Expression Logical Model**: Computable XML or JSON

CQL leverages best practices and lessons learned from:

- **Quality Data Model**: Focus on ease of authoring
- **Health eDecisions**: Focus on modularity and computability
- **eCQM & CDS Communities**: HL7 Work Groups and S&I Framework

CQL is designed to work with any data model

CQL is *(soon)* a Health Level 7 (HL7) Normative Standard

XML = Extensible Markup Language
JSON = JavaScript Object Notation
S&I = Standards and Interoperability

CQL Data Types

```
define isDeceased: false                              // Boolean
define street: 'Penny Lane'                           // String
define medianNumberOfToes: 10                         // Integer
define averageNumberOfChildren: 2.5                   // Decimal
define birthDate: @1992-03-14                         // Date
define lastModified: @2010-02-25T07:30:14.897-05:00 // DateTime
define preferredLunchTime: @T12:00:00.0               // Time
define length: 5.5 'mm'                               // Quantity
define density: 750.0 'mg' : 1.0 'mL'                 // Ratio
define letters: {'a', 'b', 'c'}                       // List
define letterPositions: { a: 1, b: 2, c: 3 }          // Tuple
define singleDigits: Interval[0, 9]                   // Interval (numeric)
define nextDec: Interval[@2021-12-01, @2021-12-31]    // Interval (date)
```

CQL Queries and Functions

```
define "Inpatient Encounters 120 Days or More":     // Simple query
  [Encounter: "Inpatient"] E
    where duration in days of E.period >= 120

define "Inpatient Encounters Following MI":         // Advanced query
  [Encounter: "Inpatient"] E
    with [Condition: "Myocardial Infarction"] MI
    such that (MI.onset as FHIR.dateTime).value
      occurs 12 hours or less before start of E.period
    sort by start of period

define function "Length of Stay"(enc Encounter):    // Reusable function
  duration in days of enc.period
```

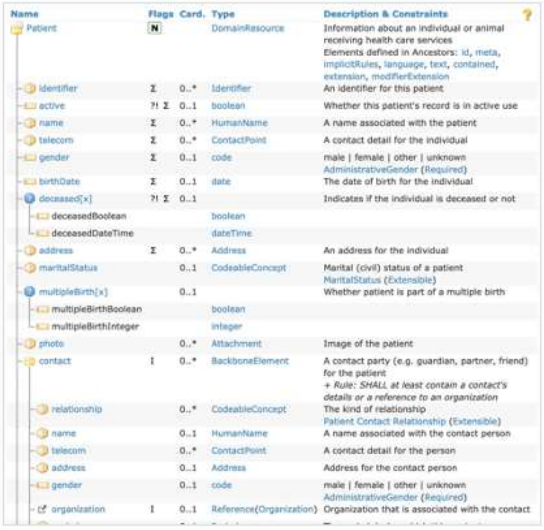
Adapted from https://cql.hl7.org/02-authorsguide.html#queries

HL7® Fast Healthcare Interoperability Resources (FHIR®)

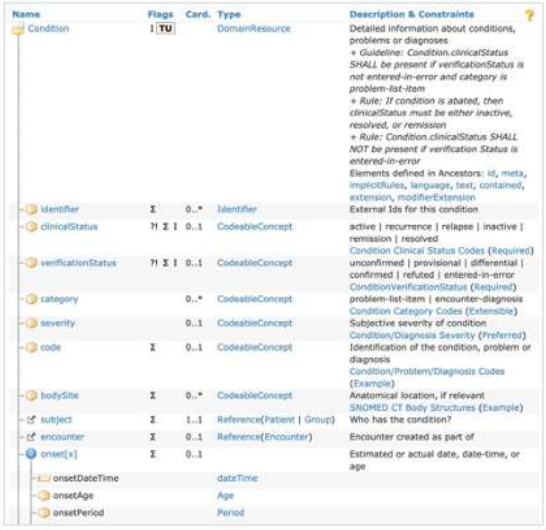
"FHIR is a standard for health care data exchange, published by HL7®."

FHIR Specification (v4.0.1: R4 - Mixed Normative and STU)
https://hl7.org/fhir/R4/index.html

FHIR Resources: Patient and Condition



Name	Flags	Card.	Type	Description & Constraints
Patient	N		DomainResource	Information about an individual or animal receiving health care services Elements defined in Ancestors: id, meta, implicitRules, language, text, contained, extension, modifierExtension
identifier	Σ	0..*	Identifier	An identifier for this patient
active	?! Σ	0..1	boolean	Whether this patient's record is in active use
name	Σ	0..*	HumanName	A name associated with the patient
telecom	Σ	0..*	ContactPoint	A contact detail for the individual
gender	Σ	0..1	code	male | female | other | unknown AdministrativeGender (Required)
birthDate	Σ	0..1	date	The date of birth for the individual
deceased[x]	?! Σ	0..1		Indicates if the individual is deceased or not
deceasedBoolean			boolean	
deceasedDateTime			dateTime	
address	Σ	0..*	Address	An address for the individual
maritalStatus		0..1	CodeableConcept	Marital (civil) status of a patient MaritalStatus (Extensible)
multipleBirth[x]		0..1		Whether patient is part of a multiple birth
multipleBirthBoolean			boolean	
multipleBirthInteger			integer	
photo		0..*	Attachment	Image of the patient
contact	I	0..*	BackboneElement	A contact party (e.g. guardian, partner, friend) for the patient *+ Rule: SHALL at least contain a contact's details or a reference to an organization*
relationship		0..*	CodeableConcept	The kind of relationship Patient Contact Relationship (Extensible)
name		0..1	HumanName	A name associated with the contact person
telecom		0..*	ContactPoint	A contact detail for the person
address		0..1	Address	Address for the contact person
gender		0..1	code	male | female | other | unknown AdministrativeGender (Required)
organization	I	0..1	Reference(Organization)	Organization that is associated with the contact



Name	Flags	Card.	Type	Description & Constraints
Condition	I TU		DomainResource	Detailed information about conditions, problems or diagnoses *+ Guideline: Condition.clinicalStatus SHALL be present if verificationStatus is not entered-in-error and category is problem-list-item* *+ Rule: If condition is abated, then clinicalStatus must be either inactive, resolved, or remission* *+ Rule: Condition.clinicalStatus SHALL NOT be present if verification Status is entered-in-error* Elements defined in Ancestors: id, meta, implicitRules, language, text, contained, extension, modifierExtension
identifier	Σ	0..*	Identifier	External Ids for this condition
clinicalStatus	?! Σ I	0..1	CodeableConcept	active | recurrence | relapse | inactive | remission | resolved Condition Clinical Status Codes (Required)
verificationStatus	?! Σ I	0..1	CodeableConcept	unconfirmed | provisional | differential | confirmed | refuted | entered-in-error ConditionVerificationStatus (Required)
category		0..*	CodeableConcept	problem-list-item | encounter-diagnosis Condition Category Codes (Extensible)
severity		0..1	CodeableConcept	Subjective severity of condition Condition/Diagnosis Severity (Preferred)
code	Σ	0..1	CodeableConcept	Identification of the condition, problem or diagnosis Condition/Problem/Diagnosis Codes (Example)
bodySite	Σ	0..*	CodeableConcept	Anatomical location, if relevant SNOMED CT Body Structures (Example)
subject	Σ	1..1	Reference(Patient | Group)	Who has the condition?
encounter	Σ	0..1	Reference(Encounter)	Encounter created as part of
onset[x]	Σ	0..1		Estimated or actual date, date-time, or age
onsetDateTime			dateTime	
onsetAge			Age	
onsetPeriod			Period	

FHIR Examples: Patient and Condition

```
{
  "resourceType": "Patient",
  "id": "e7c7c18c-06e1-4426-be5b-
494f4573b457",
  "name": [{
      "given": [ "Brenda" ],
      "family": "Jackson"
  }],
  "gender": "female",
  "birthDate": "1956-10-14"
}
```

synthetic data

```
{
 "resourceType": "Condition",
 "id": "7d0735e7-f062-45af-843c-a3e3e7f48888",
 "subject": {
  "reference": "Patient/e7c7c18c-06e1-4426-be5b-494f4573b457"
 },
 "code": {
  "coding": [{
   "system": "http://snomed.info/sct",
   "code": "203082005",
   "display": "Fibromyalgia (disorder)"
  }],
  "text": "Fibromyalgia"
 },
 "clinicalStatus": {
  "coding": [{
   "system": "http://terminology.hl7.org/CodeSystem/condition-clinical",
   "code": "active"
  }]
 },
 "verificationStatus": {
  "coding": [{
   "system": "http://terminology.hl7.org/CodeSystem/condition-ver-status",
   "code": "confirmed"
  }]
 },
 "onsetDateTime": "2013-04-05T16:00:00.000Z",
 "recordedDate": "2013-04-05"
}
```

synthetic data

CQL-related Open-Source Tools*

Authoring

- Atom + language-cql
- CDS Authoring Tool
- CQL-to-ELM Translator
- CQL Testing Framework

Execution

- CQL Execution Framework (JavaScript)
- CQL Engine (Java)
- Clinical Quality Framework (CQF) Ruler (FHIR / CDS Hooks)
- CQL Services (Custom REST / CDS Hooks)

** An incomplete list*

MITRE

Resources

- CQL: https://cql.hl7.org/
- FHIR®: http://hl7.org/fhir/
- FHIR® Clinical Reasoning: http://hl7.org/fhir/clinicalreasoning-module.html
- FHIR® Clinical Guidelines: http://hl7.org/fhir/uv/cpg/
- CDS Hooks™: https://cds-hooks.hl7.org/
- SMART App Launch Framework: http://hl7.org/fhir/smart-app-launch/
- BPM+ Health™: https://www.bpm-plus.org/
- Atom CQL extension: https://atom.io/packages/language-cql
- CDS Authoring Tool: https://cds.ahrq.gov/authoring/
- CQL-to-ELM Translator: https://github.com/cqframework/clinical_quality_language
- CQL Testing Framework: https://github.com/AHRQ-CDS/CQL-Testing-Framework
- CQL Execution Framework: https://github.com/cqframework/cql-execution
- CQL Engine: https://github.com/DBCG/cql_engine
- CQF Ruler: https://github.com/DBCG/cqf-ruler
- CQL Services: https://github.com/AHRQ-CDS/AHRQ-CDS-Connect-CQL-SERVICES
- AHRQ CDS Connect: https://cds.ahrq.gov/
- Additional Community Projects: https://github.com/cqframework/clinical_quality_language/wiki/Community-Projects

MITRE

Chris Buchanan & Chris Moesel

cjb@mitre.org & cmoesel@mitre.org

@MITREcorp

linkedin.com/company/mitre

MITRE | SOLVING PROBLEMS FOR A SAFER WORLD®

Building a Hyperledger Indy Network - Questions, Discussion, Etc.

Tuesday 1H
Convener: Lynn Bendixsen (Indicio)
Notes-taker(s): Gary de Beer, Lynn Bendixsen, Video Recording, Slides

Tags for the session - technology discussed/ideas considered:

Hyperledger Indy, Network

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

Slides link:
https://docs.google.com/presentation/d/1sUG4297GiRcUdu4aqQnc0Op0LMhbwiqy9LIAINHfSFQ/edit#slide=id.p1

Lynn did an overview of slide 3 with some great input from Paul Bastian and then opened it up for questions/comments. Questions/discussions included:

Where does discussing/determining standards belong in the flowchart?

Suggestion: Add creating different types of Networks to the flowchart (testnet,stagingnet, mainnet, etc.) Discussed cross Indy Network compatibility. It 'should' work but there seems a requirement that Verifiers would need to support/connect to any network they chose to allow holders to present credentials from. Governances issues: What if an Issuer did was 'fake' ledgered on a different network to impersonate them?

When will we upgrade Indy networks past 16.04 which is EOL at end of the month? (Soon, within the next few months. Upgrade will go straight to 20.04. Exact date unknown, no current contingency plans exist for nodes that "expire" support before the upgrade)

When do we talk about scalability? Are Indy networks scalable enough for my needs? (Lots of time was spent discussing this topic at various points in the meeting.)

Links to guides for creating your own Indy network:
High level:
https://github.com/trustoverip/utility-foundry-wg
Technical details (implementation):
https://docs.google.com/document/d/1Tg4dAEtC78TxG9AsIby_CfpbeOicK_YMKznSQOvtIVU/edit

GLEIF and KERI (Global Legal Entity Identifier Foundation)

Tuesday 1K
Convener: Karla McKenna
Notes-taker(s):

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

The Global Legal Entity Identifier Foundation (GLEIF) proposes that the Legal Enitity Identifier (LEI) can be used to establish a chain of trust for organizational identity.
In this session, GLEIF shares plans and progress regarding its development program to create an ecosystem and credential governance framework, together with a technical supporting infrastructure, for a verifiable LEI (vLEI), a digitally verifiable credential containing the LEI.

Link to presentation available until April 2022:
https://td2ec2in3mv1euwest.teamdrive.net/bgvkygms/public/I39DS3Tn?k=MMiiLXItHvmxOtB0kFROQGXMTDFgjCngWTiQFed43Ak

Mobile Agent Development FAQ

Tuesday 1L
Convener: Horacio Nunez (horacio.nunez@kiva.org)
Notes-taker(s):

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

This session had the objective to gather (and discuss) a set of recurrent questions people experience when trying to build their first mobile agents.

This was the end result of the session:

FAQ:
What's the best place to start creating your own mobile agent?
How do you get updates once you ship your first version?
Do I actually have to support a fork for every mobile agent I create?
Do I need to use a Mediator?

9a.m. PT: W3C CCG Weekly Call About VC HTTP APIs

Tuesday 1P
Convener: W3C CCG
Notes-taker(s): Orie Steele

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

We discussed:

https://github.com/w3c-ccg/vc-http-api

https://github.com/w3c-ccg/community/issues/190

https://github.com/w3c-ccg/community/issues/191

See also https://w3c-ccg.github.io/meetings/

The Principles of User Sovereignty and A Unified Theory of Decentralization

Tuesday 2A
Convener: David Huseby
Notes-taker(s): Dave Huseby

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

This was a reprise of my sessions from April, 2020 to set the table for follow on sessions about the authentic data economy. I wrote two articles about these topics a year ago:

https://uxdesign.cc/the-principles-of-user-sovereignty-515ac83401f6?sk=d37a69c8efc8a48cdd4a23d0518ba8d0

https://medium.com/swlh/a-unified-theory-of-decentralization-151d6f39e38?sk=b2a71917dcb5ce948196887c7ff48fde

Before setting out on solving the authentic data solution for global scale I wanted to best understand the problem of decentralization and then declare the principles that I bound myself while solving it. There was very little discussion other than some clarifications on what I mean by "absolute" privacy by default and how that may make users reluctant to use any software like that.

Zoom Chat:

10:04:52 From Phil Strong to Everyone : can you record this?
10:05:37 From Catherine Nabbala (Finema) to Everyone : Yes pls. A recording will be highly appreciated
10:06:25 From dsearls to Everyone : to record, please become the host. By clicking "Participants" and then "Claim Host". Then enter 232323 as the claim-host-key.
10:14:31 From windley to Everyone : I thought Dave was *trying* to scare people :)
10:14:47 From dsearls to Everyone : privacy is personal. that doesn't mean it isn't also social, political, technical, legal or anything else. But we know, feel and experience it personally. We (projectVRM, Customer Commons, the spirit of Linux Journal) have a Privacy Manifesto on a wiki here: improvements welcome. https://cyber.harvard.edu/projectvrm/Privacy_Manifesto
10:16:20 From dsearls to Everyone : We are at Square 0.x for making privacy work in the digital world. We are at Square 9000.x in the physical world, where Square 1 was clothing and Square 2 was shelter—our first two privacy technologies.
10:16:36 From camparra to Everyone : So surprised to be hearing about equity here
10:16:45 From camparra to Everyone : Really good improvement guys :D
10:16:49 From Bill Wendel1 to Everyone : Adrian, your feedback echoes a real estate use case. Asked a vendor who has government money to distribute rental assistance to tenants who are being protected from eviction. Asked if their system is using any kind of digital identity to verify the tenant's eligibility. He said, as Dave just did, we're still using paper based applications because many people at risk of eviction do not have access to tech tools or know how to use them
10:17:04 From Scott David to Everyone : So. . . What is the value proposition?
10:17:20 From dsearls to Everyone : What is the value of privacy?
10:18:05 From Scott David to Everyone : So. . . what is the value proposition specifically here vis a vis privacy, etc.
10:18:24 From Robert to Everyone : for those who do not have OCR nearby: https://uxdesign.cc/the-principles-of-user-sovereignty-515ac83401f6 ;)
10:18:40 From Scott David to Everyone : We stopped Dave early in the presentation. Please go on!
10:18:53 From Scott David to Everyone : Super-duper privacy by default.
10:19:06 From Grace to Everyone : ultra-super-duper
10:19:09 From Kimberly Linson to Everyone : +1 Scott
10:20:22 From matthewhall78 to Everyone : When you say "Paper-based" is this just a printed QR code, or is this some kind of a smart paper that has a finger print scanner on it? How do I confirm that I'm the correct holder of the credential?
10:20:44 From Nader Helmy to Everyone : Are these principles of user sovereignty a north star to aspire to or a forcing function?
10:21:01 From Michael Lodder to Everyone : I believe its something to aspire to
10:21:07 From Mark Lizar1 to Everyone : A Consent Receipt - is a physical and digital receipt.
10:21:09 From sankarshan to Everyone : Notes from Adrian's session are at https://docs.google.com/document/d/18ZGPKu4e46zeCm88Xzj74ggzulRI24WFoSiIDnHO6mE/ includes th e link to the document which has Adrian's proposal
10:21:50 From Jeffrey Aresty to Everyone : I work extensively in the mediator space - it's a possible solution; but the training of mediators is a challenge - we are working on it; they know nothing about SSI
10:22:06 From Scott David to Everyone : Step up attributes in control of individual?
10:23:03 From Scott David to Everyone : "Knowing" in the eye of the beholder. Bank doesn't "know" their customer "in the biblical sense."
10:23:49 From Robert to Everyone : In case of Amazon they don't know they own customer :P
10:23:51 From Adrian Gropper to Everyone : This is the role of a notary as presented in many SSI contexts
10:23:52 From Scott David to Everyone : Metrics of identity as consumed by perceiver. Decoding of identity. How set up the encoding and decoding from a signal theory perspective?

10:23:53 From joehsy to Everyone : It is not clear if this satisfies the “know you’re customer” regulations as they are written now.
10:24:32 From Michael Lodder to Everyone : Legal has yet to take a look at this
10:24:54 From Michael Lodder to Everyone : I haven’t heard of many lawyers in this space and pushing it to law makers, I would love to see that
10:24:57 From Jeffrey Aresty to Everyone : we have thought about notaries - the differences between the civil and common law systems matter - and local regulations will be significant - it's a path to follow
10:24:58 From Scott David to Everyone : Have we again sidetracked Dave from revealing the value proposition or is this moving toward it?
10:25:43 From Scott David to Everyone : Lawyers are rhetorical engineers. They work in intangibles.
10:25:52 From Mark Lizar1 to Everyone : LoL
10:25:52 From Scott David to Everyone : +1 Phil.
10:25:55 From Jeffrey Aresty to Everyone : The law maker space is problematic; as an attorney working in private international law for 40 years, we need to focus on best practices from the ground up to drive a solution through adoption
10:26:06 From Mark Lizar1 to Everyone : +1
10:26:19 From RickC to Everyone : Guys and gals, could I suggest we get through this quick pitch and hammer Dave with questions then.
10:26:22 From Scott David to Everyone : I have a question about Doc presenting as a human.
10:26:47 From dsearls to Everyone : These days I try to present as a glowing rectangle.
10:26:52 From Andre Boysen to Everyone : If it is not taking us off track I would like to suggest another principle for user sov
10:27:02 From joehsy to Everyone : Agree with Phil that online Pseudonimity has unique characteristics not found in the physical world.
10:27:12 From camparra to Everyone : A lot of these principles would scare governments … so is it adoptable?
10:27:48 From Scott David to Everyone : +1 Doc. You can tell it is Doc because he always “glowing” whatever the vehicle.
10:28:46 From Grace to Everyone : Almost everything scares government these days.
10:29:31 From Scott David to Everyone : User sovereignty associated with what subset of all user actions?
10:29:45 From camparra to Everyone : Well they are central authorities of identity so we need them on board
10:30:15 From Scott David to Everyone : User sovereignty increases by living off the grid, but lack of electricity means that you cannot even be on the “user subjugated” end of the slider.
10:30:38 From Cam Geer1 to Everyone : @ camparra or replace them
10:30:41 From dsearls to Everyone : Are users easier to subjugate than persons?
10:30:41 From Grace to Everyone : Depends on which way you are approaching the problem. Some people are trying to make change from within, and some are trying to create alternatives. Both approaches are legit.
10:30:49 From Scott David to Everyone : Does a red traffic light “subjugate
10:30:57 From Scott David to Everyone : Subjugate drivers?
10:31:24 From Scott David to Everyone : Does a red traffic light “liberate” or “subjugate” drivers? Answer=yes.
10:31:48 From Trevor Butterworth to Everyone : It liberates pedestrians!
10:31:58 From Scott David to Everyone : Lock in is a valid test of subjugation
10:31:59 From Frederico Schardong to Everyone : So user-sovereignty = portability?
10:32:15 From Grace to Everyone : I think he's saying it's one component of sovereignty
10:32:36 From Scott David to Everyone : Is “presentation of self” always subjugated, in that each platform “encodes” users similarly for interoperability?

10:32:42 From dsearls to Everyone : I see a continuum from minimized to maximized freedom or agency, with a social media feudal system on one end and whatever Dave's talking about at the other.
10:32:46 From Mark Lizar1 to Everyone : +1 - proposing principles - e.g - human identity and trust - vs. Digital identity and trust semantics for trustworthiness. Notice Control Semantics - so important. - Centralize transparency (sousveillance) and decentrlalize suveillance - and reference the human controller
10:34:34 From dsearls to Everyone : I think the next session, on making the intention economy happen, will be about what Dave is moving toward here.
10:35:02 From windley to Everyone : +1
10:36:17 From Scott David to Everyone : Suggest attention to ownership of “data rights” rather than ownership of “data” per se. You will not need as many antacids in the future if you stick to asserting ownership over rights/
10:37:00 From Cam Geer1 to Everyone : great point Scott David!
10:37:03 From Scott David to Everyone : Clarification of “distributed” versus “decentralized” is critical. See Paul Baran paper for RAND corporation for graphics.
10:37:07 From dsearls to Everyone : You doing a session on that, Scott? Would be good.
10:37:33 From windley to Everyone : Scott, cars are more decentralized than, say, mass transit (more autonomy, substitutability, agency). But it requires people to follow rules, which should be mostly analogous to protocol. Decentralized systems need more *explicit* rules than centralized systems.
10:37:47 From Scott David to Everyone : Need to clarify what actions the platform leverages and derricks and what it demands in return.
10:38:22 From windley to Everyone : I’d quibble with the use of the word “platform” and say “system” but yes, that’s the point of protocol, right?
10:38:45 From dsearls to Everyone : I visit Paul Baran and his graphics in Escaping the Black Holes of Centralization: https://blogs.harvard.edu/doc/2014/03/21/escaping-the-black-holes-of-centralization/
10:39:06 From Alan Karp to Everyone : @Scott: I think Dave means something different than Baran for “distributed” and “decentralized”. Dave means distributed computation and decentralized control.
10:39:10 From dsearls to Everyone : Twitter is the example of a hole there, and why it goes at the far left end of Dave
10:39:15 From dsearls to Everyone : 's graphi.
10:39:17 From Scott David to Everyone : I define sovereigns as any entity that “does not need to ask for permission or forgiveness”. That raises a Godel “incompletenesss theory” problem: Every system has statements and questions within it that cannot be answered from within. This is why identity of “subjects” by a “sovereign” is always ticklish.
10:39:23 From camparra to Everyone : Where are the majority of the bitcoin nodes located?
10:40:08 From Cam Geer1 to Everyone : +1 Doc re: Twitter
10:40:38 From Scott David to Everyone : Identity is ONLY useful in interactions. Interactions take two to tango. Two means that there is an externality. Externality cannot be directly controlled. We are all frustrated sovereigns, some of us get over it as adults!
10:41:09 From Andreas Freitag to Everyone : Usability in decentralized systems or SSI, very interesting topic
10:41:13 From Mark Lizar1 to Everyone : +1 semantics are so important — - user sovereignty is semantically referencing a state of system permission - aka - in this conversation an enslaved digital citizen.
10:41:29 From windley to Everyone : Yes, we build identity systems to manage relationships
10:41:43 From Scott David to Everyone : +1 Mark. We self-bind to rhetoric of governance in order to be free!
10:41:53 From dsearls to Everyone : baron's "distributed" drawing shows everything as connected, which on the Net we actually are not all the time. There is optionality about being connected, and what we do when connected. Which is why I call the fourth (beyond "distributed") network "independent."
10:42:11 From dsearls to Everyone : Baran. Not baron. Got auto-corrected there.

10:42:16 From Scott David to Everyone : Free from the risk of harms from P2P parties with others that are similarly bound to the sovereign.
10:44:30 From Scott David to Everyone : Sovereign (and the property concept) are ALL teleologies. All narratives created by humans to which we can self bind to deal with complex societies. ALL deities, nations, royalty, companies are projections (with apologies for the blasphemy). New sovereignties are "computational" - AI, crypto, blockchain, etc. have sufficient computational authority that it invites consideration of human self-binding. HOWEVER, like all sovereigns, we bind in way "X" in order to liberate ourselves in ways "A, B, AND C"
10:46:08 From Mark Lizar1 to Everyone : +1 Scott - A bundle of data control / privacy rights can = property rights with the right bindings
10:46:20 From Andreas Freitag to Everyone : A well designed PoS consensus
10:46:40 From Luke Ledet to Everyone : I'm sold, how do we use it? What's the most decentralized technology available now with a wallet I can have my users install and use?
10:46:49 From Scott David to Everyone : Like NEWPORT RI, railway millionaires: Decentralized systems generate wealth for gate keepers.
10:46:59 From Robert to Everyone : Decentralization is not about increasing power of user but equal distribution of that power
10:47:11 From Scott David to Everyone : Being a gatekeeper takes many forms: rhetorical, financial, regulatory, etc.
10:47:31 From Charles E. Lehner to Everyone : This project addresses the concern about value distribution between early and later users in cryptocurrency issuance: https://duniter.org/en/introduction/
10:47:32 From Grace to Everyone : I think that is a good topic for a separate conversation. It's not just about the protocols.
10:47:37 From Jordan McKinney to Everyone : Maximizing agency/freedom will always produce unequal outcomes in terms of wealth etc
10:47:38 From Frederico Schardong to Everyone : +1 Andreas, Proof of personhood seems like a viable consensus in this sense
10:48:02 From Scott David to Everyone : What is purpose of money is left unsaid
10:48:05 From Stewart Whitman to Everyone : +1 Scott David, how do you regulate the gatekeepers?
10:48:17 From Grace to Everyone : +1 Scott. Money is an antiquated protocol.
10:48:24 From Scott David to Everyone : Money as a risk consolidator (Hannessman) put it in line with nation states.
10:48:33 From Mark Lizar1 to Everyone : We need standardized transparency and accountability
10:48:51 From dsearls to Everyone : My old business partner said "Trust breaks down first around money." I'm not sure that applies only to fiat currency.
10:48:58 From Stewart Whitman to Everyone : Not true, money (and bitcoin) is subject to supply and demand, re: gatekeepers
10:50:04 From Scott David to Everyone : Nation states have the monopoly of legitimated violence in society (Mills). So government can take your life, imprison you, etc. Change of status of physical human instantly changes status of digital representation. Like "entanglement" in quantum! If I die now, I lose legal capacity instantly. Legal capacity is determined by the nation states as operating system.
10:50:32 From Scott David to Everyone : Nation states issue currency as power exertion. They will not relieve themselves of that power easily. This will be interesting.
10:50:57 From windley to Everyone : +1 Constitutional orders are based on legitimacy and almost always change through war (violence). A fork is a crypto war.
10:51:08 From Kevin Dean to Everyone : We clearly had mothers who went to different schools of child-rearing.
10:51:14 From Kevin Dean to Everyone : 😎
10:51:42 From camparra to Everyone : Thanks, Phil! You cleared up my concern

10:51:48 From Scott David to Everyone : I, nation state, issue currency. I, nation state, demand taxes. You must pay taxes in the currency that I issue as sovereign. I, the sovereign, therefore include myself in every interaction in which wealth changes hands. This is my regulatory reach.
10:52:19 From dsearls to Everyone : <apologies/promo>Again, my following session, on making The Intention Economy happen, should leverage some of what's being said here. </apologies/promo>
10:52:45 From windley to Everyone : +1 Scott. This is going to be really interesting.
10:53:08 From dsearls to Everyone : https://www.amazon.com/Scale-Free-Networks-Complex-Technology-Finance/dp/0199211515
10:53:43 From dsearls to Everyone : https://trustframe.com/
10:54:05 From Scott David to Everyone : Active Inference provides a potential statistical/mathematical structure for SSI aspirations. See Karl Friston, etc.
10:55:03 From Scott David to Everyone : Scale independent solutions are a good sign of actually achieving complexity friendly governance.
10:55:17 From dsearls to Everyone : Serious question: What is the "data economy?" Also, is there just one? Is it different from the economy itself?
10:56:24 From Scott David to Everyone : Fractals display scale-independent variables. Fractal governance sounds crazy, but is pretty predictable when humans are getting creative about all the challenges. The human mind is the constant at all scales, so
10:56:24 From Robert to Everyone : HCF definition: It is economy which is driven (fuel) by data, current economy to some extend it is already
10:57:08 From Robert to Everyone : If you get to the authenticity and privacy we call it Dynamic Data Economy which introduce security (authentic data flows) into "data"
10:57:17 From Scott David to Everyone : Perhaps sometimes people perceive SSI and its cousins as too much of a bundled set of products.
10:57:25 From dsearls to Everyone : When a lot of people talk about "the data economy," they mean the advertising one, aka "surveillance capitalism" that thrives off of data gathered about personal activities
10:57:37 From Scott David to Everyone : What if want to do some of it, but don’t want to buy into all of the aspirations?
10:57:49 From Scott David to Everyone : +1 to Doc.
10:57:52 From dsearls to Everyone : I think it's bigger and other than that, but I do want to flag it as a common assumption.
10:57:58 From Robert to Everyone : I would argue that "surveillance capitalism" is based on data but not data flow.
10:58:26 From Scott David to Everyone : I guarantee it will not be more sophisticated, but it may be nuanced.
10:58:34 From Robert to Everyone : by data flow I mean that I am free to steer my data whenever it serves me

101 Session: OAuth2

Tuesday 2B
Convener: Aaron Parecki
Notes-taker(s): Aaron Parecki

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

https://aaronparecki.com/tag/iiw and https://aaronparecki.com/tag/oauth2

> OAuth 2.0 Simplified is a guide to OAuth 2.0 focused on writing clients that gives a clear overview of the spec at an introductory level.
> In 2017, I published a longer version of this guide as a book, available on oauth.com as well as a print version. The book guides you through building an OAuth server, and covers many details that are not part of the spec. I published this book in conjunction with Okta.

https://speakerdeck.com/aaronpk/oauth-101-internet-identity-workshop-xxxi

How OAuth Works 12 videos

godiddy.com Universal DID Services

Tuesday 2C
Convener: Markus Sabadello
Notes-taker(s): Jan Christoph Ebersbach

Tags for the session - technology discussed/ideas considered:

SaaS, Wallet, DID

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

- Centralized service that shouldn't be used to host security sensitive DIDs, it contradicts the principle of self-sovereignty. The service is meant for developers to try out the technology.
- Godiddy is a service that hosts the community components universal resolver and registrar + additional proprietary components so that it offers a comprehensive DID service for creating and managing DIDs across multiple methods.
- How robust is the service on bad network connections? Markus: There are github issues concerning TTL in the DID spec WG. Self-hosting is likely to be a better option than using the centralized service.
- Feature Grid with future ideas: https://docs.godiddy.com/en/feature-grid
- Key Management: When keys are created they are stored in the wallet and are returned to the client. This is not ideal from a security point of view. An improved API is planned that would allow clients to keep the private key on the client and use the service to create for example the DID Document -> this is also part of the next session.

Why the Internet Needs DIDComm

Tuesday 2D
Convener: Sam Curren
Notes-taker(s): Brent Shambaugh

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

Presentation Slides: https://docs.google.com/presentation/d/16HTPyZV_-BtM6EifQpxjivRHKYUeVtOAReUD1eGUA9M/edit?usp=sharing

How to receive and track LoRa Satellites (TinyGS). Incl. innovative ideas for your projects
Project Cambria: managing schema change in distributed systems, Geoffrey Litt and Peter van Hardenberg

Taking notes:
Why the Internet needs DID Comm

Any questions?

I am going to make the argument that the internet needs did comm.

The DIDs are wonderful. What they do. The harmful effects of 3rd party identifiers. They could take that away. DIDs do a good job solving that.

APIs are wonderful. I think the reason that we have powerful things on the intent is b/c of API.

When it comes to persons on the internet, we are still bound by apis.

downside I am not always able to use https.

e-mail is the lucky exception. I think it is b/c mail has been around for awhile and it is a protocol.

why is e-mail not hostage. it is hard to innovate but it is widespread.

it is too hard for one company to control. twitter can change things, and nobody can stop them. they had an api, but tehy wanted control.

e-mail. intelligence is at the edge. the mail clients that are involved. we need more things like e-mails. we need to emulate and improve on it

i don't think that did comm is going to kill e-mail. I think there is a lot to learn... e-mail identifer...a bunch of usernames have become e-mails.

e-mails are approvable identifiers.... good for password recovery...

can we make e-mails into dids? dids as did documents .... can see where I am going.... did comm can be as powerful as e-mail addresses.

Benefits of did comm. enables verifiable presentation....has routing....that moves messages....all the intelligence is in the clients....
it is protocol based like e-mail.... it supports https like apis...

One of the really cool ones was did comm like bluetooth... that enables it to mobile and offline friendly...if my battery dies and I have
bad cell reception...the message based nature of did comm ... will make it friendly to devices like that...also allows rotating of dids with another dids

there are a lot of different did methods that don't have all the features that you want...

the peer-did method... not stored on a ledger... the ability to rotate from one did to another ... allows you to cross did methods...

did comm allows security ...transport ?/

work about ... security transport of did comm over different....

anyway...we can't stretch this too far...

a lot of apis are built on http....api don't have to start with http...but still get the benfits of it....

it is unline http in that it is a higher level....

it doesn't fall in the same position of the stack...

try to present some diagrams.... good work being done on the did core spec...it doesn't do a lot itself...just enough to exchange dids ...

representations of protocols that can be built on that....protocols to send human messages .... to send verifiable credentials...

work on did comm meeting group at diff..

drawing that diagrom...have alice and bob...have dids and did documents to interact...

I've said a lot of words? any questions have a lost anyone?

George said, Do you think the monotic nature of dids will be a problem?

You're right. Nobody wants to remember a did. I think that all of the operations of the DIDs..

What I am thinking is you go to someone, and you say what e-mail address? My Dad doesn't have a smart phone. I worry about something
where a device must be present to establish communication. It is the think that has all of the dids. I have to choose which one of these
makes sense. you can type in george fletcher and there are the dids. e-mail.

yes, you sound like a plant. I will talk a bit about it tomorrow. If people have to see the tech, then we are doing it wrong. You are
correct that this ecosystem has that not ... but there will be a part... concrete work?

Google wave..
I've thought about the ... kind of a replacement for e-mail...but then it died because google kills things.

There is attachments....there is better semantic meaning in did comm than e-mail.

(question)

guardianship is a good one. compensate with smart card or a piece of paper. You need people to be able to partipate in an ecosystem.
Cool. I want to touch on DID Comm transport. http. https. websockets ...

people have done things with bluetooth, but not standardized.. we've experimented with qr codes. If you and I want to exchange dids.
If we present. QR code nice way to transport . usability

did comm with rfid. lots of similiarities between reading an nfc tag and ...

lots of transports, that is a useful thing because it enables a peer-to-peer thing..

here is a big ... independence of the security model ... not relying on the security of the transport layer... did comm ...transport encrypted ... so you can use https but you are doubly encrypting... it ends up being rendundant...

cause of https... different than websockets ... different from bluetooth...if we relyed on the security of the transpart...
then ... can switch to bluetooth ... don't lose things that the security provides...

when developing on did comm not ... security of transport layer... downside is we lose the independence of the transport layer....

there is more...more on the transport...

paul...says that NFC is the only thing.... paul you are right. NFC does have some problems. It is not entirely foolproof. Someone with a good camera can see
exhcnage.

identifers with dids and did documents. did comm gets you protocol discovery support. you don't have to develop something.... processing flows...I didn't type
this in but you cna have multiple parties in a flow...

desinging a did comm protocol it isn't more complicated than designing an http api.

there are two version of did comm. comes to be v1 and v2. v2 is what we are now working on at DIF. There is lots of good work going on here, and I am quite excited
about where it is going.

the last time I edited it was in january. I didn't update it. the first 90% and the second 90%. We are definitely in the 2nd half.

If you want to join us. If you are a small organization. streamlined way to join DIF. The calls are at noon U.S. Pacific.

Questions, thoughts anything. Sam you don't think that did comm will kill email, why?

did comm has a lot of advantages that e-mail doesn't solve at all. did comm will build on..

advanced open source chat. most...wouldn't have had a problem...goal of did comm was not to solve chat...

e-mail itself will decrase in usage...b/c there is a lot of suff that it isn't good for...now it may fall off...but if it does kill e-mail it will take a long time...

The first thing ... having a did comm connection basically means you exchange dids with another party... messages will travel independently...you will send messages
travel...

having a connections mean you've exchanged dids with another party. we can communicate with that did comm that we are confident that the other party will see.

there are two ways that updating that connection happens. If we update e-mail. We will update MX records. If you are going to move for whatever reason
you will update your did documents. if it is keri you will approximate with keri. then when they send the message next time. this is analagous to updating MX
records in DNS. If we communicate...all of sudden we find ourselves together at the coffee cart at IIW. We can send messages across... using the keys...
Of course if we walk away than we can still use the connection...

technology doesn't allow it...still finalizing the way that the transport will work

q; you talked about that analgous updates in mx. .... are we creating an opportunity to correlate....sharing mx record...if they sidechannel they realize that they
all talk to me... the thing is technology allows that. you can use.... you are reusing the same did that allows for correlation.

you are going to have a unique key for each person, you get what is called herd privacy...it is sort of like the way that ... if you use g-mail...that gives herd privacy...

the other thing is the ... you won't personally have to do that...your software in the background will work on relationship names... as developers that is one thing
to consider...

what would you compare...

that's a really good question..I actually see a lot of these things as complimentary. did comm thrives in things that are not browser based. various levels of support.
chaffee doesn't care...enables ... chapi relies on the fact ...nor does it need to for a particular use case....

did comm like .... couple options....chapi did comm transport...standards how to use chapi as credential exchange .... and so there has been some talk about using
the chapi like API and extending them outside of the browser. the other one, as long as.... there is a harmonious part... enable a user as a part of a reality of
servives...

one question regarding ... one thing when introducing new protocols....if did comm becomes the trust layer for the internet...how old servers...old technology...

when I say the internet needs did comm... will say that the web will continue to exist. I don't think that is going away. if you would like to leverage the features of
did comm...tunnel over that connection...if you have ... this is a messaging oriented...could get to a stream oriented ...

if you had something that was message based...could tunnel and e-mail

my question...did comm for establishing trust... anything one has used....use did comm and establish initial trust....

that's great I mis-understood. caller id is untrusted. scammers ... I could imagine a protocol where you could pre arrage a phone call through a did connection... maybe
it could use... it could allow to transfer some amount of trust between ... excellent way to use did comm to use pre call handling ... now you have implemented some trust
in a prexisting...

kyle your hand is up...

we haven't pushed this out to a standard... use a username and password.. you use a username and response... access to tokens ... post on a login screen...QR code that is
scanning...agent that you are responding ....trust by authentication serve....respond with a standard...

pass back ... authenticate this token...you are actually using this to be able to authenticate...

that's cool...kyle you have peaked georges interest.

openID connect doesn't sound like anything you authenticate.... verifiable credentials....

the BCR spec specifically is built to allow sort of random....has multiple ways....any ecosyem... it doesn't actually prevent impersonation but it makes it harder. if did comm
allows for proof... the entity that ... how does my mobile app instance....

register my mobile app instance have some assurance ... this is an entity that I want to communicate with....generally...what I think will happen at the dcr side of things.
I actually have 2 talks about this. using the os ability to attest to this app.

Bringing all of this back, why do I even care? This is sort of answering. We are running into this specifically. Browser....some of that infrastructure may be easy to work
with, some of it not. I like the idea of using did comm from an authentication perspective..

so kyle is on the Q. I want to mention one more thing george.. could have openID connect have a side effect of DID COmm. When I think about every site asking to send push
notifications...if you had something....

DID Comm could be first, or it could be last. I definately see a lot of ways....sending a coding via SMS to a phone is inherently insecure....there are a lot of opportunities
there....and then prioritize...

George....Kyle...

the public clinet registration?---mobile app will register with .... could have the authorization method send back a shared secret.... could have some reasonable trust...
if you use the client id and client secret...you could use the protocol that way...DCR is really about how you can .... the tricky part... openID spec that was
done first... most people a mix of both....for most people it isn't that clear

OpenID connect...In terms of authentication....zero RC is effect... we are oftne times trying to integrate request token....set up HTTPS call... try to releverage....
Use two factor authentication.... Zero round trip is the ....

protocol of exchange...worked around in v2 and send to the other party ... sematniclly meaning ful... before talk ....

did com...progress...in v2...anything added to v1...pretty close to frozen....add .... contains ... steps

making .... short answer v1 deprecated and moving to v2...

Him and I have envisioned....starting to do JWM kind of messages ....by the time we hit 3.0 doing did comm v2.

v2 contains an optional target that a lot are working with....will help with the aries community....

try not to communicate any of the energy in v1...difference in how we handle ....should make migrating factors easy...

(q)

likely how it happnes.. build on v2 unless they want compatibility .... this is a way of formalizing...now we will change the defualt into the new and now
we will remove the old...there is a lot of energy to reach compatibility in aries...we will make rapid progress there...

everything I've seen is very few people.... when secuity...https over did comm...didn't see it going anywhere....nobody has explored...most common answer...
people going in direction as most valuable for their use case at the time....find some sort of way...

Ivan will host something very technical tomorrow... reading into your question... how to present verifiable credentials amongst clients. Kiva presented an
SVG(?) client on

SVG is very nice....if you include in client...something that used to display...

ongoing efforts .... browsers ... sometimes they get along, sometimes they don't...directly collaborative or not...how to make it consistent.... how to leverage
As there is an interaction...

Where my mind goes ... lets me skip the refinement process.... in general it is knowable how to .... did comm messages ... it is a little better than e-mail...
trying to learn our lesson...protocol... rather than encode an image include it....the software would know...

Have you ever send over constrained networks like IoT?

some explorations....lots of talk...when you got to IoT it gets varied... compare to raspberri pi...some have cryptochips...some don't ... currently out of spec...
would love to see work to see how it integrates.... a lot of these things will communicate with a gateway... the gateway could be the point...

the average size of the did comm message in the size of 5kb....also consider cryptographic auth... if you push into 256kb of ram...start have ...constraints of messaging

system...can make it work on very small...

running and creating the message....the challenge is transporting through the constrained network...we've talked about a compact form for did comm envelopes.... one of
the things that might help....convert from did com from using a JSON payload to a binary payload.... considered future work not part of v2.

we're rouly at time... happy to answer questions....

the best iiw sessions are not presentations sessions... if you are curious about future things....did we talk about did comm over NFC... we did talk about early...

Decentralized Semantics 101

Tuesday 2E
Convener: Paul Knowles (paul.knowles@humancolossus.org)
Notes-taker(s): Neil Thomson

Tags for the session - technology discussed/ideas considered:

Data, Semantics, Schema, Input, Data Capture

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

The form of the session was a presentation (intended for those new to the subject), followed by Q/A and discussion

Presentation: Decentralized Semantics 101

Vocabulary:

- Form - taken from paper forms used filled in by subjects and service provider reps (e.g., clinician). A Form is a composite/aggregate packaging of claims/attributes from one or more Verifiable Credentials (VCs) for presentation (e.g., to a verifier) or for data exchange.

Q/A & Discussion
[Erica Connell] If a DID has a DID Doc, how does a VC exist with relation to a DID?

A Credential is something you would put in your wallet. Using a vaccination (status) VC as an example, what you put in your wallet is an equivalent of a paper vaccination card with your identifier (of some kind, binding the card to you) and a date completed. All the supporting data (including PII data, details on the lab, vaccination batch, etc. etc.) may be in separate VCs (which the vaccination status VC is derived from), such as detailed information on the vaccination visit.

A DID is NOT the identity of the holder, it is a communication channel identifier for enabling holder to service agency communication. A DID may be created for each communication channel (e.g., one for each internet service) or for each transaction.

A subject/holder's identity is defined by their VCs, which are obtained from an Issuer by creating a communication channel where the Issuer and Holder each present a DID for the channel, verify identity and trust by exchanging existing VCs (with minimal disclosure), followed by the Issuer creating and delivering a new VC, based on data (lab vaccination data/credentials) held or provided to the Issuer (e.g., it's issued by the lab that did the vaccination).

[Steve Venema] - How does the Dec. Sem. model work with the lifecycle of a VC (e.g., specifically revocation)?

Scenario - your vaccination VC is revoked (rendered invalid) by a later discovery that the vaccine was not effective, or the vaccination batch was compromised.

Revoke in this case may be marking the VC as being invalidated (note: should be a standard field for any VC, including a reason for the invalidation). There is still value of the invalidated vaccination VC (and underlying health record data), so "revoke" is not = discard the VC (and underlying data)

A key layer (top layer in the Trust over IP model is governance. And governance is determined by jurisdiction (e.g., national, province/state, agency, ….), which is where complications due to different criteria, processes and approval complicates interoperability .

[Erica Connell] What is decentralized about this approach?

While the creation of the data collected for a vaccination and how a vaccination status VC is constructed and bound to the user is defined by a governance authority (central), the key is that while a [VC] Issuer will keep a copy of the issued VC, the holder (person) for whom the VC was issued is the one that stored and controls access to their VCs and health card records.

This is analogous to a paper travel passport. The Gov't may have a record of issuing it, but only you - the person in possession of the passport - determines where it is stored and where it is presented.

How decentralization applies to the Input/Semantic model

- Decentralized identity - authentic data
- Decentralized semantics – harmonized data
- Decentralized governance - distributed data
    - Root of trust – KERI vs. ledger (semi centralized)
    - KERI allows on personal device

A concern is that the current (many) DID methods which are typically tied to blockchains or similar ledgers become a lock-in a "root of trust". For example, if you have Europe and China using different DID methods tied to a different ledger (blockchain), then they will not share a root of trust, which makes interoperability difficult.

The KERI model allows for decentralized root of trust based on DIDs and other structures under control of PIK management controlled by the holder.

How does a holder/subject delegation (guardianship) work in this model (parent/child)?

Guardianship can go very wrong in a “crooked family”.

This is a complex topic covered in some other sessions (sovrin presentation by Jo Spencer at IIW 32). Two experts to connect with are Chris Buchannan (Mitre) and Jeff Orgel (Jeff O) who are both attending IIW 32.

[Lucy Yang] A key factor for delegation/guardianship is the governance framework (which is a key part of Trust over IP)

[Jeff O] A key issue on identity, guardianship and governance is that the human (operating system) needs a clear and understandable (but not necessarily simple) model of the roles, rights, responsibilities and interplay in a guardianship relationship - of the guardian and the dependent.

The digital (identity) operating system needs to support the human model, to the vice versa.

Governance in this case is derived from “Policy” and logically sound policies (on paper) don’t necessarily map to real life/scenarios or how people think about the subject matter covered by policies.

To be continued in other IIW 32 sessions..

OpenID Connect for W3C Verifiable Credential Objects

Tuesday 2F
Convener: Oliver Terbu, Torsten Lodderstedt, Kristina Yasuda, Adam Lemmon, Tobias Looker
Notes-taker(s): Kristina Yasuda

Tags for the session - technology discussed/ideas considered:

OpenID Connect, Verifiable Credentials, Verified Claims

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

Presentation Slides: https://www.slideshare.net/TorstenLodderstedt/openid-connect-for-w3c-verifiable-credential-objects

- Have been incubated in OpenID Foundation and DIF’s joint Self-Issued OpenID Provider WG - contact Kristina (kristina.yasuda@microsoft.com for participation details)

Presentation (link will be posted later)

- Goal is to make this work with any OIDC flow, any credential format
- Propose to extend a standard way to request claims in OIDC - `claims` parameter
    - https://openid.net/specs/openid-connect-core-1_0.html#ClaimsParameter
- Option 1

    - Are `credential_types` meant to be IRIs to VC type definitions?
    - From Paul DIetrich to Everyone: 02:13 AM
    - A bit of a OpenID newbie. The RP is the verifier and the OP is the wallet(holder)?

- Option 2
    - Aggregated and
    - https://openid.net/specs/openid-connect-core-1_0.html#AggregatedDistributedClaims

- Option 3
    -
- Discussion/Questions:
    - David Chadvick: more complicated request syntax is needed to cover more complicated use-cases
    - Mike: embedding VCOs inside an ID Token is the option easiest from the extensibility PoV
    - Vittorio: Re-using existing code is a painful illusion.
    - Tobias: another way to think about this - will all claims presentations require end-user re-authentication
    - DW: There are other credential formats (CBOR-LD, CWTs, etc.) coming up. Having VC/VP as a separate concept from ID token is a preferred option. Some use-cases might not require ID token.
    - Mike: possible to use the "claims" request parameter to request information from the UserInfo Endpoint
    - Daniel McGrogan: why using “userInfo” is not a preferred option from the consent aspect?

Security Considerations of KERI. Why & How KERI Provides Secure Portability

Tuesday 2K
Convener: Sam Smith
Notes-taker(s): infominer

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

https://identity.foundation/keri/docs/Q-and-A-Security.html#part-two-security

**Q: What are the security risks of KERI with regard to the identity protocol?
Harm that can be done to the a controller: Unavailability, loss of control authority, externally forced duplicity
Harm that can be done to a validator: Inadvertent acceptance of verifiable - but forged or duplicitous events

Breaking the promise of global consistency by a controller is a provable liability. However, global consistency may only matter after members of that community need to interact, not before. (SamMSmith)

*Q: How secure is the KERI infrastructure?
KERI changes the discussion about security. From a discussion about the security of infrastructure to a discussion about the security of your key management infrastructure. Most people when they think security, the think “oh, blockchain!”: permissioned or permissionless, how hard is it to get 51% attack, etc.None of that matters for KERI. KERI is all about “are your private keys private?!” And if yes, that drastically slims down the security discussion to brute force attacks to public keys. And because the next public keys are in fact protected by a hash, you have to brute force the hash algorithm, that is post-quantum secure. So that is a very high level of infrastructural security.
So private key management and protection is the root of your security in KERI.

**Q: Can I rotate keys with Tangem in KERI?
Suppose I’d trust a Tangem card for generating public private key pairs at will and the NFC communication allowing to interact with a wallet app.
One of the main concerns is that there is a theoretical link (a binding) between the cards and a user, via the card-ID (CID). However the CID is used only for checking the authenticity and integrity of the chip itself. Tangem publishes and anchors a list of CIDs with corresponding public addresses in a public blockchain. When checking authenticity, the verifier looks up the pub CID and corresponding pub address in the published list, and verifies that the chip controls the correct pub address by means of a challenge-response scheme. Even though for blockchain or SSI interactions, a completely new wallet with new pub/priv keypair is generated, the pub/priv key of the CID is used when the authenticity of the chip is checked by means of a challenge response scheme. Everything happens in the client app (2021: iOS or Android; and the client code is open source), where there is no communication with Tangem, so Tangem is not able to see any activity conducted by this CID in an authenticity check. The CID and corresponding key pairs are not used in any other interaction. A new wallet with new pub/private key pair is generated on chip, with these keys being used for any transactions, signing, etc.
Q: With the chip firmware being proprietary, how can we be sure that the newly generated private keys for new wallets are not still linked somehow to the cards CID? A: The firmware is audited by Kudelski and can be verified with a published hash. TBD: How can it be verified, when and by whom? If the firmware is not open source, then somebody has to draw a hash from it in an authorized situation. However, Tangem cards are EAL6+ and FIDO2 certified.
On the issue of Rotation: {TBW prio 2}

**Q: DHTs are not an immutable linear chronology oracle, which is the heart of the actual security problem. You claim KERI solves the security problem with DHTs?!

The immutable linear chronology is provided by the key event log (KEL) data structure itself. Getting a full copy is all you need. When retrieving a KEL over a network, then as you say a witness can prune some amount of the latest events, but every witness would have to be compromised for that to be undetectable.

If parties are so concerned, they could establish a large collectivised set of witnesses that sign and distribute all key events presented to this network (this would essentially be a Proof of Authority/federated blockchain but would require (configurable)% compromise for undetectable pruning of recent history. Only PoA/federated because the witness sets are designated by the controllers, so you could not just use arbitrary witnesses who join and leave the network at leisure (afaik).
The difference between the chain and the DHT is that not all DHT nodes act as witnesses for all KELs in the system (in the sense that they don't provide receipts for every KEL and aren't referenced in the witness sets

of every KEL), but they could all (or at least the ones holding the KEL you seek) still provide availability for KELs and thus would have to all be compromised in order to hide a recent-history-pruning, only one has to transmit the new/complete version to prove all the other versions as being old/incomplete.

(CharlesCunningham)
The point of KERI is to encapsulate all the guarantees within KELs nothing else is needed. DHT is just for resolution process to find a place from where I can get it. This place can change as you like I could even get it in p2p interaction from someone else. DHT seems to be the most reasonable way to build solid infrastructure for resolution process but none of the nodes can actually inject or tamper KELs so you don't have to trust them or get any guarantees from them. Since if the node will miss behave it is very easy to detect that.

(RobertMitwicki)
**Q: You are arguing KERI affords greater security than a decentralized linear event system like Bitcoin?
…you would be fundamentally arguing that you can record a singular, immutable linear event history more securely than Bitcoin, and I see nothing in KERI that would indicate that.
Read the answer to this first.
If you read Szabo's paper on threshold structures, you get security of the same type when ever you use a threshold structure, be it MFA, Multi-Sig, or Distributed consensus. They all are using a combination of multiple relatively weak attack surfaces that must be simultaneously compromised for a successful attack. So multiplying simultaneous weak surfaces = functional equivalent of a stronger attack surface. So when you look at KERI you see that the security is primarily due to cryptographic strength and the witnesses are not the primary source of security but merely secure one thing, that is the availability of the KEL for an identifier. Not the KEL itself. The KEL itself is secured by signatures.
From a Validator perspective their security is due to duplicity detection. Successful attack against duplicity detection requires an eclipse attack. Ledgers such as bitcoin are also susceptible to eclipse attacks. So in an apples to apples (resistance to eclipse attack) a KERI watcher network of comparable reach (1000's of watchers) would have comparable resistance to an eclipse attack.

***Q: Differences between blockchain-based security and KERI security

- Where KERI doesn't need total ordering in its logs, blockchain do need that. What KERI needs is watchers that construct string of event in the relative order of reception of the KEL {TBW please explain or improve this: what is this, why is it important?}
- Another characteristic is that KERI identifiers are transferable and blockchain-based identifiers are not, they are bound to their ledger.

***Q: How does FIFO prevent effective DOS attacks in Out-of-order KAACE?
An escrow cache of unverified out-of-order event provides an opportunity for malicious attackers to send forged event that may fill up the cache as a type of denial of service attack. For this reason escrow caches are typically FIFO (first-in-first-out) where older events are flushed to make room for newer events.
Paragraph 11.3.1 Question: how does FIFO prevent effective DOS attacks?
By loadbalancing the incoming messages. If you don't have any loadbalancing, the messages are going to be processed First In First Out. Only when an attacker has full bandwidth available to overload the buffer, they could frustrate the process to get honest messages in. As soon as you're able to balance the receipt of messages in the buffer, you'll be able to get the right messages (from honest senders) through.
(@henkvancann)

ION 101-401: What is ION (the Public, Permissionless DID Network), How Can You Use It Today, and What Comes Next

Tuesday 3A
Convener: Daniel Buchner (Microsoft)
Notes-taker(s): Jan Christoph Ebersbach

Tags for the session - technology discussed/ideas considered: Identifiers, DID, ion

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

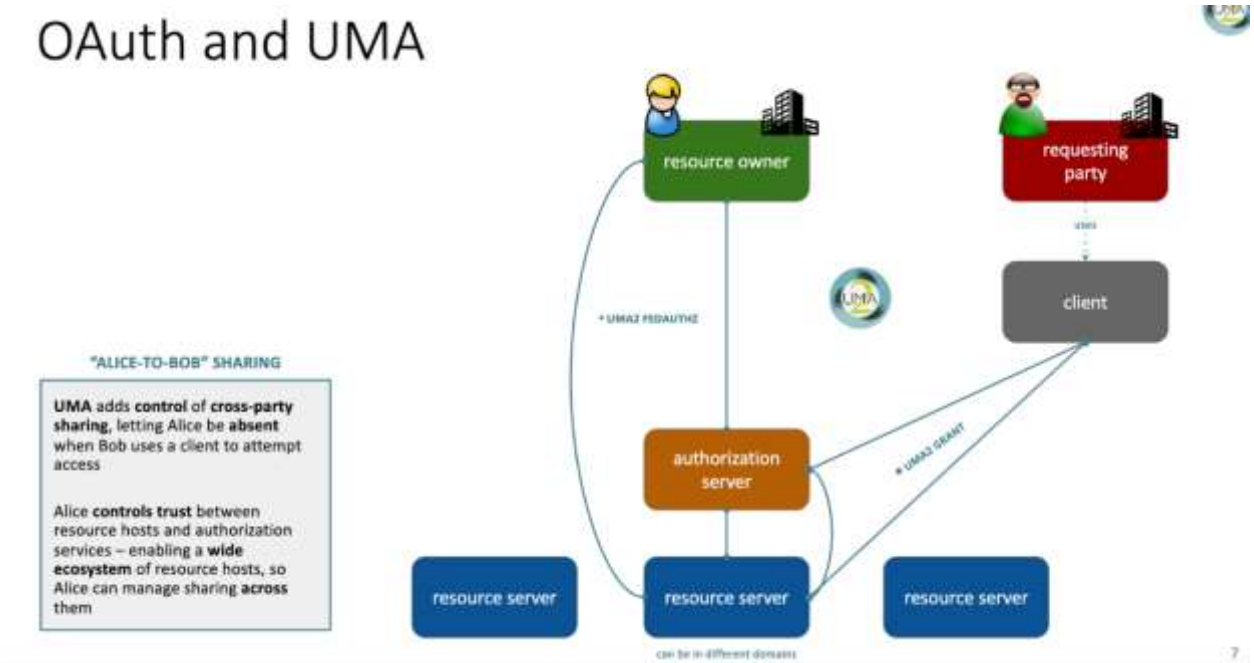
- Decentralization of did:ion if anchoring transactions are batched by an operator: it's possible to choose the operator or to incur the cost of anchoring the transactions. Furthermore, the operator doesn't gain access to the private key.
- ION delivers: massive scale, cost efficiency (despite running on the bitcoin network - best case if bitcoin a transaction costs 100 USD one action costs 1 cent), decentralized & flexible, decentralized registries
- ION has a type system so that DIDs can be used, e.g. for software packages, vehicles, … This makes it possible to make the centralized data repositories that we rely on today, npm registries etc., to be fully decentralized. This is a Sidetree feature that is currently only used by ION.
- DIF is currently working on personal data stores. Expected impact on private messaging, social media, gig services, ..
- ION is live and in production today
- Ion-tools is a selection of tools to interact with the ION network: https://github.com/decentralized-identity/ion-tools
- Resilience of ION: It's pointed out that not only Bitcoin needs to survive attacks but also the IPFS network as both are required for ION to work properly. With Bitcoin it looks unlikely that it's currently possible to reverse transactions on the network. However, with IPFS data can be unpinned and potentially disappear from the network.

101 Session: UMA - User Managed Access

Tuesday 3B
Convener: Eve Maler and George Fletcher
Notes-taker(s): George Fletcher

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

User-Managed Access (UMA) 101 George Fletcher, Kantara Initiative UMA Work Group



The UMA extension grant adds… docs.kantarainitiative.org/uma/wg/rec-oauth-uma-grant-2.0.html

- Party-to-party: Resource owner authorizes protected-resource access to clients used by requesting parties
- Asynchronous: Resource owner interactions are asynchronous with respect to the authorization grant
- Policies: Resource owner can configure an AS with rules (policy conditions) for the grant of access, vs. just authorize/deny

  •Such configurations are outside UMA's scope

Standard Interfaces for DID Create/Update/Deactivate

Tuesday 3C
Convener: Markus Sabadello
Notes-taker(s): Jovan Shandro

Tags for the session - technology discussed/ideas considered: DID, specification, DID operations

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

- There is an attempt to specify abstract interfaces if you want to Create/Update/Deactivate a did that could be implemented for all did methods.
- The idea of this specification is to provide a standard with the same assumptions as with resolution. It should be in an abstract level, meaning it should specify the inputs and outputs of creating/updating/deactivating a did but not how it should be implemented.
- There are many differences on how the operations of different did methods work, so it is still a question whether this standard will work for all did methods at the current state.
- Two greatest architectural questions that have come in the way:
  - How should key management be handled: where are keys created, how are they handled etc?
  - The concept of internal state or longer running jobs
- Regarding key management, in the current early draft there is a section which describes 3 possible way to handle key management:
  - **Internal secret mode**: The service itself generates keys and either stores them or returns them to the client. The disadvantage is that the service has to be highly trusted. This mode could make sense if you run the service yourself.
  - **External secret mode**: Key management is handled by some kind of externally hosted wallet that the service can call (e.g hardware wallet).
  - **Client-managed secret mode:** The client that makes use of the registrar service would first create the keys and then call the different functions of the service. This would mean back and forth communication between server and client (e.g server sends sign request, client signs etc.).
- Regarding the internal state concept, write operations could sometimes take some states to complete, so there could be an internal state machine keeping track of the states until the operation is complete e.g when you say you want to create a did, the *create* method might not directly return the did, but there might be multiple steps and a bit of back and forth communication between client and registrar and the client will need to take some more action.
- The next step would be to see if the current specification is generic enough (can it be applied to all did methods).
- Regarding future changes: It is sure that one such generic specification will be able to work for all did methods, the question is if it is too generic, then is it useful?

Links:

- https://peacekeeper.github.io/did-registration/
- https://dev.uniresolver.io/
- https://uniregistrar.io/
- https://w3c-ccg.github.io/did-resolution/
- https://w3c.github.io/did-rubric/
- https://github.com/decentralized-identity/universal-registrar
- https://godiddy.com/

Data Unions, Banks, Coops, Fiduciaries etc -- Has Their Time Come?

Tuesday 3D
Convener: Johannes Ernst
Notes-taker(s): Group

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

Historical analogies: rural electrification, telecommunications, insurance

Examples for where such data coops would be useful:

- Sharing of environmental monitoring data among farmers, e.g. in the California central valley
- Shared backup infrastructure for individuals / families
- Collective bargaining with data brokers etc

Different data unions may focus on different things, just like different credit unions might have different investment priorities

Would make it possible to "Bring the algorithm to the data, not the data to the algorithm". Compute at the edge.

Possible functions:

- Community with like-minded people, values
- Governance of data
- Hosting of tools
- Data vault
- Doesn't go away in the longer term as the coop wouldn't be as likely to be acquired, focus on more profitable products etc

Zoom Chat:
ben@bengo.co to Everyone (11:36) I used original opened on my first tumblr about… 16 years ago
ben@bengo.co to Everyone (11:45) * I'd want to know if my data needs to be unencrypted or encrypted to be a member (or what kind of member) https://www.storj.io/whitepaper
I signed up this week for social.coop!https://mastodon.social/
Me to Everyone (11:49) social.coop
ben@bengo.co to Everyone (11:50) My use case is I want to operate https://twitter.com/permanentcpu as a coop :) https://disco.coop/
@PrivacyCDN to Everyone (11:52) Did someone mention this
ben@bengo.co to Everyone (11:52) https://en.wikipedia.org/wiki/Rochdale_Principles
Coop defined there ^
ben@bengo.co to Everyone (11:56) Diff credit unions might give me different mortgage rates (in the most financialized example), which might be based on other constraints they commit to (like John is mentioning)
@PrivacyCDN to Everyone (11:58) Privacy preferences and consent are fraught when they involve a ceding of control to the 'data controller'
ben@bengo.co to Everyone (11:59) It's probably valuable enough for a 'data bank' to *ONLY* provide redundancy of encrypted data.

ben@bengo.co to Everyone (11:59) Then share opportunities with me to decrypt it (locally) and share back a subset that is really required for the opportunity to share (selective disclosure, even to the data bank governors) (Or ZKP things) 1770s
ben@bengo.co to Everyone (12:00) For those that joined late: “What would a data coop need to provide for you to be interested in joining?"
ben@bengo.co to Everyone (12:01) “The earliest mutual organization established in the British North American colonies was created in 1735 in Charleston, SC”
https://en.wikipedia.org/wiki/History_of_cooperatives_in_the_United_States#18th_century
ben@bengo.co to Everyone (12:02) “The Philadelphia Contributionship mutual insurance company, founded by Benjamin Franklin in 1752, is the oldest continuing mutual insurance company in the continental United States. “ “Bring the algorithm to my data” YES!
ben@bengo.co to Everyone (12:03) Coop says more about the governance (democracy + open membership) than the business model, IMO
@PrivacyCDN to Everyone (12:04) WWDES? What would Douglas Englebart Say?
ben@bengo.co to Everyone (12:06) +1
https://www.colorado.edu/lab/medlab/2020/08/31/exit-community-community-primer
@PrivacyCDN to Everyone (12:09) https://platform.coop
@PrivacyCDN to Everyone (12:09) A cooperative is defined as an autonomous association of persons united voluntarily to meet their common economic, social, and cultural needs and aspirations through a jointly-owned and democratically-controlled enterprise.
ben@bengo.co to Everyone (12:11) Good book of case studies on “Platform Cooperatives”
https://www.orbooks.com/catalog/ours-to-hack-and-to-own/
ben@bengo.co to Everyone (12:11) (Not a playbook :(, but good inspiration)
Working through this now: more of a playbook https://elements.disco.coop/
ben@bengo.co to Everyone (12:17) This is the ‘exit to community’ co starting up in SF.
https://www.understory.coop/ (On solidproject.org for now)
Dogfooding:
https://understory.garden/u/tani.myunderstory.com/default/pFcGoTnHLbR6vXHZdEVW89bZYgmJesMkyK
ben@bengo.co to Everyone (12:20) https://en.wikipedia.org/wiki/Regulatory_capture
In 5 years, will the cloud service your’e renting be the same price or functionality or still exist?
ben@bengo.co to Everyone (12:25)
https://community.webmonetization.org/valueflows/valueflows-software-for-distributed-cooperative-economic-activity-on-the-open-web-grant-report-1-3mjk
https://mothership.disco.coop/NextCloud
Run https://github.com/colab-coop/coopernetes
ben@bengo.co to Everyone (12:27) Then run https://github.com/solid/community-server
(Or next cloud + https://github.com/pdsinterop/solid-nextcloud)
@PrivacyCDN to Everyone (12:31) https://www.tru.net
ben@bengo.co to Everyone (12:31) New to me, thanks for sharing
@PrivacyCDN to Everyone (12:33) https://www.sitra.fi/en/topics/fair-data-economy/
@PrivacyCDN to Everyone (12:36)
https://d1muf25xaso8hp.cloudfront.net/https%3A%2F%2Fs3.amazonaws.com%2Fappforest_uf%2Ff1587410240363x746891124614691500%2Fmartech_2020_final-1600x900-web.jpg?w=1024&h=576&auto=compress&dpr=2&fit=max

Making The Intention Economy Happen

Tuesday 3E
Convener: Doc Searls (& Customer Commons)
Notes-taker(s): Doc Searls

Tags for the session - technology discussed/ideas considered:

#vrm #intentioneconomy #byway #intention #customercommons #cuco #ssi #SSEC

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

The session was prepared in haste to come ahead of Hadrian Zbarcea's demo in the demo hour, which would come up shortly.

Doc and Hadrian presented the Information Byway that Customer Commons is working on, and which was later detailed in this blog post. The slide deck used was a subset of the one used two days later in the final session in this series on the Byway. That one is here.

It became clear in this session that we would need more sessions on days two and three, which we held.

Revocation: Introduction and Overview - Goal Is To Connect

Tuesday 3G
Convener: Andreas Freitag
Notes-taker(s): Chat and edit from Andreas Freitag

Tags for the session - technology discussed/ideas considered: #revocation #privacy #standards

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

Link to presentation:
https://drive.google.com/file/d/1HBr2VinzbJxq8dOs4b398tOUbRXmhraE/view?usp=sharing

ZOOM CHAT (Edited and discussion sorted to headlines):

QUESTIONS addressing cryptographic accumulators with delta files
20:37:49 From Rouven Heck1 to Everyone : Ever holder needs to update the Witness file, even if their stuff is not updated, correct?

20:38:24 From Micha Kraus to Everyone : Yes, on each accumulator update
20:39:04 From Paul DIetrich to Everyone : Is that pushed to all credential holders or do they just go get it when they need to present next time?
20:40:52 From Christian Bormann to Everyone : afaik normally it's not pushed, wallets get it when they need to present a proof of non-revocation (could also be done with certain intervals)
Andreas F.: You can implement in different ways.
20:41:36 From Dominic Wörner to Everyone : In Indy, updates/deltas are on the ledger. Depends on the wallet implementation when they fetch the updates

20:48:36 From Jeremie Miller to Everyone : Short expiration is exactly how OAuth/OIDC work w/ access token (and refresh tokens to update them), I don't believe scalability is really an issue with this approach given its adoption.
20:48:51 From Michael Lodder to Everyone : but privacy is
20:48:56 From Paul DIetrich to Everyone : thanks. Which of these methods does CredentialStatusXXXX use?
20:49:43 From Brian Richter to Everyone : List based I believe Paul
20:52:22 From Rouven Heck1 to Everyone : I'm wondering what credentials have practical use-cases if they are not tight to an individual / entity
20:52:37 From Kristina Yasuda1 to Everyone : like coupons?
20:53:06 From Rouven Heck1 to Everyone : ok, in this use-cases - what are the privacy concerns?
20:53:36 From Stephen Curran to Everyone : Proving age?
20:54:28 From Rouven Heck1 to Everyone : Proving age in which use-case? Entering a bar - needs your photo. Ordering something online - requires your address, etc.
20:54:49 From Rouven Heck1 to Everyone : if it's just an age proof without anyting - wouldn't this be something whcih can be shared easily?
One ring to rule them all, one ring to don't find them?
Andreas: I wish for a privacy preserving, scalable solution and the SSI community should agree on one (but not unlimited number) revocation method

20:56:00 From Rouven Heck1 to Everyone : @Andreas - why is your wishlist including that it's only one revocation list? Don't you think that it would be useful to use different methods depending on use-cases?
Andreas: Multiple methods would cause a lot of implementing effort for an agent which want to be interoperable. A second challenge is to keep privacy level high.
With a limited and agreed implementations privacy-by-design can be ensured.

20:59:15 From Paul DIetrich to Everyone : As far as I can tell the SSI community hasn't select one method for anything yet. I hope this changes the game.
20:59:51 From Kristina Yasuda1 to Everyone : ^ so true

21:00:32 From Rouven Heck1 to Everyone : I would argue it's not a desirable outcome
21:00:38 From Rouven Heck1 to Everyone : (at least not yet)

21:05:31 From Jeremie Miller to Everyone : +1 privacy by design!
21:05:32 From Karim Stekelenburg to Everyone : +9000!
21:06:19 From Michael Lodder to Everyone : +++

21:07:52 From Paul DIetrich to Everyone : How many credential revocations standards exist today?
Andreas: It is realized with lists/hidden list. The only implementation with cryptographic accumulators I know is the indy implementation.

21:19:19 From Rouven Heck1 to Everyone : @Andreas - what are we doing if the new approach with the Silverbullet will not work? :)
21:30:32 From Andreas Freitag to Everyone : @Rouven search a new one

“Standards”
21:09:25 From Paul DIetrich to Everyone : these are drafts right now? or have they been standardized.
Andreas: Yes, no standards at the moment.
21:10:36 From Kristina Yasuda1 to Everyone : no real standardization for 1 and 3, for 2, this is the one: https://w3c-ccg.github.io/vc-status-rl-2020/
21:11:03 From Kristina Yasuda1 to Everyone : I meant no real standardization *needed* for 1 and 3
21:11:59 From Paul DIetrich to Everyone : I get that for 3, but for #1 there has to be some kind of API?
21:12:29 From Michael Lodder to Everyone : how many ways are there to check for revocation with x509 certificates

Driving licence use case
21:02:26 From Michael Shea to Everyone : how many driver’s licenses are there in Austria?
Andreas: we have about 4Mio in Austria. For our testing we decide to have a setup with 10Mio items.
21:02:40 From Michael Lodder to Everyone : we started with w
21:02:49 From Michael Lodder to Everyone : revoke 600/day, add 1K/day

Almost every use-case / customer needs revocation
21:06:39 From Kristina Yasuda1 to Everyone : maybe you realize you gave an entrance pass to a criminal and want to revoke it within an hour...

Miscellaneous
21:08:49 From Kristina Yasuda1 to Everyone : one is Issuer call-home - you put that endpoint in the credential; Credential revocation list 2021 in W3C CCG; and no revocation needed
21:10:06 From Michael Shea to Everyone : IoT is very broad, if the IoT is a Medical device the requirements are very different
21:11:55 From Karim Stekelenburg to Everyone : Will BBS+ revocation lower the performance issues for JSON-LD once it’s there?

PRIVACY & Revocation by API
21:12:36 From Kristina Yasuda1 to Everyone : Issuer offers an API, and you put a link to that API inside the credential which verifier hits?
21:13:06 From Paul DIetrich to Everyone : But what do I get when I call it? Does 200 mean its OK?
21:13:07 From Michael Lodder to Everyone : @Kristina then you get correlation and disclosure
21:13:21 From Michael Lodder to Everyone : you get tracked by the issuer and every verifier
21:13:30 From Michael Lodder to Everyone : you don’t want the protocol to betray you
Andreas: It has disadvantages in privacy
21:13:34 From Michael Shea to Everyone : +1 Andreas
21:13:39 From Jeremie Miller to Everyone : +1 Andreas!
21:13:40 From Michael Lodder to Everyone : we have enough of those already
21:13:46 From Kristina Yasuda1 to Everyone : pairwise DIDs can prevent RP correlation, but yeah IdP correlation is there
21:13:53 From Stephen Curran to Everyone : +1 Andreas
21:13:57 From Rouven Heck1 to Everyone : It depends on who your customers are … ;)
21:14:14 From Michael Lodder to Everyone : DIDs don’t get you correlation, credential presentation could without ZKPs

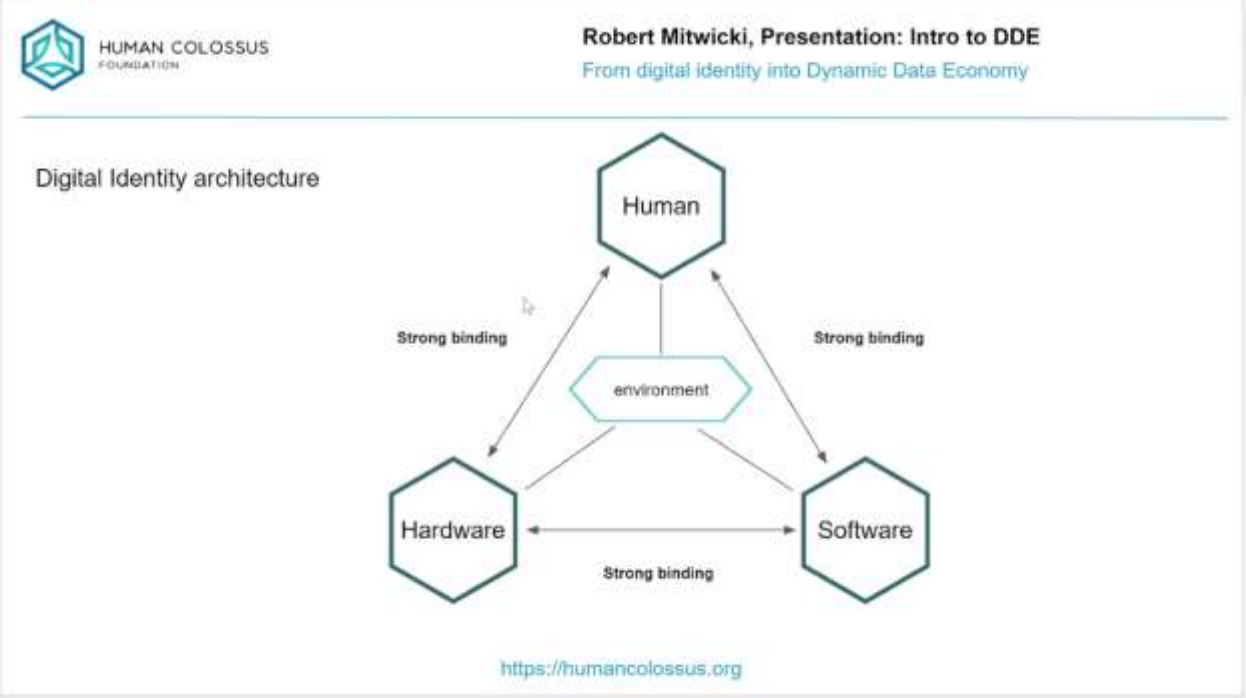
21:14:25 From Rouven Heck1 to Everyone : governments and big corporate might have other requirements than peer to peer use-cases
21:14:32 From Kristina Yasuda1 to Everyone : I am listing options and +1 to Rouven, some issuers ask for the call home...
21:15:08 From Kristina Yasuda1 to Everyone : if you have a different DID in each credential of the same content issued per RP, that prevents correlation
21:15:37 From Michael Lodder to Everyone : its only prevented if its never disclosed
21:15:46 From Michael Lodder to Everyone : if the DID is revealed, its correlatable
21:16:01 From Michael Lodder to Everyone : especially since its a unique number

Biometric and Digital Identity

Tuesday 3H
Convener: Robert Mitwicki / Adrian Gropper
Notes-taker(s):

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

Background document from session 1A http://bit.ly/biometricVC



Identity and the environment
Environment as certificate authority / identity restoration / deduplication
Naked at the airport

- http://bit.ly/biometricVC
- Trust chain

Biometric

- Non-repudiation
    - Local
- Deduplication
- Identification
    - Human
    - Machine

Ambient Surveillance

U.S. Department of Education & Universal Wallet: Bring Your Wallet!

Tuesday 3I
Convener: Kim Duffy
Notes-taker(s): Niels van Dijk

Tags for the session - technology discussed/ideas considered: Wallets, Education

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

Slides presented:
https://docs.google.com/presentation/d/1j5QQCbXg-hoPPSZW45UBWG9ByOxHjcNLIUAKgOBcKGM/edit#slide=id.gd34895ce5b_0_43

Reviewed the US Dept of Education's Student Wallet project, which MIT recently began work on.
The goals of the talk included:

- Presentation of high-level view of work so far
- Discuss/ Get feedback on approach
- Discuss next steps and how to collaborate

The work done so far focused on the student wallet draft standard. 4 relevant sections were discussed:

- Wallet Functional Requirements
- Interaction Flows and Procedures
- Wallet Design
- 3Vs - Verification, Validation, and Veracity

A Q&A followed, touching on:

- UI/UX - mostly out of scope of this effort, but eager to participate in follow up effort
- Method for evaluation of DID methods and other technical selections

People are encouraged to participate in the following ways:

- Universal Wallet: https://w3c-ccg.github.io/universal-wallet-interop-spec/
- Review/contribute to the draft spec:
  https://docs.google.com/document/d/1vPqb4bJ6pfuAPYF_fMW_Lb-7GZugasWKfrSCotpuv6o/
- Verifiable Credentials for Education Task Force: https://w3c-ccg.github.io/vc-ed/

KERI Q&A Basic Introduction

Tuesday 3K
Convener: Henk van Cann
Notes-taker(s): ? feel free !

Tags for the session - technology discussed/ideas considered:

KERI, basic introduction, Self Certifying Identifiers, pre-rotation, ledgerless,

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

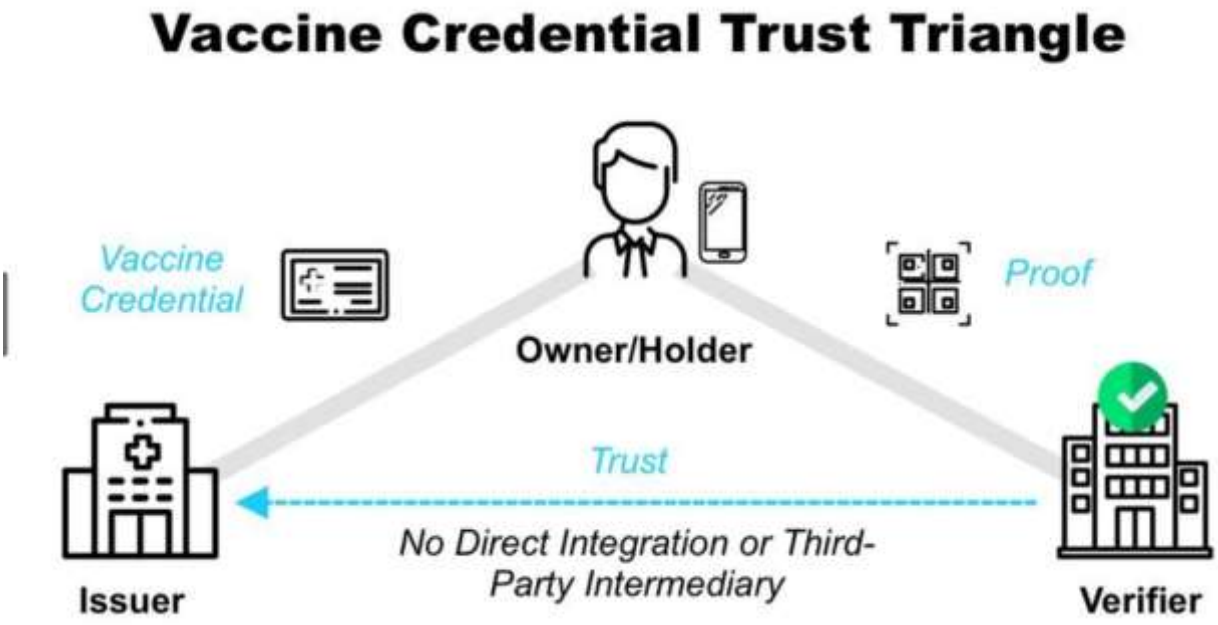
This the link to the 20 minute introductory presentation in pdf:
https://blockchainbird.org/downloads/KERI-QA-introduction.pdf

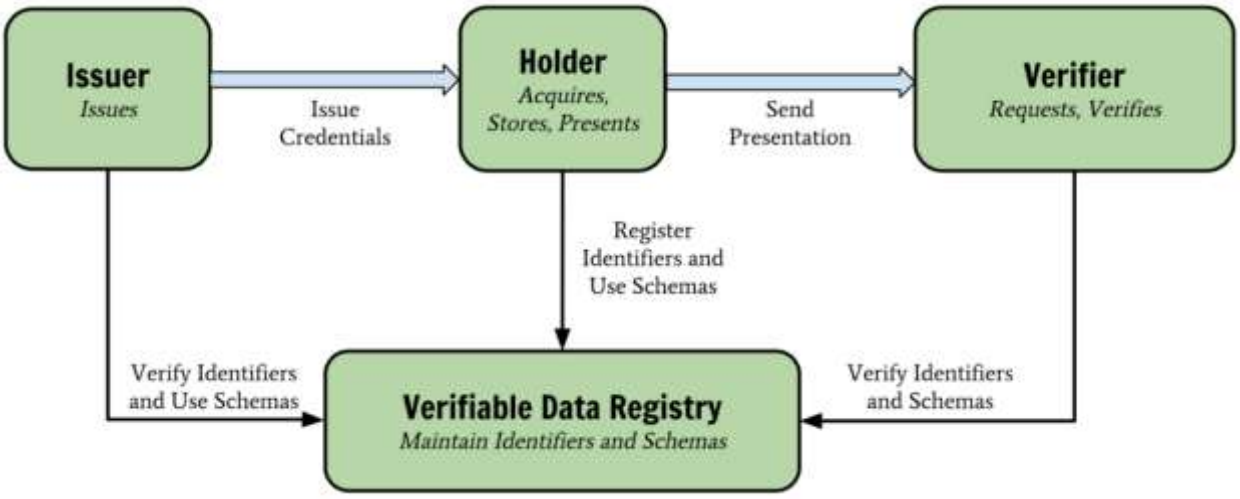
It has lots of relevant links in it to start your journey in KERI.
With my notes:
https://blockchainbird.org/downloads/KERI-QA-introduction_notes.pdf

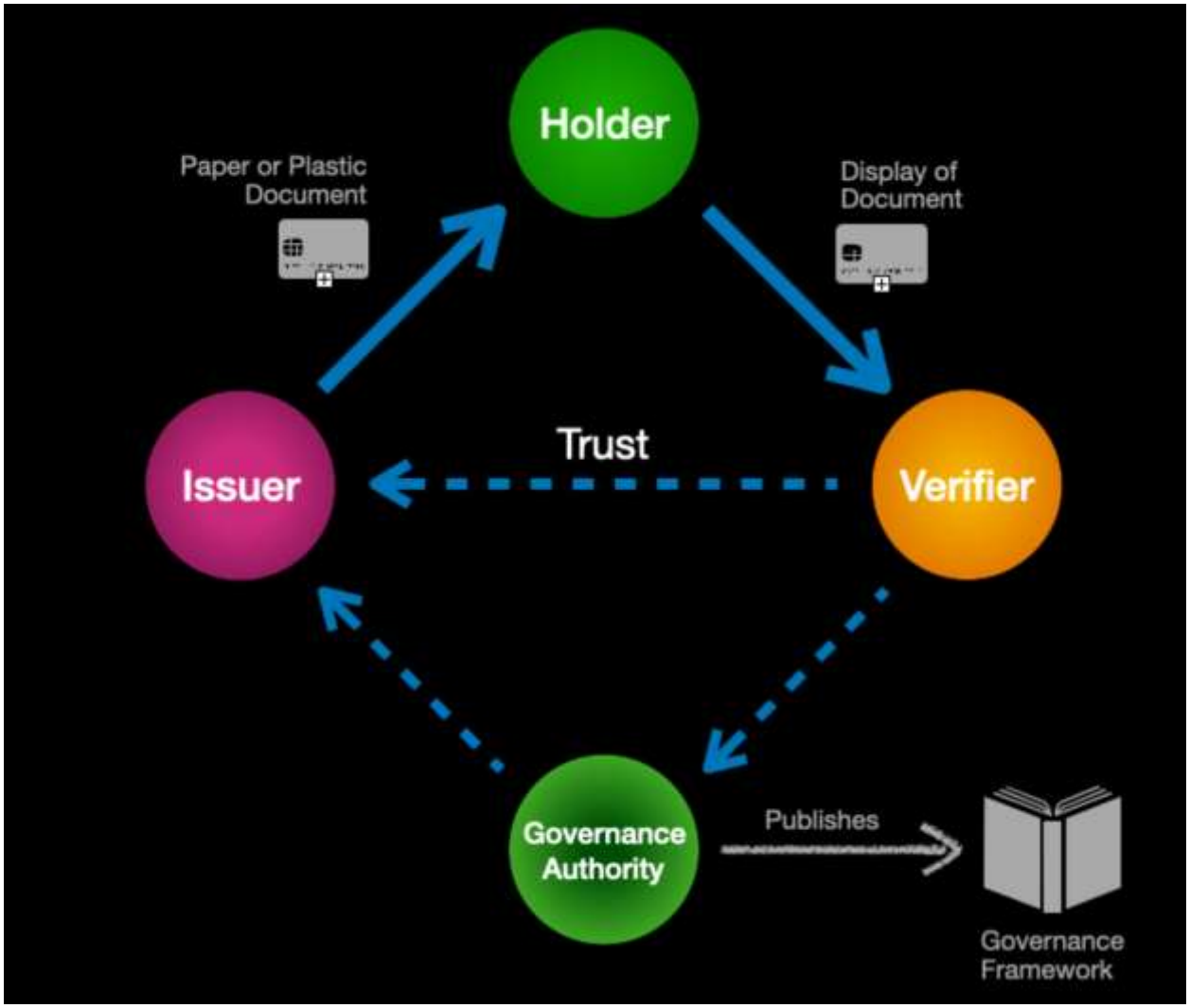
Is the Verifiable Credential Trust Triangle Incomplete?

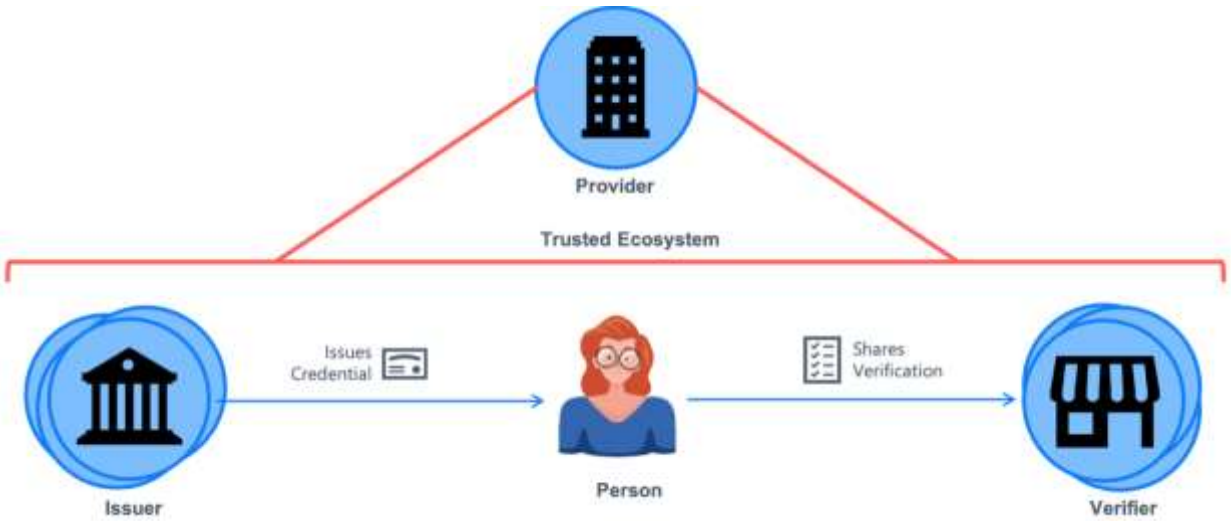
Tuesday 3M
Convener: Riley Hughes
Notes-taker(s): Riley Hughes

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:









Fundamental problem:

- Why should a verifier trust a credential?

VC marketplace project at DIF is talking about a reputation system for issuers, using VCs

We need to agree on:

- Machine-readable document (governance framework)
- URI for a governance framework that we need to agree on

Sterre's organization (TNO) is developing a software implementation called a "credential catalogue" which is like the yellow pages for verifiable credentials

- With yellow pages, who publishes it, and will everyone trust it? That brings us full-circle to the first issue

Yellow pages also might work in a given geo or ecosystem, but might not work in a global/international context

- Perhaps there are multiple yellow pages systems
- Somehow these need

Drummond shared work at the Good Health Pass is tackling this

- Trust registries
- Rules engines
- Governance frameworks

Original question is: how does the verifier know who to trust? Then how do they know which governance framework to trust? Then who governs that list? And how do you trust that? It always comes full-circle

Scott shared the screen of Trinsic Ecosystems

One of the final points I saw in the Zoom chat window was a suggestion that a good next step would be to wordsmith the problem statement.

Keep discussion going:

1. Riley Hughes (riley@trinsic.id)
2. Sam Curren
3. Steve Venema (Steve.Venema@forgerock.com)
4. Dan Robertson (dan@productintuition.com)
5. Eric Weber (eric.weber@digital.etat.lu)
6. Sterre den Breeijen (sterre.denbreeijen@tno.nl)
7. Stepan Gershuni (gershuni.stepan@gmail.com)
8. Katrie Lowe (katrie@domilabs.io)
9. Pavel Metelitsyn (pavel@domilabs.io)
10. Lohan Spies (lohan.spies@didx.co.za)
11. Jo Spencer (jo.spencer@460degrees.com)
12. Jace Hensley (jace@bloom.co)
13. Frederico Schardong (frede.sch@gmail.com)

Andrea Reginato (info@dede.is)

Overlays Capture Architecture (OCA): A global solution for data capture and semantic harmonization

Tuesday 4A
Convener: Paul Knowles
Notes-taker(s): Neil Thomson

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

The form of the session was a presentation (intended for those new to the subject), followed by Q/A and discussion

Presentation: Overlay Capture Architecture

Some additional notes on the presentation slides

A "Form" :

> can be both a capture tool and a way of presenting data that maps to and from multiple documents (or tables) in a base schema.

Data collection format and structure may be very different from the (base schema) structure in a OCA model.

> A base schema design consideration is to ensure that the structure is compatible with all types of data usage. This can include data captured and structured to support (real time) transactions, operational behavior, historical analysis, prediction and machine learning. That does not mean that the OCA structure itself can support all these data uses. But that it contains all the information to construct (by transformation) structures optimized for those uses. How to do that is beyond the scope of OCA.

OCA differs from JSON-LD

> JSON-LD is used as the core technology/language to define the structure of the schemas and the backbone of the layered approach. JSON-LD is a highly expressive way of defining semantically rich metadata and structures, beyond what traditional relational database metadata and modelling supports.

Q/A & Discussion

> How can you deliver an OCA based schema (say, for a VC being exchanged by a Holder with a Border Guard) in a different language?
>
> A
>
> > The OCA is a model for capturing and exchanging data in a way that addresses semantic, structure, data type and localization (language/format) issues. That doesn't mean you should implement the OCA model within a wallet to provide multilingual support.

An OCA model can be used as the source to "compile" different dynamic overlays to be applied (say, as a language look-up in a relational model) so the border guard can read the labels, attribute names and values of a VC in their preferred language.

The key there is to have a machine readable key for labels and data that must be internationalized. This is not new.

Would this not get large (for a smartphone)?

A

Not if you compile the localization overlays to only what is needed to run on a smartphone vs required for transformation modelling.

The "presentation" of most VCs from a Holder's wallt to a Verifier is mostly about confirming the identity of the Holder to the Verifier and determining if the VC is valid (valid vaccination: yes/no) say a screen or two on a smartphone (vs. the 640 pieces of data collected in a vaccination or health test record)

So there is relatively little data for each "as used on a smartphone" localization layer.

A Credential in many ways is a simple proof of status vs a collection of all the data supporting that status. It's message is very much of asserting "the chain of trust verifies <this claim>" which is mostly a yes/no answer.

How can you trust (data and overlays) from an OCA model?

<Notetaker - incomplete - more notes to come>

101 Session: Self Sovereign & Decentralized Identity

Tuesday 4B
Convener: Karyl Fowler & Juan Caballero
Notes-taker(s): Karyl Fowler & Juan Caballero

Tags for the session - technology discussed/ideas considered:

https://www.uschamberfoundation.org/sites/default/files/media-uploads/Applying%20SSI%20Principles%20to%20ILRs%20Report.pdf

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

Links:

- **Video from last IIW**

- **Slides from this session Karyl Fowler (Transmute) and Juan Caballero (DIF) present Intro to SSI at #IIW31, Oct 2020**

ZOOM CHAT – not edited by session conveners

From Peter Mackinnon to Everyone: (3:01 PM) caffeinated really informative, I'm brand new to all this. Both @ juan
From Matt Domsch - SailPoint to Everyone: (3:02 PM) Learning for work @ SailPoint
From Erica Connell to Everyone: (3:02 PM) personal
From Antony Wang to Everyone: (3:02 PM) personal
From Mihai Chiorean to Everyone: (3:02 PM) Personal interest but might be able to use it professionally
From Benjarat to Everyone: (3:25 PM) Can we record this session pls?
From Juan Caballero (DIF/Spruce) to Everyone: (3:25 PM) oh shucks
From Andrea Reginato to Everyone: (3:25 PM) Yes, it would be helpful
From Juan Caballero (DIF/Spruce) to Everyone: (3:26 PM) we recorded it last time. let's record Q&A
From Radu Popovici to Everyone: (3:27 PM) Can we have the slides?
From Juan Caballero (DIF/Spruce) to Everyone: (3:27 PM) one sec i'll get you both links More on data portability later :D Rebase CG starts up soon, a project I'm involved with on that front slides and video from last time in the notes, btw
From Juan Caballero (DIF/Spruce) to Everyone: (3:32 PM)
https://docs.google.com/document/d/1L74mjPN-ydwoyH-zQaLB1eZ2q6Pb24Vgt-ObrH3Gxzc/edit can't figure out how to claim host tho for cloud-recording :/ selective disclosure is an architecture/UX primitive; ZKP is a kind of math
From Kimberly Duffy to Everyone: (3:36 PM) Is doge listed there yet?
From Juan Caballero (DIF/Spruce) to Everyone: (3:36 PM) https://github.com/spruceid/did-doge
From Juan Caballero (DIF/Spruce) to Everyone: (3:36 PM) errr https://spruceid.github.io/did-doge/index.html
From Kimberly Duffy to Everyone: (3:36 PM) Thanks, which use cases does did:doge solve? :)
From Juan Caballero (DIF/Spruce) to Everyone: (3:37 PM) rude
From Kimberly Duffy to Everyone: (3:37 PM)Sorry
From Kaan Uzdogan to Everyone: (3:38 PM)What could be an example for a different did methods on same blockchain network, or why there might be a need for that
From Kimberly Duffy to Everyone: (3:39 PM) Kaan - there are at least 2 diff BTC-based methods
From Andrea Reginato to Everyone: (3:39 PM) Could we have a link about the project working on VC and education?
From Juan Caballero (DIF/Spruce) to Everyone: (3:39 PM)
https://w3c-ccg.github.io/vc-ed/ Kaan - Doge is a BTC fork too, so might count as a BTC-based method if you squint a little and Kim - DOGE knows no "use value", it descends from the labor theory of value
From Kimberly Duffy to Everyone: (3:40 PM)Kaan - As for why, one addresses scaling better than the other. But it requires 2nd layer solutions and some might view it as less “self-sovereign" YESid:doge solves the meme problem
From Juan Caballero (DIF/Spruce) to Everyone: (3:41 PM)
until DID:Doge, memes didn't scale
From Kimberly Duffy to Everyone: (3:41 PM) correct
From Kimberly Duffy to Everyone: (3:41 PM) But there is also a did:mem Did:meme
From Juan Caballero (DIF/Spruce) to Everyone: (3:42 PM)
did:mlem will serve the little-known finnish mlem community that forked dogecoin in 2018
From Kimberly Duffy to Everyone: (3:43 PM)
Things get less fun as you go to the right :(

From Kimberly Duffy to Everyone: (3:49 PM) W3C CCG is a good way to get an intro; it's free and open to the public: https://w3c-ccg.github.io/
From Kimberly Duffy to Everyone: (3:49 PM)
There is a CCG 101 work item that's trying to make all of these more accessible. Joining that is a great way to get up to speed and contribute to a CCG work item at the same time If you are interested in education, check out https://w3c-ccg.github.io/vc-ed/
From Juan Caballero (DIF/Spruce) to Everyone: (3:54 PM)
https://docs.google.com/document/d/1L74mjPN-ydwoyH-zQaLB1eZ2q6Pb24Vgt-ObrH3Gxzc/edit
From Kimberly Duffy to Everyone: (3:54 PM) Great job Karyl and Juan!
From Sandeep Bajjuri to Everyone: (3:55 PM) Thank you Karyl and Juan 😊
From Quang Tu LE to Everyone: (3:56 PM) Thanks for the talk!
From Me to Everyone: (3:56 PM) <3 thanks Kim! And thanks Sandeep!
From Me to Everyone: (3:56 PM) thanks for attending all!
From Erica Connell to Everyone: (3:56 PM) Thank you, Karyl and Juan. I appreciate your presentation!
From Kimberly Duffy to Everyone: (3:56 PM) Juan I can hem and haw around this
From Me to Everyone: (3:57 PM) The Kim speaking is one of the two Kim's we referenced a few times in our presentation :) Very cool to have her at the intro sash!
From Simin Ghesmati to Everyone: (3:58 PM)Could you please go over privacy issues that may arise using the technology?
From Juan Caballero (DIF/Spruce) to Everyone: (3:58 PM) absolutely ack they traded in the leafblower for a weed whacker
From Kimberly Duffy to Everyone: (4:01 PM) I might have a couple of things
From Juan Caballero (DIF/Spruce) to Everyone: (4:02 PM)
https://www.amazon.com/Domains-Identity-Understanding-Contemporary-Collection/dp/1785274910
From Me to Everyone: (4:04 PM) add literature links to the session notes if you've got any!
From Juan Caballero (DIF/Spruce) to Everyone: (4:04 PM)
https://en.wikipedia.org/wiki/Contextual_Integrity
From Kimberly Duffy to Everyone: (4:05 PM)
https://www.uschamberfoundation.org/sites/default/files/media-uploads/Applying%20SSI%20Principles%20to%20ILRs%20Report.pdf
From Marius Scurtescu to Everyone: (4:05 PM) getting 404 for above
From Ian Culp to Everyone: (4:06 PM) worked for me
From Kimberly Duffy to Everyone: (4:06 PM) What's the link to the session notes?
From Juan Caballero (DIF/Spruce) to Everyone: (4:06 PM)
https://docs.google.com/document/d/1L74mjPN-ydwoyH-zQaLB1eZ2q6Pb24Vgt-ObrH3Gxzc/edit
From dsearls to Everyone: (4:10 PM) We worked out privacy in the physical world thousands of years ago, which started with the technologies called clothing and shelter. The connected digital world is still new: decades old at the most. .This world also came without privacy tech, which we have still barely invented.
From Juan Caballero (DIF/Spruce) to Everyone: (4:11 PM) "forward privacy"
From dsearls to Everyone: (4:11 PM) Meanwhile we have, in the absence of personal privacy tech, had massive amounts of privacy-violating tech deployed, which we have addressed mostly with regulation. Which amounts at most telling those incentivized to spy on naked people to stop doing that. Which they haven't.
From Andrea Reginato to Everyone: (4:13 PM) I've a question: how can I trust an issuer? Or better, why should a verifier trust a credential? I'm working in a project where we want to generate VC that are connected to impact. One way (the one we see today) is to pass through an auditor and get a certification. We are working on a community based approach where different stakeholders (community members, investors, trusted parties, travellers, AI), but we are new to this. Any direction for "issuer trust" topic?

From Kimberly Duffy to Everyone: (4:15 PM) @Andrea — right, there are many layers of deciding whether to accept a credential. We are currently dividing it into the 3 V: https://github.com/w3c-ccg/vc-http-api/blob/main/docs/verification.md Oh that's scary — Daniel?
From dsearls to Everyone: (4:15 PM) Look up https://www.google.com/search?q=gdpr+compliance and you'll get >200 million results, nearly all of which are about obeying the letter of the law while screwing its spirit to the wall.
From Simin Ghesmati to Everyone: (4:15 PM) Perfect, thanks
From dsearls to Everyone: (4:16 PM) ProjectVRM and Customer Commons, which started here, have a privacy manifesto on a wiki: https://cyber.harvard.edu/projectvrm/Privacy_Manifesto
From Riley Hughes to Everyone: (4:17 PM) In fact I just held an entire session on this question 😂
From Juan Caballero (DIF/Spruce) to Everyone: (4:17 PM) There is also a conversation/thought experiment around Andreas's question happening in the ESSIF-LAB program in Europe: https://gataca-io.github.io/verifier-apis/
From Juan Caballero (DIF/Spruce) to Everyone: (4:17 PM) Oh! And get the recording of Riley's session!Highly decentralized allow lists :D
From Andrea Reginato to Everyone: (4:22 PM) Thanks a lot (can't speak as people are sleeping)
From Michael Black1 to Everyone: (4:22 PM) Thank you!
From Peter Mackinnon to Everyone: (4:22 PM) thanks!
From Simin Ghesmati to Everyone: (4:22 PM) Really useful and nice presentation. thanks all.
From Ian Culp to Everyone: (4:22 PM thanks for the knowledge!
From Kimberly Duffy to Everyone: (4:22 PM) Thanks!!

Introduction to Picos

Tuesday 4C
Convener: Phil Windley
Notes-taker(s):

Tags for the session - technology discussed/ideas considered:

IoT, digital twins, device shadows, Conflict-free replicated data type (CRDT), CSP over DIDcomm

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

Pico is short for "Persistent Compute Objects."

Why Picos

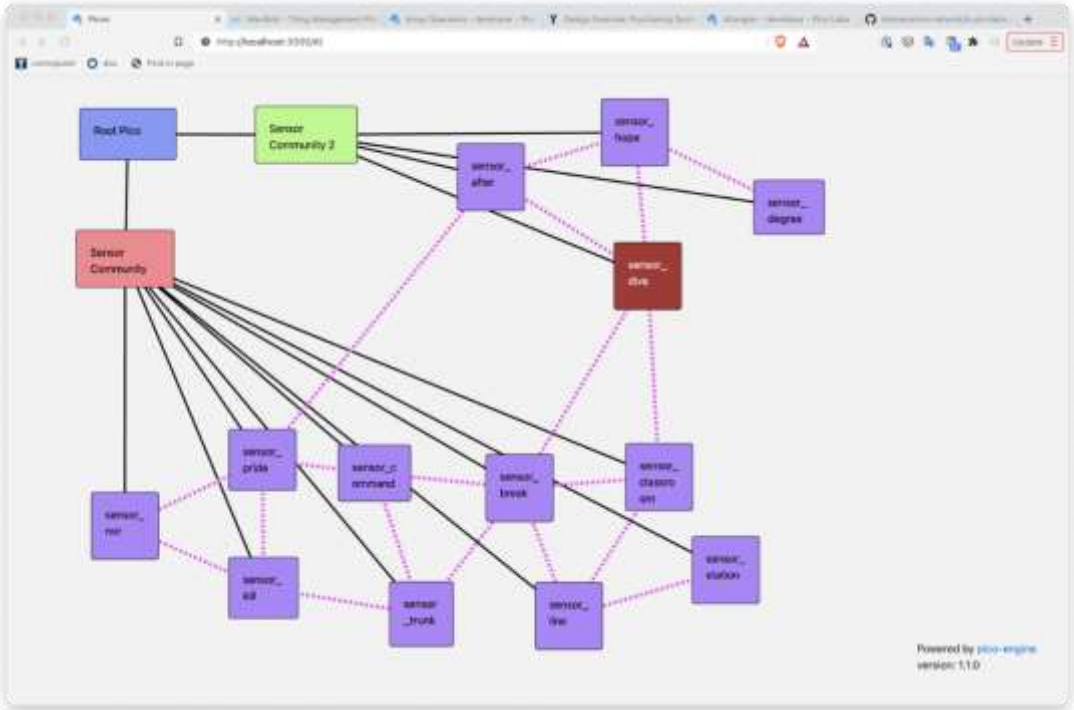
- Persistent, personal, computational nodes → More individual autonomy
    - Computational node for anything: person, place, organization, smart thing, dumb thing, concept, even a pothole
- Better, more scalable model for IoT → trillion node networks
    - Picos support social things and trustworthy spaces

    - Better sharing, more natural relationship-based interactions (borrow my truck, Fuse with two owners)
    - Scales
- Substitutable hosting model → freedom of choice
    - pico mesh
- Build the Intention Byway
    - (picos =? intentrons)
- Use the self-sovereign internet
    - DIDComm-based channels
- A better IoT

What are Picos?

- "Pico" is a neologism for persistent compute objects.
- Persistence is a core feature of how picos work.
- Picos exhibit persistence in three ways:
    - Persistent identity—Picos exist, with a single identity, continuously from the moment of their creation until they are destroyed.
    - Persistent state—Picos have state that programs running in the pico can see and alter.
    - Persistent availability—Picos are always on and ready to process queries and events.

Pico Engine 1.0 released in January



Links:
https://picolabs.io Pico Labs
https://github.com/Picolab/ repos
https://picolabs.atlassian.net/wiki documentation
http://stackoverflow.com/questions/tagged/krl programming Q&A

Posts: Announcing Pico Engine 1.0

Managing Authorization: Who Has What Access?

Tuesday 4D
Convener: David Schmudde
Notes-taker(s): David Schmudde

Tags for the session - technology discussed/ideas considered: #UX
Focused on communicating risks/harms to the user. Focus on the high-level user experience.

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

- Steve Venema suggested the Privacy Co-op
- Make an individual's policy decisions disappear into their workflow. Whenever the application needed a resource, we knew the answer from the action they took in the UX.
- Trust based on the context of the other people I know.
    - **Web of trust**: have my friends shopped here?
    - **Reputation**: what is the ranking of this place?
- Revocation
    - Information is given, cannot be revoked (photo of a driver's license)
    - Permission is given, can be revoked (allow a 3rd party to say I have a driver's license)
- Trust based on browsing history
    - TOFU: Trust based On First Use - trusted it once, will trust it again
    - Kantara Initiative: agreed to terms once. Will stay agreed unless they change.
- The opposite of "who do you trust?" is "how are you making yourself vulnerable?"
- Kantara Initiative
    - obligations/consequences for violating the consequences
    - "identity trust workgroup" - Adopt the Personal Data Categories from Enterprise Privacy for the Consent Receipt V 1.1

- Consent for each purpose. People give consent at the purpose-level.

An Introduction to The Authentic Data Economy

Tuesday 4E
Convener: David Huseby
Notes-taker(s): Dave Huseby

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

This was a session to discuss the topics I brought up in my article on the authentic data economy: https://dwhuseby.medium.com/the-authentic-data-economy-9802da67e1fa

I talked about how the break from the W3C DID specs and other key innovations in cryptography have enabled me and Mike Lodder to design a solution for identity and all data provenance that is 1. privacy preserving, 2. scalable to global scale and how that creates an opportunity for authentic data to become the primary way data is used in the world.

Guardianship Showcase - The Sovrin Working Group Tech Requirements and Implementation Guidelines

Tuesday 4G
Conveners: John Phillips & Jo Spencer
Notes-taker(s): John Phillips & Jo Spencer (others welcome!)

Tags for the session - technology discussed/ideas considered:

Guardianship
Solve guardianship using verifiable credentials
Guardianship and impersonation are different things!

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

Presentation link: https://docs.google.com/presentation/d/1aGTPmlno3WScpSYMs1HLhWsrVRx9B-I0yhOQsRgmqRw/edit?usp=sharing

Sovrin is looking to promote the governance process and where guardianship fits in. The IdRamp wallet is an example of how the wallet could provide helpful features.

Philippe Page (The Human Colossus) - We are turning a “birth attestation” into a VC is a particularly complex problem. The allocation of a DID to the delegate is going to be a problem as it is “too dangerous”. We need to understand the social scenario and then apply the technical solution.

ESSIF-lab healthcare scenarios. KERI is key - we can't rely on the human context, we have to rely on the cryptography

Philippe - Consent is another concept that should be considered as a "building block" - lots of interest in this topic from the group…

ZOOM CHAT:

06:02:39 From John Phillips to Everyone : https://docs.google.com/document/d/1DnyG5hhZeM3Nwkm0yQJs2Bjj-dTjtjPcybbyEa3XSoM/edit
06:04:06 From Sterre den Breeijen to Everyone : 232323
06:07:22 From Jan Lindquist to Everyone : are the slides available on the internet?
06:07:55 From Jo Spencer to Everyone : link is in the meeting minutes... https://docs.google.com/presentation/d/1aGTPmlno3WScpSYMs1HLhWsrVRx9B-I0yhOQsRgmqRw/edit?usp=sharing
06:09:11 From Jo Spencer to Everyone : Whitepaper is here.. https://sovrin.org/wp-content/uploads/Guardianship-Whitepaper2.pdf
06:09:32 From Sterre den Breeijen to Everyone : (spoiler alert: this whitepaper is in the process of being updated)
06:09:54 From Jo Spencer to Everyone : Good point...
06:10:32 From Jo Spencer to Everyone : We're looking for people to join the team in doing the update
06:11:23 From Ken to Everyone : Deputy vs Confused Deputy
06:13:21 From Jan Lindquist to Everyone : maybe jumping ahead but is the direction in Sovrin based on Aries rfc 103 and if yes is there an open source component to demonstrate it
06:14:14 From Jo Spencer to Everyone : Useful Jan - have you looked at this in detail?
06:14:58 From Sterre den Breeijen to Everyone : Jurisdiction is meant as a concept: a company can also be a Jurisdiction
06:16:28 From Jo Spencer to Everyone : Sure thing... a Bank can issue a VC that they (and others) use because otherwise they keep forgetting that this exists....
06:18:53 From skyberg to Everyone : I think you hit on an important differentiator, John. Guardianship is NOT impersonation.
06:19:33 From Jo Spencer to Everyone : The terms used are Transparent (good) and Opaque (bad)
06:19:45 From Sterre den Breeijen to Everyone : the eSSIF-Lab: https://essif-lab.eu/
06:25:44 From skyberg to Everyone : Sorry for joining late. Is there a link to the docs?
06:26:03 From Hira Siddiqui to Everyone : https://sovrin.org/wp-content/uploads/Guardianship-Whitepaper2.pdf
06:26:13 From skyberg to Everyone : Thank you!
06:26:41 From Jo Spencer to Everyone : We're just in the process of publishing these... Sovrin will be doing the process..
06:27:51 From Jo Spencer to Everyone : The whitepaper needs updating. Please join the group if you're keen to be involved.
06:28:20 From Jo Spencer to Everyone : The Tech Requirements and Implementation Guidelines are just about to be published..
06:29:00 From skyberg to Everyone : "privacy by opacity". Is that like "security by obfuscation"? :)
06:29:16 From Jo Spencer to Everyone : Nice!
06:32:05 From skyberg to Everyone : Extreme noob question: Guardianship feels like an "entitlement" credential. Are there any similar Decentralized ID around entitlements?
06:33:22 From Jo Spencer to Everyone : They are certainly contextual. The Verifier decides what the Guardian is allowed to do and when... I would say that all VCs are entitlements
06:33:52 From Sterre den Breeijen to Everyone : *issuer, the verifier decides whether to accept this VC

06:39:21 From Ken Adler | ThoughtWorks | San Francisco | He/Him to Everyone : “Relationship Credentials”
06:41:59 From Katrie Lowe to Everyone : The more common situation that most people normally have to deal with I imagine is more of a delegation of authority situation rather than guardianship (sorry I might be mixing terminology meanings). I'm wondering whether verifiers (like the bank example you gave) really need to be issuing separate credentials to the delegate or whether I as the original holder should be able to just issue a delegation credential to the person I want to represent me and that should be enough to recognise my wishes?
06:42:36 From skyberg to Everyone : Business relationships are based on “ownership” Ie, dependency = subsidiary, etc. I think “ownership” is likely not a good term to apply to human entities.
06:47:23 From John Phillips to Everyone : Two hands raised, we'll get to you...
06:47:38 From skyberg to Everyone : Actually, banks do allow “authorized users” on an account - which is a form of delegation.
06:50:57 From Jo Spencer to Everyone : That's more like a joint account or small business accounts... All possible, but that's not typically delegation that isn't seen by the bank. Financial POA is the complex and legal process normally in my experience
06:51:43 From skyberg to Everyone : That’s true, Jo.
06:53:09 From Jo Spencer to Everyone : https://www.eventbrite.nl/e/tickets-techruption-stagegate-meeting-ssi-guardianship-poc-results-148912135205
06:55:53 From Sterre den Breeijen to Everyone : https://service.ssi-lab.nl/ SSI service provider to ensure interop
07:02:34 From skyberg to Everyone : Just curious. Why do you see KERI as a requirement?
07:04:18 From Sterre den Breeijen to Everyone : perfect example why a bunch of technologists should not decide what guardianship look like ;)
07:04:37 From Sterre den Breeijen to Everyone : but also context, business requirements etc should be taken into account!
07:12:16 From skyberg to Everyone : That makes sense! If guardianship is a relational entitlement within the context of a specific jurisdiction, then cross-jurisdictional engagements become challenging.
07:15:18 From skyberg to Everyone : Best meeting of the day! Thanks everyone!
07:16:34 From Jo Spencer to Everyone : Thanks, really appreciate your input!
07:16:48 From skyberg to Everyone : In a perfect world, the authoritative source of a guardianship VC is the jurisdiction itself?
07:17:17 From Hira Siddiqui to Everyone : How can we pitch in to help with the guardianship whitepaper etc?
07:19:08 From skyberg to Everyone : This starts to sound a lot like Trust Frameworks. In order to understand what an IAL3 assurance attestation means, you need to reference the trust framework. Can’t consume the assurance statement independent of that trust framework.
07:19:14 From Jo Spencer to Everyone : The Sovrin Guardianship WG Group is here … https://guardianshipwg.atlassian.net/wiki/spaces/GWG/overview or just reach out to John or Jamie Stirling or I
07:19:30 From Hira Siddiqui to Everyone : Thanks!
07:19:31 From Jo Spencer to Everyone : https://groups.google.com/a/sovrin.org/g/guardianship
07:19:41 From skyberg to Everyone : So, maybe a guardianship VC needs to include the jurisdictional reference also.
07:19:56 From Sterre den Breeijen to Everyone : yes, we included that i nthe requirements
07:20:02 From Jo Spencer to Everyone : Exactly - it's proposed...
07:20:03 From skyberg to Everyone : So, I’m a guardian under COPPA, or something.

The New did:indy DID Method - Future of Indy Ledgers

Tuesday 4I
Convener: Stephen Curran, BC Gov and Hyperledger Indy
Notes-taker(s):

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

Link to Presentation
Getting involved with this work:

- HackMD Document with current spec
- Home of future spec: indy-did-method
- Meeting Wiki and schedule
- Hyperledger indy-did-method chat channel
- Currently seeking developers to implement the required updates
    - Python for indy-node, Rust for indy-sdk and indy-vdr

Introducing: WACI (Wallet And Credential Interactions)

Tuesday 4K
Convener: Jace Hensley (Bloom)
Notes-taker(s):

Tags for the session - technology discussed/ideas considered:

VCs, Presentation Exchange, Credential Manifest

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

https://specs.bloom.co/wallet-and-credential-interactions/
https://specs.bloom.co/wallet-and-credential-interactions/versions/v0.1.0
We reviewed the spec above,

Orie linked this related github issue and discussion:

https://github.com/w3c-ccg/universal-wallet-interop-spec/issues/84

Also related: https://w3c-ccg.github.io/vp-request-spec/#format

Use cases support mobile wallets, backend services and web apps.

Supports chaining of requests…. Relies on credential manifest and presentation exchange

W3C CCG work seems focussed on the “vc-http-api” and “vp-request-spec” as the solutions to this problem…

We reviewed IoT / Web / API considerations for presentation exchange.
We notes the following hypothetically viable non interoperable solutions to this problem:

1. DIDComm v1 (IIW ticket flows?)
2. vp-request-spec + CHAPI
3. vc-http-api + …. ? / w3c ccg traceability API.
4. OIDF vp-token spec?

Leave your email if you want to be contacted about WACI:

- orie@transmute.industries
- pevanwolf@gmail.com

OIDC Claims Aggregation

Tuesday 5B
Convener: Nat Sakimura, Edmund Jay, Kristina Yasuda
Notes-taker(s): Kristina Yasuda

Tags for the session - technology discussed/ideas considered: OpenID Connect, Claims Aggregation, Claims Issuance

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

Session Slides: https://docs.google.com/presentation/d/1w-rmwZoLiFWczJ4chXuxhY0OsgHQmlIimS2TNlce4UU/edit?usp=sharing

This session discussed how OIDC Claims Aggregation Draft solves certain problems left open in Connect-Core: 1/ How to get a token from CP is hand-wavy; 2/ No specified method to down scope the userinfo of the CP; 3/ No way to provide a binding information between CP:sub and IdP:sub.

The draft specifies the methods for an application to:

- perform discovery for a Claims Provider
- register a client to a Claims Provider
- obtain claims from the Claims Provider
- return aggregated claims from Claims Providers to requesting clients

After the presentation we discussed

- How consent will be handled. IdP gets consent from the user to share to the RP. Does Claims Provider have to get consent from the user to share the claims to the IdP?
- Signed Claims mechanism in Claims Aggregation draft vs DPoP in Credential Provider draft?
- What does making aggregated claims mandatory in the response mean for the implementations?

Notes Day 2 Wednesday April 21 / Sessions 6 - 15

Secure Scuttlebutt Intro

Wednesday 9A
Convener: Charles E. Lehner
Notes-taker(s): Charles E. Lehner

Tags for the session - technology discussed/ideas considered:

Secure Scuttlebutt, Onboarding Difficulty, Append-only Logs, Gossip Protocol

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

Convener asked for suggestions. Participant suggested an onboarding demo. Convener accepted and directed participants to website https://scuttlebutt.nz/ and to the download page https://scuttlebutt.nz/get-started/ .
Participants downloaded an SSB app: Patchwork and/or Manyverse.
Convener introduced the concepts of SSB Rooms and Pubs, and proposed using Rooms for onboarding, referring to a public list of SSB rooms:
https://github.com/ssbc/ssb-server/wiki/%23ssbrooms
Convener picked a room from the list for use and shared the link to the participants.

Convener participated by running Patchwork on a new device.

Participants used the invite code from the Room in their SSB app, successfully joining the room. including convener, They found eachother's profiles in the room connections list, approving the apps to make connections to eachother when prompted. Participants noticed there were also other SSB IDs visible in the room, which were visible only as IDs (public key based) without name or icon. Convener said that these were other SSB IDs connected to the Room whose content had not yet been "replicated". Convener attempted to explain SSB replication. A participant requested diagrams. Convener referred to the Scuttlebutt Protocol Guide:
https://ssbc.github.io/scuttlebutt-protocol-guide/
Convener explained that SSB messages, including updating the profile info and following other users, any time when the "Publish" button is used, are permanent. A participant asked about the SSB ID (string of characters beginning with "@" and ending in ".ed25519"), if it can be used publicly; convener answered that it is public identifier for their SSB account.

One or more participants may have found the onboarding experience difficult, confusing, and/or frustrating. The convener referred to UX Research that was done on Manyverse in the hopes of expressing trajectory of improvement:
https://www.manyver.se/ux-research/

Some participants may have been unable to fully onboard. Convener continued the onboarding with the people were able to join the room.

Convener did not record session or chats, but did take a screenshot, included later in this document.

A participant asked for more technical information. The convener attempted to describe the data model of SSB, consisting of JSON messages that are hashed, signed, and structured in an append-only list called a SSB feed. The message signing format is not a standard, predates JSON Canonicalization Scheme, but has multiple implementations, and uses ed25519 (and sha256). The SSB DID Method Draft Pull Request was not mentioned.

The participants during the session did not follow anyone outside their small network, although they could connect to others via the room.

Further resources:
https://scuttlebutt.nz/docs/introduction/detailed-start/
https://en.wikipedia.org/wiki/Secure_Scuttlebutt
https://github.com/ssbc/patchwork/

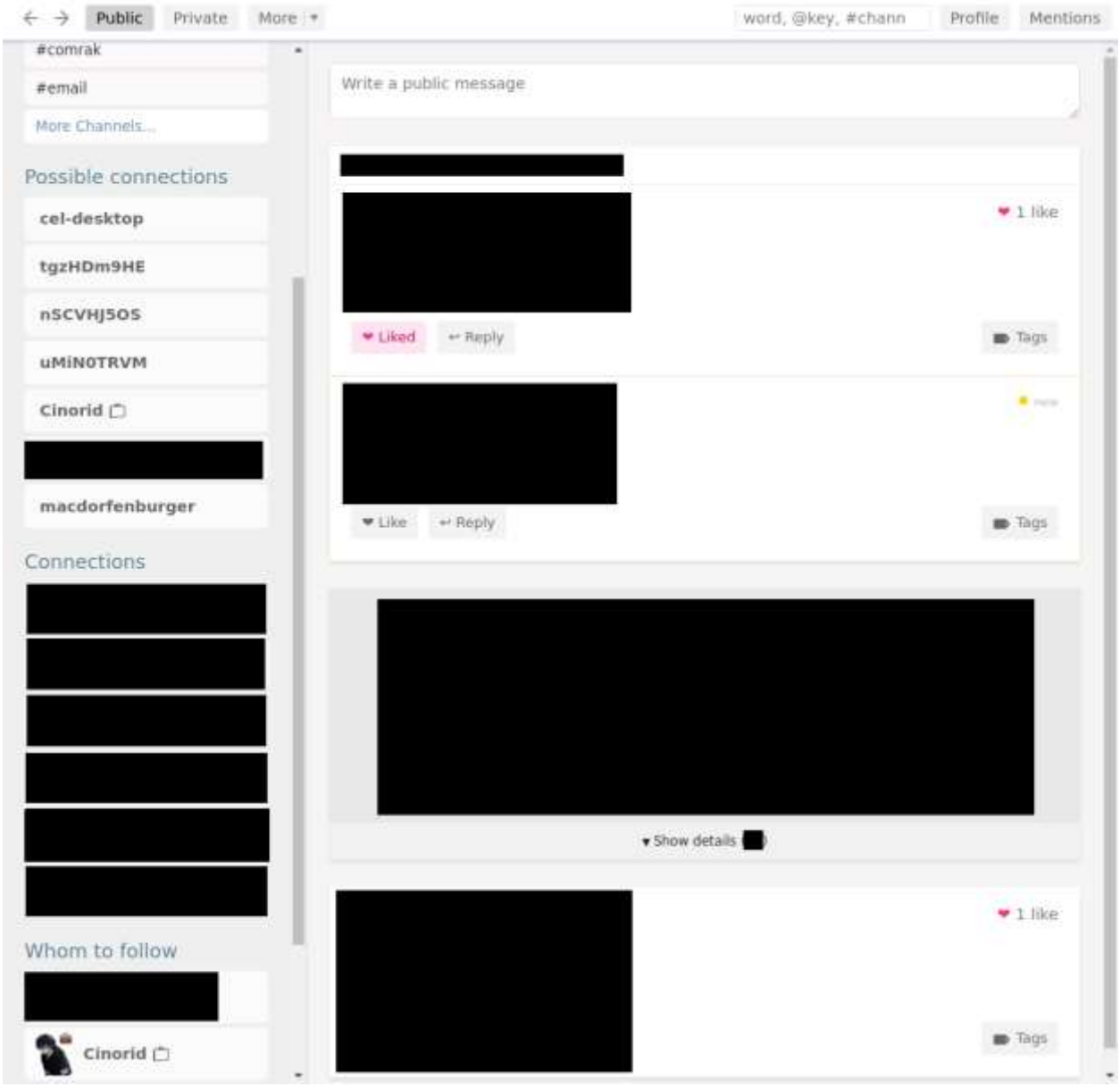
Additional notes by the convener:
This was the first time I tried to lead something like this, and I apologize there was difficulty with it. If done again, I believe it should be planned more in advance, and with better preparation for answering questions. I hope this document effectively represents the onboarding process that took place at this session, that it may be useful for others doing similar processes, and that it can serve as a reference for better understanding of the Internet Identity Community and Secure Scuttlebutt. Parts of this document may be published on SSB and the Internet.

This was also my first time onboarding via a SSB Room, while previously I had always used a Pub, or LAN connection, or other method of onboarding. The Room method was successful. It resulted in a separate network but which can easily join the "main SSB network".

Things to do differently next time:

- Invite another SSB person in advance, to help answer questions from participants and provide additional perspective.
- Prepare to answer common questions, with diagrams as well as words.
- Consider preparing the session notes document as a template, with intro text and participant info ready to fill in.
- Consider recording session video.
- Consider saving chat.
- Request consent from participants during the session to record their SSB ID in this document.
- Request consent from participants during the session to record their other content appearing in screenshot(s) in this document, such as profile picture/icon, name, description, posts, contact/follow message, likes/upvotes, channel subscriptions, connections.
- Note that pubs and room peers both appear in "Possible connections" in Patchwork.
- Request consent from other SSB participants whose ID appear or who are mentioned in the screenshot.
- Note that the room server does not need to be followed.
- Request additional way(s) to contact participants securely.
- Consider using a room server specifically for the event.
- Consider onboarding via a pub or by LAN instead of room server.

Screenshot, Redacted



The above image is a redacted form of a screenshot of Patchwork taken by the convener during the session.

Closing Sessions 5 - 9 / Opening Day 2 Agenda Creation

Don't Use DIDs, DIDs, nor DIDs: Change My Mind (a.k.a. Oh No He DIDn't!)

Wednesday 10A
Convener: Dave Huseby
Notes-taker(s): Dave Huseby

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

This session was to talk about the topics I put in a recent article that created a huge fire in our community where I lay out the case for completely abandoning the W3C DID standards.

https://dwhuseby.medium.com/dont-use-dids-58759823378c

Joe came and fervently disagreed with my assertions. Lots of people had reasonable counter arguments. My main arguments are 1. DID Documents don't have history when old keys are always relevant and 2. having 94 different DID methods that aren't compatible nor replaceable and don't function the same way is a HUGE problem.

There was no conclusion other than Sam Smith and I came to the conclusion that we have more in common than we thought.

Terasing out the details of DIDs

ZOOM CHAT:
Rouven Heck115:14 Oh no, no fighting here today? ;)
Steve McCown18:27 There have been demonstrations of re-writing GitHub history, so it's not entirely immutable.
Oliver Terbu21:21 DID Docs are time oriented now; DID Docs have old keys available; -> versionId query param; -> nextVersion, nextUpdate etc
Markus Sabadello22:13 +1
Rouven Heck122:17 DID methods - usually with a blockchain for timing :)
Balazs Nemethi24:58 "College Students Make First-Ever Successful Flight And Landing Of A Concrete Airplane"https://www.popsci.com/technology/article/2013-05/these-college-students-flew-tiny-airplane-made-concrete-because-why-not/
Windley25:08 Haha
Steve McCown25:18 @Balazas, I was just posting that! :-)
John Court25:22 How many others were searching for that I wonder
Markus Sabadello25:47 You can "transfer" a DID by updating the controller's key.
Tobias Looker26:04 Yeah +1 ^
Brent Zundel26:06 yeah, I'm not following
Joe Andrieu26:48 Actually you could add whatever you want to the DID Documet
Tobias Looker26:49 So you think the data model should expose a commitment scheme?
Joe Andrieu27:06 So, please add the property to the DID Spec Registries and you're done
Markus Sabadello27:38 ya this could be added as an extension property.
Michael Lodder27:50 but then its only specific to that method
Oliver Terbu28:46 i think you just pick the did methods that address your requirements
Michael Lodder31:27 but then how do you move if you want

Darrell O'Donnell31:33 93 DID Methods - will resolve down to a power law distribution. No different than API proliferation - but better.

Tobias Looker31:59 The DID spec is really bug light for innovation

Paul Bastian32:00 a few DID methods will survive after few years

Tobias Looker32:00 IMO

Darrell O'Donnell32:08 Agreed Joe - DIDs are early - we're in a Premature Standardization phase

Markus Sabadello32:16 I don't think it's accurate to call DID methods "silos". This is an oversimplification and one of the reasons why the DID Rubric was created

Darrell O'Donnell32:18 We're learning,

Paul Bastian32:18 http, ftp were not the only protocols, but the ones that survived

Joe Andrieu32:31 +1 to Brent's notion that this is "what email looks like"

Darrell O'Donnell32:42 "gonna take my marbles and go home"?

Kerri Lemoie33:53 Right now it seems very hard for individuals to choose which DID they'd like to use. Vendors make that decision for them.

Paul Bastian35:41 Email uses like 3 dozen RFCs under the hood and still its pretty interoperable

Andreas Freitag35:50 @DB Thats the reason why you are "locked" in when you decide for a DB…

Dave Huseby36:05 But those RFCs cover each aspect, not multiple RFCs for the same thing

Andreas Freitag36:08 And only can migrate with a certain pain :)

Darrell O'Donnell36:27 @Kerri - agreed, to me the companies that are using DIDs well, are isolating the DID churn from the user.

Kerri Lemoie38:52 +1 @Darrell

Joe Andrieu39:40 +1 to layer innovation.

Darrell O'Donnell39:52 We are in EARLY days - the churn here is high and will continue to be high. Throwing a standard into play that folks think is more advanced (i.e. mature) than it really is.

Joe Andrieu39:56 that's right.

PhilWolff40:04 control as an emergent property of the architecture?

Darrell O'Donnell40:21 @Sam - 100% - "hey DID:method, do you KERI or am I on my own here?"

Dave Huseby40:55 @Darrel "hey KERI can I have my data back?"

Dave Huseby40:58 :)

Darrell O'Donnell41:33 @Dave - yeah, and "Hey DID:method - where else do you anchor KERI"

Darrell O'Donnell41:44 wait - someone is making $$$ here?

Rouven Heck142:01 haha - yeah, for sure not with DID methods :)

RickC42:02 that was going to be my question;)

David Waite42:02 Mostly on side bets, sure

Lynn Bendixsen42:29 Maybe his money comment was "tongue-in-cheek"?

Joe Andrieu42:36 LOL. http is also a silo

Kerri Lemoie42:47 In education credentials, there's common thought to use methods that aren't blockchain (vendor) related.

Darrell O'Donnell42:55 "I do wonder whether at this point, Bitcoin should also be thought [of] in part as a Chinese financial weapon against the U.S.," - Peter Thiel

Joe Andrieu43:17 That's right. Blockchain fixes this.

SamSmith43:20 Hourglass theorem stack of thin layers wins over stack of thick layers

Joe Andrieu43:20 *snort*

Rouven Heck144:01 Sam - agreed. The question is - what is the thinnest part of the hourglass?

Steve McCown44:15 Why is it not possible to "take your data and go home"? If it's a problem, then why not create a way…

Darrell O'Donnell44:17 @Sam - +100 - we're discovering the natural thin layer delineation, but we aren't done that learning. Your KERI work is a seminal piece that helps.

PhilWolff44:25 So, what are the alternatives? A fork of DIDs/VCs? Or something new?

SamSmith44:31 Control security should be lower thin layer than namespace layer.

Darrell O'Donnell45:53 @Sam - lower layer for sure. We may need a GetCapabilities() at the namespace layer that allows me to know what that DID:method does -from most basic, to advanced.

Tobias Looker45:57 Well its a standard to construct namespaces

Tobias Looker46:06 URN that is

Tobias Looker46:07 Syntax

PhilWolff47:41 Identity of Things requires offline operation.

Joe Andrieu48:23 Your term "identity" is under defined, Dave

Joe Andrieu50:58 As anyone can do, to assert that same ownership, of that same image

Joe Andrieu51:09 NFTs != DRM

Tobias Looker52:40 How do you communicate which places you have anchored too?

Tobias Looker52:49 And which anchors you are keeping up to date?

Rouven Heck153:20 yeah, why cross ledger?

Tobias Looker53:26 Yeah +1 Sam

Rouven Heck154:02 NFTs require double spend protection -> so it cannot live at 2 ledgers at the same time.

Dave Huseby55:38 Sam’s assertion is wrong

Dave Huseby55:46 Because the provenance log commits to registrars

Joe Andrieu55:55 @rouven There are some ways to achieve some semblance of cross-chain NFT operation, but generally its lock at source chain, play on second chain, and return to first by releasing second. With that pattern, you can get "on-chain" activity on different chains, although I agree that it isn't really active on both chains at the same time.

Rouven Heck156:08 Duplicity detection -> detection that the NFT has an unclear owner now? How would solve the conflict?

Dave Huseby56:24 So even if a stale key is compromised they don’t automatically compromise even older keys

Dave Huseby56:44 Also KERI doesn’t have a way of committing to the requirements for validity of the next event

Dave Huseby56:59 Which prevents stale key compromise from creating a fork

Rouven Heck157:08 @joe - yes, bridges to switch between ledgers. So it’s usually locked on all ledgers, beside one

Joe Andrieu58:08 @rouven yep. eventually we'll get cross-chain state changes, but that requires shared semantics, which is, IMO, a bespoke research project for some future utopia

Brent Zundel58:35 now that this has turned into ADS vs KERI, I'm going to check out

Riley Hughes59:00 Dumb question, are we still talking about why we shouldn’t use DIDs?

Balazs Nemethi59:07 nope

Joe Andrieu59:07 LOL

camparra59:11 Is this the KERI session?

Joe Andrieu59:45 Sort of. This is about some missing features that DID-based applications really wish were solved, but DIDs don't solve on their own

Steve Todd59:48 I'd enjoy a KERI vs ADS slug fest, but I want the DID one first. :)

Michael Lodder01:00:17 I'm happy to have the KERI arg in the KERI session

Michael Lodder01:00:23 I'm interested in DIDs for this one

PhilWolff01:01:01 My biggest takeaway is that the standards processes that lead to the current state of VCs, DIDs, etc. did not hear from Dave (and his concerns) and others that had Dave's concerns. This discussion would have been better a few years' ago so the functional concerns could have been fed into the design stream.

Riley Hughes01:01:13 Markus asked my question

Tobias Looker01:01:14 Exactly my point markus

Riley Hughes01:01:25 Sounds like Dave has created option #94
Tobias Looker01:01:26 Haha and Riley!
Jace Hensley01:01:45 ^^
Tobias Looker01:01:53 Yeah I'm going to spawn another IETF called ADS-2
Michael Lodder01:01:5 I'm failing to see how this is option #94
Tobias Looker01:02:12 Which uses a diff serialisation tech than BARE and other crypto instead of BLS
SamSmith01:02:15 @philWolff I have been arguing the layering change for years in the w3c discussions but one year too late
Tobias Looker01:02:27 Ala another standard and silo
camparra01:02:51 I would like Dave to be able to tell us his solution without being interrupted and being stopped every other word to define it
Rouven Heck101:02:54 @Sam - how do you solve duplicity events?
Tobias Looker01:02:54 *another IETF draft
Rouven Heck101:03:01 (once detected)
Michael Lodder01:03:05 My main takeaway is that the current standard is too silo'd and needs to change
Joe Andrieu01:03:29 that's not entire true. servers often favor IMAP over POP or vice versa
Jace Hensley01:03:39 But isn't that just because everyone adopted the same standard?
Tobias Looker01:03:46 +1 ^
Joe Andrieu01:03:50 @Jace that's right
Steve Todd01:03:50 Why should I build applications on DID if I still have to adapt to every method? What is the standard buying me?
Michael Lodder01:04:15 Exactly @SteveTodd
Kerri Lemoie01:04:17 It's important keep in mind that email addresses are not always used by one individual.
Michael Jones01:04:18 E-mail uses domain names that are issued through a centralized, hierarchical system
Jace Hensley01:04:19 I do feel that pain point Steve ^^
Joe Andrieu01:04:24
@steve it's standardizing how ANY method represents verification methods & relationships and service endpoitns
Darrell O'Donnell01:04:32 @SteveTodd - you won't, some will fall into the "not touching that with a 10 foot pole" for whatever reasons (lack of features, problematic governance, etc.)
camparra01:04:43 Steve has a point
Joe Andrieu01:04:50 it is NOT about standardizing how the information represented in a DID Document is managed in any kind of storage system or network
Rouven Heck101:05:09 At least the interface is same/similar - but agreed, you don't want to trust 94 methods, read from 94 sources/blockchains
SamSmith01:05:34 @rouven Immutable append only first seen policy of any watcher means that the first seen version is the only seen version for that watcher. Distributed consensus amount the set of watchers that any validator trusts provides the authoritative provenance log for that validator.
Joe Andrieu01:05:42 Really, what we've standardized is like the context of a DNS record, while allowing how you read & update those records to be defined at another layer
Andreas Freitag01:05:43 Maybe an idea for an TimeBlockchain, which timestamps all others
Darrell O'Donnell01:05:48 @Rouven +1 - good enough to start exploring and learning - to see where we need to go.
Tobias Looker01:05:52 I don't understand how you can migrate registrars without the duplicity problem sam spoke of
Darrell O'Donnell01:06:16 @Joe - exactly - look at the loose use of DNS TXT, SPF, MX, etc. records

Steve McCown01:06:29 Another question is how will users / services know whether they should trust a particular DID method? Interoperability is important, but trust (given divergent implementations) is also a problem in need of solving.

Darrell O'Donnell01:06:34 DNS is a place to put your tailored thingamajigger

Darrell O'Donnell01:06:47 @Steve McCown - governance

Darrell O'Donnell01:07:12 "We support X, Y, Z for our health records in our jurisdiction" - you can petition to add more.

Joe Andrieu01:07:30 FWIW, I think Dave's bringing interesting challenges to the DID architecture, just like KERI brought forth interesting challenges to the blockchain-based assumptions behind much DID thinking.

Darrell O'Donnell01:07:56 @Joe - agreed. There are nuggets of goodness here.

Rouven Heck101:08:02 @Sam - so Consensus across watchers. Isn't that like a blockchain?

Joe Andrieu01:08:22 And like Keri, I expect the best way to leverage the ADS work is to integrate parts into new or existing DID methods.

Wayne Chang 01:08:34 team `did:adi`!

Tobias Looker01:08:41 haha

Rouven Heck101:08:57 @Tobias - I think with an 'exit' event on chain / registar, you could move to a new chain

SamSmith01:09:01 @Tobias The incepting event commits to the first registrar if its a different registrar then the identifier because its derived from the contents of the incepting event would be different so even compromising keys doesn't allow one to use a different initial restitrar so the root of trust is inviolable. So one can then hop to hop from that unique root.

Darrell O'Donnell01:09:51 @SamSmith - like the post office will be forwarding my mail when I move until everyone figures out my new address - except its better.

Tobias Looker01:10:12 Yes so the initial state of the identifier has to nominate that registrar right?

Darrell O'Donnell01:10:15 @Rouven "he's not here now - he's over _____"

Rouven Heck101:10:26 @Darrel - yes

Rouven Heck101:10:42 like I can forward emails, or DNS :)

Joe Andrieu01:12:35 Wayne, I missed that handoff.

Riley Hughes01:15:04 https://xkcd.com/927/

SamSmith01:15:45 @Rouven yes its a form of distributed consensus but its a much simpler form. It only guarantees safety but not liveness or global total ordering. The stellar protocol uses something similar. Each user gets to pick which subset of stellar nodes its trusts. This allows an open network of validator nodes for Stellar. But a stellar use can select validator nodes in such a way that they do not get liveness. In fact Stellar has a different safety margin from its liveness margin. This has resulted in Stellar having two episodes where liveness stopped. I.e. the ledger stopped coming to consensus for a couple of hours. The ledger was safe, no erroneous transactions were entered but no new ones were either. Once the problem was fixed (in one case is was poor node selection in the other it was a code bug) then consensus resumed on the next proposed transaction. The nodes were not dead but could not come to consensus because the faults exceeded the liveness margin but not the safety marging.

Berend Sliedrecht01:15:47 Great comic!

Tobias Looker01:16:23 Sidetree methods are pretty scalable

Riley Hughes01:16:32 If I'm just dumb, then I'd love someone to explain this to me. But I don't see how this solves the portability problem - unless EVERYONE adopts the single approach (which is not realistic) - but that same thing could happen if everyone adopted a specific DID method.

Tobias Looker01:16:44 But it depends on what you mean by scalable?

Jace Hensley01:16:53 I agree riley

Drummond Reed01:17:07 DIDs are not a Web technology

Tobias Looker01:17:24 DIDs has an ADM though?

SamSmith01:17:26 Cryptographic accumulators are cool and provide some scalability advantages. But any DID method can use crypto accumulators. They are not necessarily tied to ADS. Certainly KERI can use them.

Markus Sabadello01:17:30 JSON LD isn't a requirement for DID methods

Drummond Reed01:17:37 DIDs do not require JSON-LD. It uses an abstract data model - at Dave's strong suggestion ;-)

Lynn Bendixsen01:17:39 millions of issuers is a lot more realistic...not billions

SamSmith01:18:43 @tobias Yes. The incepting state crypto commits to the first registrar of the indentifer derived from the crypto commitment.

Darrell O'Donnell01:18:53 NETBEUI we miss you

Markus Sabadello01:19:43 I think there's a bright future for did:ads :)

Hunter Cain 01:19:55 haha

Darrell O'Donnell01:19:57 but @Markus - we're allowing advertising?

Tobias Looker01:20:46 Agree sam wasn't clear with ADS if that was the same situation

SamSmith01:21:53 So an NFT using that identifier is locked to the first registrar. A subsequent event that changes registrars will have to be first registered on the first registrar. It will be first. You still need duplicity detection for stale later attacks in the future but its trivialized due to the priority of the first seen policy.

Riley Hughes01:22:05 Dave how is this a user sovereign if a user can't "take their data and go home" to another system that uses DIDs?

Drummond Reed01:22:14 And it has a patent pending component, yes?

Michael Lodder01:22:23 @Riley you're missing the point, you can with ADS

Michael Lodder01:22:46 No @drummond, he's recommending RSA accumulators, no patent there

Riley Hughes01:23:03 Any DID method can use RSA accumulators too though no?

Michael Lodder01:23:08 Correct

Michael Jones01:23:11 Thanks for the session, Dave, and for the discussions, Joe, Sam, etc.

Michael Jones01:23:13 Demo time now

SamSmith01:23:35 @Tobias currently AFAIK ADS is incomplete. It needs duplicity detection like KERI in order to solve the security issue I described. Should ADS add that then is will be essentially a variant of KERI.

Brent Shambaugh01:24:01 +1 did:key

Brent Shambaugh01:24:21 horrible security though :: grin ::

SamSmith01:24:28 Crypto accumulators operate at the VC layer not the keystate layer

Tobias Looker01:24:41 Yeah +1 this is a great conversation none the less

Tobias Looker01:24:55 Understand @Sam

Tobias Looker01:25:11 Thanks dave

Making The Intention Economy Happen, Part 2

Wednesday 10B
Convener: Doc Searls
Notes-taker(s): Doc Searls

Tags for the session - technology discussed/ideas considered:

Intention VRM

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

This was a small meeting primarily meant to tee up Hadrian Zbarcea's demo of Customer Commons' new Intention Byway model for better signaling between demand and supply in markets of all kinds

Here is the slide deck we used: https://www.slideshare.net/dsearls/iiw-xxxiiintentionsession

COVID Credentials Initiative: Challenges & Learning

Wednesday 10C
Convener: Lucy Yang
Notes-taker(s): Neil Thomson

Tags for the session - technology discussed/ideas considered: #COVIDCredentials

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

Challenges and Learning covered. (Slides 13-14)
Slides covered
https://docs.google.com/presentation/d/11K027LlitWljJu_XNTztqc6BGvhsD8JBX5OkavLEEMA/edit?usp=sharing

Solution assumption with the Good Health Pass is revoking is not necessary as VCs are short lived (solution to invalid credential). Issuers will re-issue vs. revoke
In many cases, labs are providing incorrect information in vaccination records, which need to be re-issued

- Still need to notify the holder that their (current VC) is invalid and they need to take action to resolve
- Issuers asking what if we make a mistake – (re-issue)
- Holders having problems findin there vaccination VC
- Many of the unresolved issues are governance/policy related (for which the "health authorities") have not worked out the details

- Policy providers are applying the brakes through in-grained bureaucracy to produce a perfect standard for their jurisdiction vs. rapidly evolving a common standard and "usable solution" in the short term.
- Unclear on how to get VC and underlying data into the hands of holders, particularly as holders don't have the technology and skills to manage their health data.
- Data privacy is an issue across each of the implementers and users of the Issuer, Holder and Verifier roles. Lack of common understanding and agreement on how and who owns and controls the data
- WHO standard will likely be adopted in the Global South (hemisphere)
- GHP looking to paint a forward looking common picture, including interim solutions (iterate standards)
- The number of players (and their levels of understanding/expertise and agreement with the current direction) alone makes consensus very difficult
- Paper credentials have been getting consensus on interim solutions.
- W3C and WHO are great candidates.
- Affinidi is making a universal verifier application (https://www.affinidi.com/)

Question – what experience from the "wild" is contrary to the solution direction

- Existing imlementers (with proprietary solutions) are reluctant to move to evolving standards until they ARE standards (particularly if there are "competing" standards
- There are so many moving pieces (conceptually and details and governance frameworks and…)
- Some countries are insisting on seeing the underlying vaccination record (vs. a VC yes/no)
- What is relationship between CCI and GHP?

  Answer – both groups have a large overlap in involved organizations and people

- GHP is driven by payments and travel industry
- CCI is being driven by the VC technologies
- [Anil john] this involves Pipes, Payloads and Policies

Some industry have comfort in being FHIR derived, supported by those how have bought into Electronic Health Records

Juristication – big friggin' bomb of an issue

This is a place were Gov't leadership would help, but concerned on hot Gov't is acting

Perhaps throwing in out for solution and depending on Gov't to sort out policy – is not a strong path to success

- Organization's putting vaccines in the arm of people are not obligated to share most of the vaccination record information – but it is reality (major existing players make to much money on the data) – particularly for US organizations who are profit driven. Consistent with "Data benefiting tech" not willing to give up their data (that they make money from)

Directories in Distributed Identity

Wednesday 10D
Conveners: Sam Curren, Ken Ebert, Suresh Batchu, Kiran Addepalli
Notes-taker(s): Kiran Addepalli [kiran@digitaltrust.net]

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

Slide Deck:
https://docs.google.com/presentation/d/1YjTJK1Zq8Z5iRmo3cn321EUu4fjwpCci/edit#slide=id.p1s

ADIA site: https://adiassociation.org

- Does the Directory support a pairwise DID - The directory supports exchange between two parties. The directory enables the interaction.
- Would including a DID in an LDAP be a good way to implement the directory?
- Much of the social web doesn't require KYC. Trusted Issuer = Trusted by the Directory. We don't prohibit the model where self-asserted identities are not left out. Ex: Email provider can be a trusted issuer. Some services like Instagram are getting good at providing ads that are relevant.
- Directory is responsible for the DID and then it is up to the parties to decide what information to share.
- Will Alice be notified by the directory when one of her DIDs has been shared with Bob — or only if/when Bob reaches out to her via the DID obtained from the directory? - Yes
- I am just wondering if there is probably a need for syncing in a decentralized manner. E.g. I am registering a Service at a specific Directory Service (because I know exactly that one) but I want to be distributed (in a verified way) that the service will be available on all other directories which somebody else want to trust.
- How would customer integrate with the ecosystem
    - We have the specification coming up in june. The technology working group meets on thursdays. Please contact jason@digitialtrust.net for further details.
    - The specification also aims to address some of the protocols to interact with the directories.
- Will the Directory analyze/store query results to optimize future query results or would that violate the Directory's privacy model? - we are focussing on the metadata lookups for faster lookups.
- I think there is room for zero-knowledge service type directories that don't know about the data they process, as well as transparent ones that do query optimization and analytics
- Dan Robertson - On an earlier topic, even when hashed search values are used, a client could potentially do fuzzy matching with a local list of synonyms, where a user inputting "dan" would also automatically get results for "daniel" and "danny".

Integrating FIDO with Verifiable Credentials

Wednesday 10E
Convener: David Chadwick
Notes-taker(s): John Callahan, David Chadwick

Tags for the session - technology discussed/ideas considered:

FIDO2, Web Authn, Verifiable Credentials, IAM.

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

W3C Web Authentication (FIDO2) provides a mechanism for strong authentication whilst W3C Verifiable Credentials provide a mechanism for strong identification and authorisation. Together they make an unbeatable pair for identity management.

Prof. David Chadwick presented work on sharing W3C Verifiable Crendentials via FIDO2 key setup with issuers of credentials. In a nutshell, the holder and issuer use the WebAuthN protocol to strongly authenticate before the issuer protects the credentials with its signature. Upon providing credentials to a relying party, the issuer (acting in an IDP capacity, so they must be online) will verify the identity of the holder via FIDO2 WebAuthN so that the credentials (or selected claims in the credentials for selective disclosure) can be shared with the relying party. Ephemeral keys are created to bind the holder with such credentials shared to the relying party/verifier. The relying party/verifier can use X.509 certs to confirm that the issuer is valid by checking the signature on the derived credential from the holder.

David has a slide deck and video at https://youtube.com/watch?v=l3taGxBdrRU

The eSSIF TRAIN project from Fraunhoffer url:
https://essif-lab.eu/essif-train-by-fraunhofer-gesellschaft/
Is building a trust infrastructure for SSI, whereby a VC will contain the name of its trust federation, and the verifier will call the TRAIN API passing it the name of the trust federation, the URI of the VC Issuer, and asking if this issuer is really a member of this trust federation. The response will indicate how trustworthy the issuer really is. TRAIN will work with both blockchain DID and X.509 trust infrastructures.

Verifiable Credentials for Authentic Data in the Supply Chain

Wednesday 10G
Convener: Gena Morgan, Kevin Dean
Notes-taker(s):

Tags for the session - technology discussed/ideas considered:

Using DiDs and VCs for verifiable product data in supply chains, leveraging the largest supply chain standard system in the world,
2.5 million users companies, over 6 billion product scans per day

Product data and attestations from a number of various authoritative sources
Leverage DIDs/VCs for distributed data sharing, verification

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

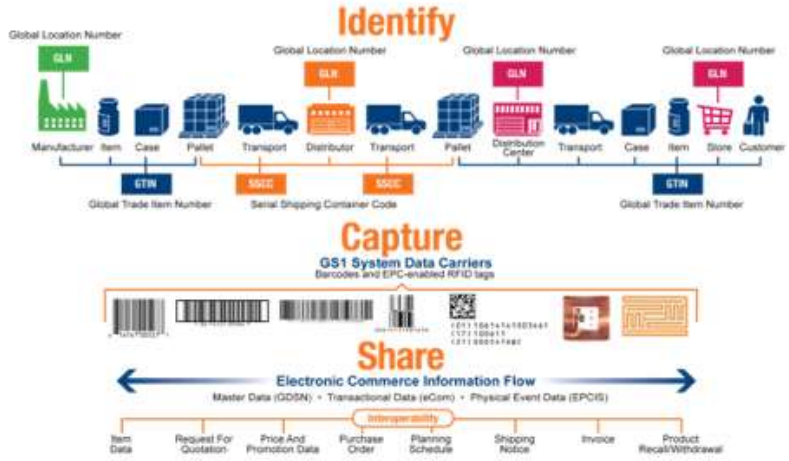
Goal was to present a real world application/PoC of this techin supply chains/enterprises. Looking for feedback. Largest issue in actually implementing with users is interoperability. FUture session will ask questions of the technologists.

Link to presentation slides accessible until May 28th: public link or see images embedded below.

The GS1 overview video referenced in the presentation can be found at https://www.youtube.com/watch?v=iDkANArgdKI.

Key industries served

Identify, Capture, Share



GS1 standards **identify products**

Global Trade Item Number (GTIN)
20614141000030

Global Trade Item Number (GTIN)
10614141000033

Global Trade Item Number (GTIN)
00614141000036

GS1 standards **identify physical locations and entities**

Manufacturing plant

Global Location Number (GLN)
0614141010042

Distribution center

Global Location Number (GLN)
9521101530018

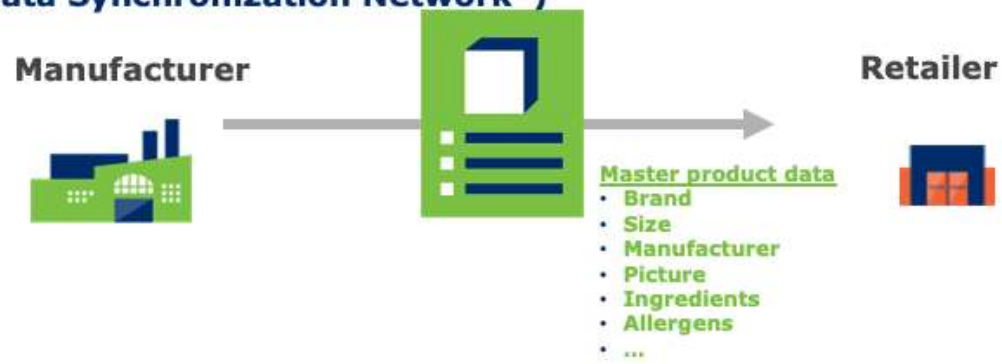
Retail store

Global Location Number (GLN)
9528731996092

GS1 provides standards for **data carriers** to hold the identifiers

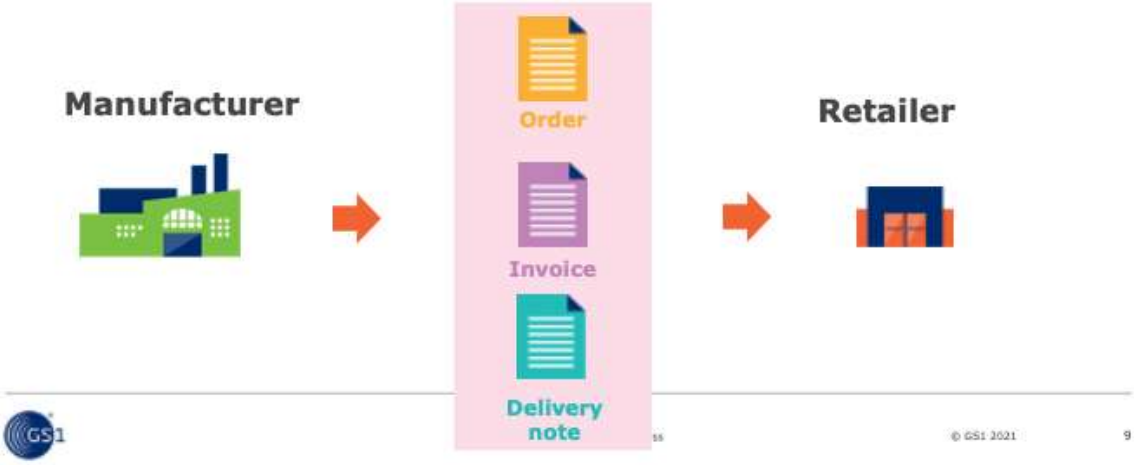
GS1 provides standards and services for **sharing master product data** (GDSN)

Product data input by manufacturers into a worldwide network of databases that retailers can access ("Global Data Synchronization Network")



GS1 provides standards for **Electronic Data Interchange (EDI)**

Flow of financial and supply chain documents to match the flow of goods ("Electronic Data Interchange")



GS1 provides standards and services for sharing **Traceability** information

2020 – A year of discovery

GS1 Technology Value Proposition

- GS1 License Credentials bring the 50-year-old identification system into the world of Verifiable Credentials and form the foundation for identification with VCs
- GS1 Digital Link (URI representation of barcode content) as credential subject in VCs connects trusted data to the existing ecosystem
- GS1 Web Vocabulary VC Link types (and link-sets) allowed trusted discovery
- GS1 certification VC provide increased portability and trust in data from multiple certification bodies and parties

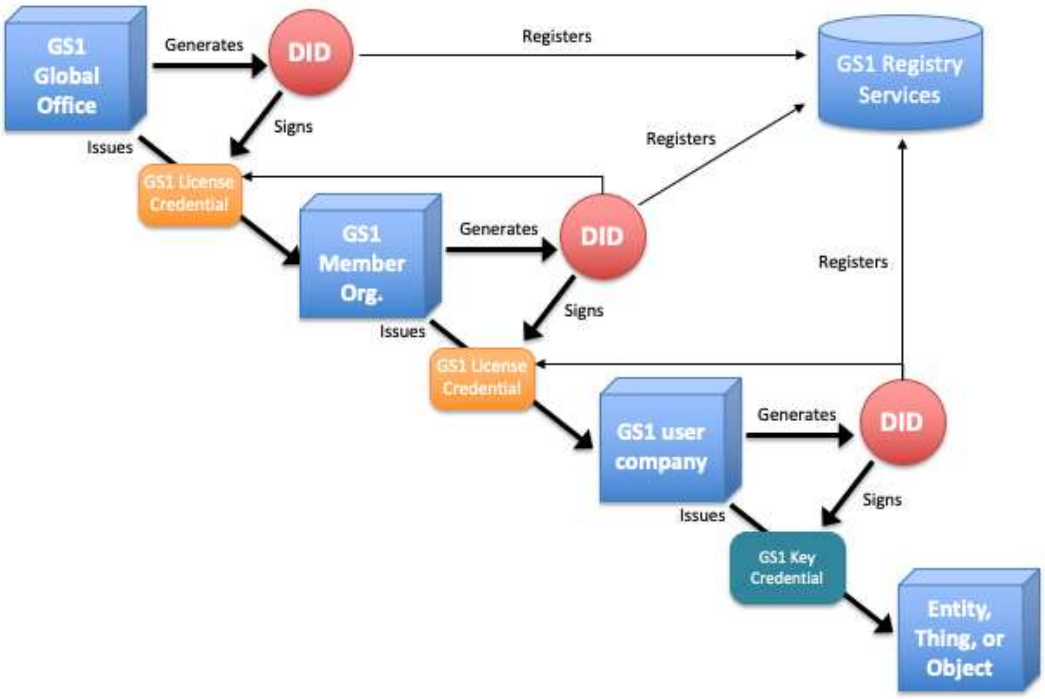
NPI Value Proposition

- New products to shelves faster
- Trusted partner identification without human intervention
- Validate GTIN licenses save conflicts and errors
- GS1 certified planograms without human intervention. No duplicates.
- Verifiable product data from 3rd parties and registries
- Trusted data flows from brand to customer

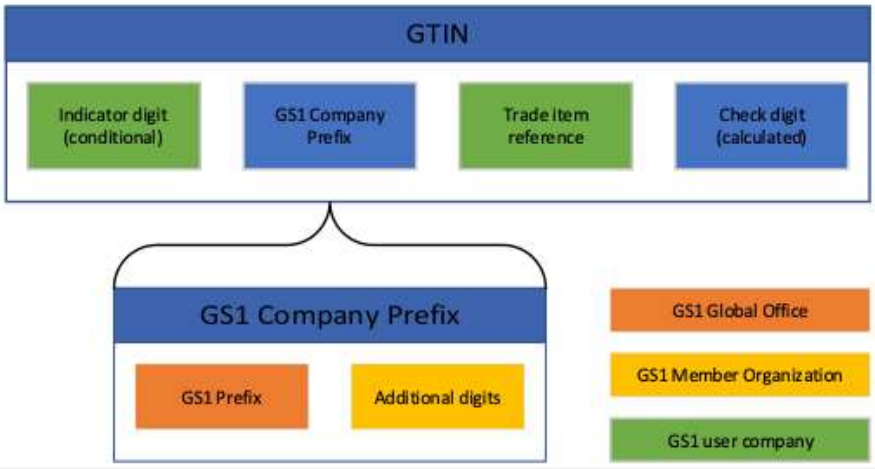
Demo

https://www.youtube.com/watch?v=iDkANArgdKI

Implement GS1 Verifiable Credentials to provide digital verification of the authenticity of GS1 identifiers and of the data associated with them



Global Trade Item Number (GTIN) Structure



GS1 Prefix

- Unique string of two or more digits
- Issued by GS1 Global Office
- Allocated to a GS1 Member Organization
- GS1 Canada allocated "754" and "755"

GS1 Company Prefix

- First digits are a valid GS1 Prefix
- Unique string of four to twelve digits
- Issued by a GS1 Member Organization
- Allocated to a GS1 user company

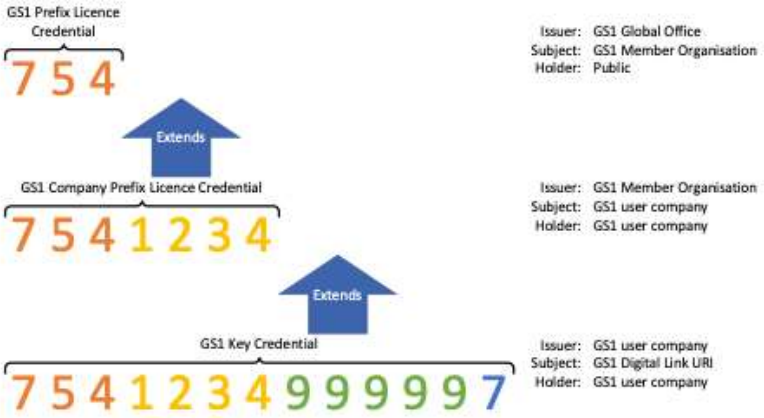
Trade Item Reference

- Assigned by GS1 user company
- No significance
- Must be unique within the GS1 Company Prefix

Check Digit

- Mathematical function of preceding digits
- Used to minimize errors when entering digits manually
- Catches 100% of single-digit errors, 90% of all others

"Extending" Verifiable Credentials



"Extending" Verifiable Credentials

- GS1 Prefix Licence Credential is the root credential, issued by GS1 Global Office
- Every subsequent credential has a reference to the credential that it extends
- It's not enough for an individual Verifiable Credential to be validated
  - The credential that it extends must be validated as well, all the way up to the GS1 Prefix Licence Credential
  - The issuer of credential must be the subject of the extended credential
  - The GS1 Prefix Licence Credential must have been issued by GS1 Global Office (well-known DID)

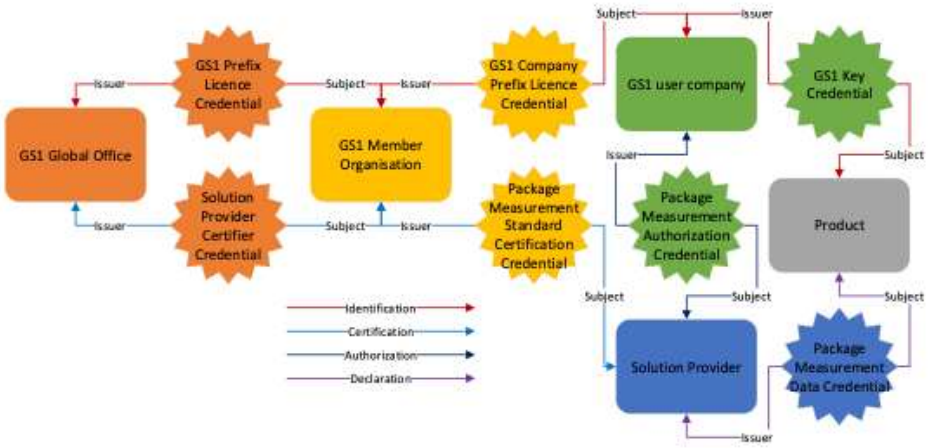
"Extending" Verifiable Credentials

- Key feature of the extension mechanism is that it does not require that every credential be issued under the same ecosystem
  - As long as the ID of the extended credential matches the "extends" attribute of the extending credential, the chain is valid
  - Requires validator to understand all ecosystems present in the chain
    - Easier than requiring issuers to issue the same credential in multiple ecosystems

Authentic Data

- For data about a product (or anything identified by a GS1 identification key) to be authentic, it must be declared by the licensee or an authorized agent on behalf of the licensee
- Verifiable Credentials may be used to declare the data and to authorize an agent to declare data on behalf of the licensee
- Trusting the data to be correct may require certification of the agent as being competent to provide it

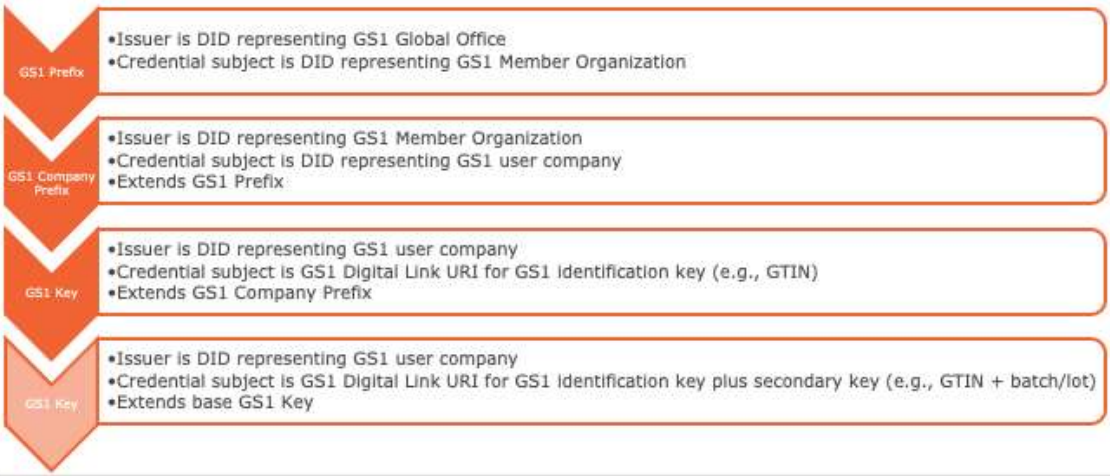
Authentic Data – Verifiable Credentials



Licensing and Declaration

Review

Verifiable Credential Chain



GS1 Digital Link URI as Credential Subject

- Credential subject is an object or array of objects
  - Single Verifiable Credential can assert something about multiple subjects, e.g., a marriage relationship between two people
  - Only a single object is under consideration in GS1 declarations at this time
- Credential subject object may contain an ID, which must be a URI
  - It is recommended that the URI in the ID be one which, if dereferenced, results in a document containing machine-readable information about the ID
  - May be accommodated by having a link type that points to such a document

GS1 Digital Link URI as Credential Subject

- Using a DID requires the generation of a private/public key pair
- Number of DIDs could rapidly get out of control, especially for a serialised product or a large warehouse with thousands of sub-locations
- GS1 Key Credential is only about generating the key and is required to validate the key through the licensing chain to the GS1 Prefix issued by GS1 Global Office

GS1 Digital Link URI and DID

- Some GS1 identification keys can identify subjects who have a DID
  - GLN identifying a party
  - GDTI or GSRN identifying an individual
  - GIAI or GRAI identifying a smart object
- Connection may be made through a "sameAs" attribute

Declaring Data

- Data declarations are the association of the GS1 identification key to the object
- Credential subject is GS1 Digital Link URI

Party Identification Verifiable Credential

Best Practice

- Assertion of identity is association of an external identification key with a DID
  - Assertion may contain additional data such as name and address
- GS1 process is about creating the identification keys themselves
- Party identification is about associating a key with a party
  - Inverse of GS1 process, which associates a party with a key
  - GS1 needs a separate Verifiable Credential type to align with best practice

Party Identification Verifiable Credential

- Party Identification Verifiable Credential is an assertion of identity for a party
  - Credential subject is DID for the party
  - GLN is included in the credential, preferably as GS1 Digital Link URI
    - GLN is traceable through the licensing and identification process
  - Name and address may be included, or may be in a Party Data Verifiable Credential associated with the GLN

Signing Party Identification

- In the GS1 system, the licensee is ultimately responsible for issuing a GS1 identification key and associating it with an object
- As long as the GLN is traceable through the licence credentials, the credential subject of the last licence may issue the Party Identification Verifiable Credential to itself
- For convenience, the GS1 Member Organization usually generates the first GLN from the GS1 Company Prefix and declares that to be the party GLN for the licensee
  - The GS1 Member Organization is acting as a proxy for the licensee

Issuance and Validation Walkthrough

Proof and Credential Status

- Validation assumes that, for all credentials, proof and credential status are properly validated
  - Validation of proof is against issuer's public key
  - Validation of credential status is first against expirationDate (if present) and then against credentialStatus (if present)
- Failure of any proof or credential status invalidates the entire process

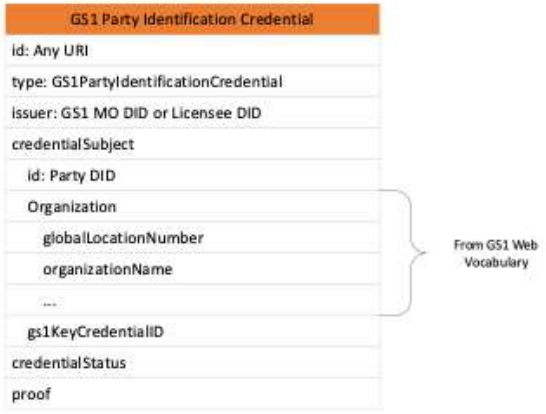
Party Identification Credential Content – Header

- ID: Any URI, not necessary that it be resolvable
  - Party may not want credential to be publicly accessible
- Type: GS1PartyIdentificationCredential
- Issuer: Either of
  - GS1 Member Organization that issued the licence (GS1 MO DID)
  - The party to whom the licence was issued (Licensee DID)

Party Identification Credential – Credential Subject

- ID: DID of the party to whom the Party Identification Credential applies
  - May or may not be the same as the Licensee DID (e.g., subsidiary)
- Organization: From GS1 Web Vocabulary with minimum of
  - globalLocationNumber
  - organizationName
- gs1KeyCredentialID: ID of GS1 Key Credential in which the GLN (as GS1 Digital Link URI) is declared

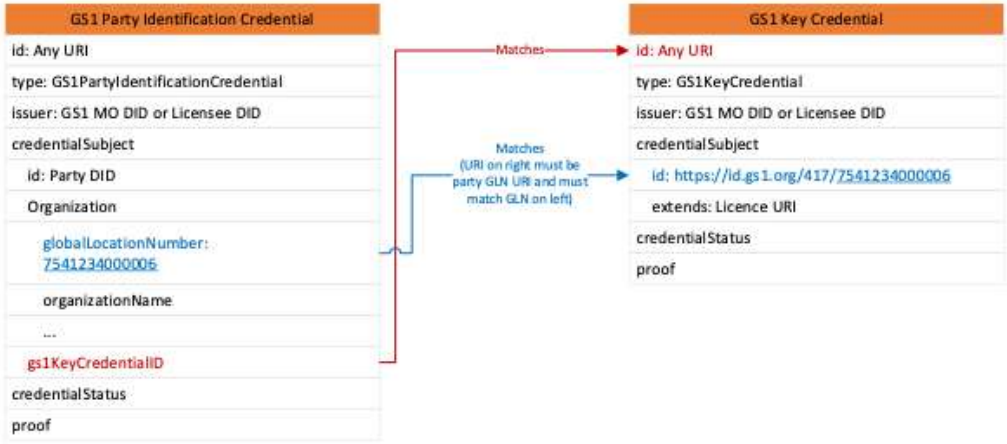
Party Identification Credential



Validation – GLN

- Locate GS1 Key Credential ID
  - Must be resolvable from "gs1KeyCredentialID" in Party Identification Credential or presented with Party Identification Credential
  - If presented with Party Identification Credential, verify that its ID matches "gs1KeyCredentialID" in Party Identification Credential
- Verify that GLN in GS1 Key Credential (as GS1 Digital Link URI in credential subject ID) is the same as GLN in Party Identification Credential (in Organization)

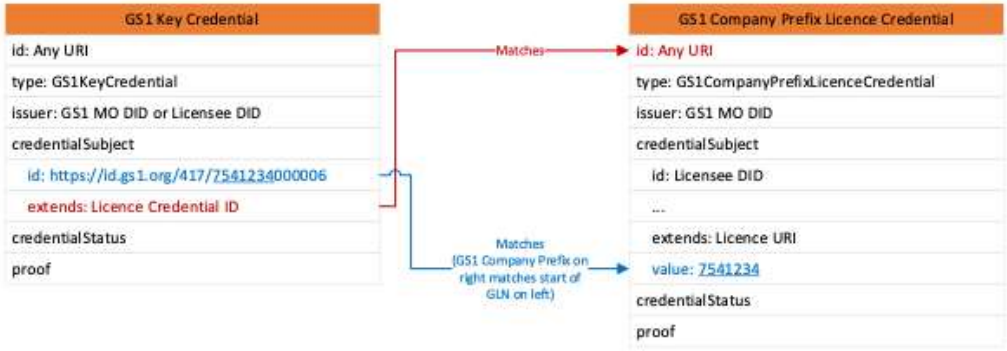
Validation – GLN



Validation – Licence

- Locate GS1 Licence Credential
  - Must be resolvable from "extends" in GS1 Key Credential or presented with GS1 Key Credential
  - If presented with GS1 Key Credential, verify that its ID matches "extends" in GS1 Key Credential
- Verify that GLN in GS1 Key Credential is within scope of GS1 Licence Credential
  - If licence is for a single-issue GLN, must match exactly
  - If licence is for a GS1 Company Prefix, must match up to length of GS1 Company Prefix

Validation – Licence



Validation – Issuer

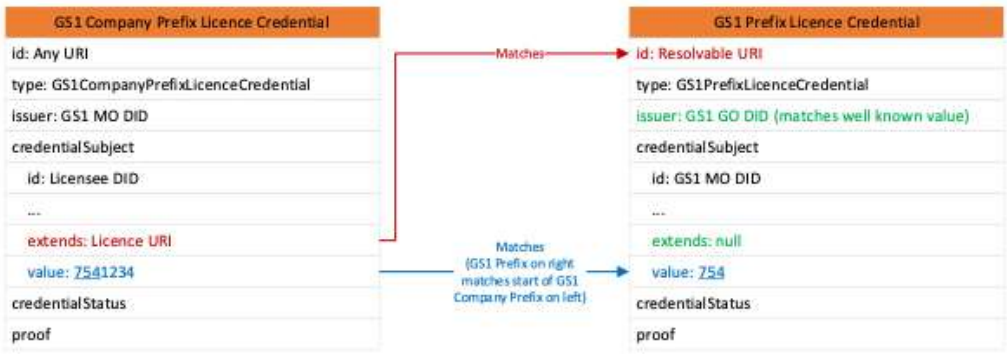
- Verify that issuer of Party Identification Credential is same as issuer of GS1 Licence Credential (GS1 Member Organization) or as credential subject of GS1 Licence Credential (licensee)

Validation – Issuer

Validation – Licence Hierarchy

- If "extends" is not null
  - Resolve "extends" to get GS1 Licence Credential on which current one is based
  - Verify that credential subject ID of extended GS1 Licence Credential matches issuer of current one
  - Verify that current GS1 Licence Credential is within scope of extended one
  - Repeat process for extended credential
- If "extends" is null
  - Verify that issuer is GS1 Global Office

Validation – Licence Hierarchy



Validation – Summary

Validation	If done...	If not done...
GLN	Confirms that GLN has been properly issued	Allows arbitrary GLNs to be declared
Licence	Confirms that GLN has been issued from a valid GS1 Company Prefix licence	Allows GLNs to be declared from other parties' licences
Issuer	Confirms that GS1 Party Identification Credential was issued by an authorised party	Allows arbitrary parties to declare identity of other parties, possibly leading to impersonation
Licence Hierarchy	Confirms that GS1 Company Prefix Licence Credential was issued by a GS1 MO	Allows arbitrary parties to issue GS1 licences

Proof of Concept

Sandbox(es) Development Overview

Goals

1. Expand learning in this area to build expertise required to create an enterprise architecture for a Digital GS1 License system.
2. To evaluate the technology to expand our internal understanding of maturity and compatibility.
3. To create and issue credentials to members engaging in Digital trust pilots. These members are looking for verifiable credential-based supply chain organizational identity.

Scope

Functionality

- Credential Issuance (VC) & Signatures (DIDs)
- Credential Exchange
- Wallet Functionality
- Credential Presentation & Verification

Scale

- Minimal
- Goal is to understand the tech, and functional and technical requirements generally and for scale
- Appx 100s of credentials issued across the stakeholders

Security

- Important to understand the broader requirements for security for post-pilot
- Some degree of security required for pilot - especially as credentials are used in outside pilot projects
- Private key management critical component

Commercialization

- Through sharing credentials with members, we will help to uncover the value proposition and make recommendations **for future** commercialization.
- This effort should enable our tech teams to develop (on paper) an architecture to roll out GS1 License issuing at global scale.

Self-Sovereign Communities of Self-Sovereign Agents

Wednesday 10H
Convener: Adrian Gropper
Notes-taker(s): Adrian Gropper

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

Minimal Demo: https://adriang.xyz/ Use Card Number 4242 4242 4242 4242 04/22 123
(don't use a real email address because it will be stored in Stripe.)

Demo sequence diagram: https://github.com/HIEofOne/Trustee-Community/wiki

Community dimensions - learning and expertise

Organic community growth - supportive - "loud" people" -

- Trustee is just about policies not governance
- DAOs are about governance and that's hard and not very successful

Internet Governance - UDDI - Universal Declaration of Digital Identity

Wednesday 10I
Convener: Jeff Aresty, Kristina Yasuda, Jean Queralt
Notes-taker(s): sankarshan

Tags for the session - technology discussed/ideas considered:

Internet governance, human rights, digital identity, Identity for All, Guardianship

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

The UDDI is a call to action to IIW, which we've said before, to adopt a set of universal principles which can be used now to bring Identity for All projects to fruition.
I want to frame the UDDI discussion in terms of what we did with Jean at the last IIW - our work on the UDDI is step toward the larger humanitarian vision of a Universal Declaration of Digital Rights, which is what he is working on.

We should present the Universal Declaration of Digital Identity as a way to say what the users of tomorrow's technology expect from the technology created by industry and from their governments when it comes to a new digital world, where SSI is at the root of trust.

As we have presented these affirmations at prior IIW and since then to others - we can post a document in the session to get agreement on the affirmations in the UDDI.

This is a Call to Action for IIW to support our role as a convenor in this important area of human rights in cyberspace.

The UDDI Declarations we will discuss are these predicate conditions:

Reaffirming **the human rights and fundamental freedoms enshrined in the Universal Declaration of Human Rights and relevant international human rights agreements such as the UN GP on BHR and Constitutional Rights;**
Reaffirming the relevance of international human rights standards in the digital environment and the need to explore and expand new human rights guarantees for the future;

Recognizing **that the ever constant digitalization of societies has created a number of digital spaces, defined by any network of communications where citizens' data may be stored, with or without their knowledge and with or without their consent;**

Recognizing that individuals in a democracy have full autonomous control over their beings;

Recognizing that while one individual may express itself differently over time, it remains the same individual as it already happens with the different digital identities managed by independent platforms;

Observing **the developing nature of self-determination and digital identity as an emergent human right, necessary for the full realisation and proper enjoyment of economic opportunity, social inclusion, and cultural participation;**

Acknowledging **the increasing degree of responsibility situated upon individuals to administer the security of their personal identities with stakeholders across digital spaces;**

Recognising **that the conflicts of laws arising from competing jurisdictions in digital spaces have created confusion in the due application of the law, demonstrating conflict between societal norms and codified laws;**

Recognizing that all interactions from citizens with digital spaces are performed and create data that cannot be dissociated from them, creating both digital identities and digital assets that belong to the originating source entity:

Affirming that this impossible dissociation entails the observance of Rights by all stakeholders to both the source entity and the associated representational entities;

Emphasizing **the fundamental basis of identity as grounded in natural law, derived from the inherent nature of the world, independent of the roles of government and identity solution providers;**

Deeply conscious **of justice for all as the foundation for any society, where harmonization of the rule of law in digital spaces is central to addressing the trust deficit between governments and citizens;**

Acknowledging **that all individuals have agency to develop the normative behavior governing relationships affecting the well-being of societies, and to direct measures which rebuild trust in the rule of law in digital spaces and foster a new digital trust among digital stakeholders;**

Concerned **that attempts to control and exploit access to identity information through digital technologies for political, commercial, security or other reasons are contrary to democratic principles;**

Deeply concerned **by measures aiming to, or that intentionally prevent or disrupt access to an individual's personal information in violation of human rights law;**
Reaffirming **the relevance of international human rights standards in the digital environment and the need to explore and expand upon novel human rights guarantees for the future;**

At the end of the session, I am inviting anyone who wants to work on this to join an IBO working group which will continue the work on the remainder of the UDDI. When they join, they will receive a copy of the IBO White Paper - Digital Identity for Stateless Refugees - issued at the World Justice Project in May, 2019, for their comment and review.

1. [Jeff] introduction and background context to his interest in this specific topic
    1. Standards fights over a long time leading to industry led standardization
    2. No international humanitarian law exists in cyberspace
        1. UN SDG talk about 'Identity for All'; but there is balkanization happening around geo-political lines
        2. There is a need to speak from the ground up, including developers
        3. UDDR happened at the last IIW with JFQ

See above for the basic principles
. Right to access (for cyberspace)
a. Copyright law
b. Who owns our data
[JFQ] There does not exist a humanitarian law in cyberspace
. Not much of advancement has happened
a. UN panel on digital cooperation could be considered as one of the attempts. The document produced fell short of expectations because it wasn't looking into implementation
    1. UDHR was more focused on governments as BigTech was yet to take the shape/form as of now
b. UN Guiding Principles on Business and Human rights
c. National Action Plans which attempt to address this topic have a non-descriptive language and approach
[Jeff] This specific place has been developed coming from State and other actors.
. The results of these efforts have not resulted in significant adoption
a. Historically there are other ways to adopt global rules eg. trade routes were developed independently of state sponsorship, legislation
b. The above could be a model which can be looked into for technologists to give voice to the notion
c. SSI is not able to comprehensively the topics of ownership of data, control of identity and rights
[Chris] Is this effort focused on identity data or all forms of data
. [jeff] identity data constitutes what could be called a 'digital footprint'. All forms of data originate from/around the individual
a. [Chris] Work at Sovrin focuses on ownership of identity credentials and data conversations. Identity credentials are not 'owned' by the identity holder (eg. DL)
b. [Jeff] The possession of a DL indicates a data which originates from us - the journey includes an issuer and thereafter a credential is created to indicate specific condition is met. The source of this information originates at the individual
c. [Scott David] See Jedediah Purdy (Yale) on issue of "property as a legal imagination". Ownership of data and information "rights" may be a more tractable and scalable approach. Ultimately this is window

dressing. We can call the structure anything we want. Property, according to Blackstone (codifier of English common law) is about the relationship that we have to each other vis a vis an object, rather than our relationship to the object. It is intrinsic artifact of the social contract. I mean that property issue is window dressing. The discussion is very important and serious Challenge of conflicting claims to control needs to be refereed by set of processes. That is birth of law. Licensing model may encounter scaling challenges. Can license/lease tangible property also, but all based on bilateral relationships? What are challenges of scaling bilateral arrangements up to multilateral scales?

d. [JFQ] Is the DL example a more 'participatory model'? The holder gets the choice when verification is being invoked. Data Protection laws are failing because there is transparent enforcement infrastructure which helps the user understand the nature of the technology as well as the facets of data management. Governments see data as intrinsically a part of their citizens.

e. [Scott David] We know how and that licensing works. Query whether it is the most appropriate approach for human existential realization that is implicit in identity. I am not saying that it is not, but it is legitimate question of whether that is the "final enclosure" of late stage capitalism - where we self bind to enclose ourselves into tradable commodities. I think this may be a logical extension of Erving Goffman projections (see 1960s writing), but are we ready for that level of abstraction of self? What if "licensed", but from a selling cooperative structure that represents the group? Like an identity grange? Better negotiating leverage? If you want my data, you have to agree to "OUR" community terms

1. [Jeff] community is the key how you create the community is the challenge trusted online communities can have 'norms' which are enforced by the community members
2. [Scott David] Seed crystal of self interest is at root of all organism and organization cohesions. Enlightened self interest is good if available.
3. [Jeff] standards for what is a trusted online community are what is needed - and, that goes to the issue of who owns the source data I create
    1. [Line] @Jeffrey Would you consider the Principles of SSI an example of such 'norms'?
    2. [Jeff] That's exactly what we are doing - taking Principles of SSI - broadening the stakeholder discussions, including the people especially whom we are serving from the Identity for All projects, and, giving them a seat at the table to develop the new norms for cyberspace - we have to raise our voice

ZOOM CHAT NOTES:

From Kristina Yasuda (US) to Everyone: 09:48 AM Can you record this, Jeff?

From Scott David to Everyone: 10:10 AM See Jedediah Purdy (Yale) on issue of "property as a legal imagination"

Ownership of data and information "rights" may be a more tractable and scalable approach.

Ultimately this is window dressing. We can call the structure anything we want. Property, according to Blackstone (codifier of English common law) is about the relationship that we have to each other vis a vis an object, rather than our relationship to the object.

It is intrinsic artifact of the social contract.

I mean that property issue is window dressing. The discussion is very important and serious@

Chaof conflicting claims to control needs to be refereed by set of processes. That is birth of law.

Licensing model may encounter scaling challenges.

Can license/lease tangible property also, but all based on bilateral relationships? What are challenges of scaling bilateral arrangements up to multilateral scales?

We know how and that licensing works. Query whether it is the most appropriate approach for human existential realization that is implicit in identity. I am not saying that it is not, but it is legitimate question of

whether that is the “final enclosure” of late stage capitalism - where we self bind to enclose ourselves into tradable commodities. I think this may be a logical extension of Erving Goffman projections (see 1960s writing), but are we ready for that level of abstraction of self?
From Scott David to Everyone: 10:12 AM What if “licensed”, but from a selling cooperative structure that represents the group? Like an identity grange? Better negotiating leverage?
If you want my data, you have to agree to “OUR” community terms
From Me to Everyone: 10:13 AM community is the key
how you create the community is the challenge
trusted online communities can have 'norms' which are enforced by the community members
From Scott David to Everyone: 10:13 AM Seed crystal of self interest is at root of all organism and organization cohesions. Enlightened self interest is good if available.
From Me to Everyone: 10:13 AM standards for what is a trusted online community are what is needed - and, that goes to the issue of who owns the source data I create
From Line Kofoed to Everyone: 10:18 AM
@Jeffrey Would you consider the Principles of SSI an example of such ‘norms’?
From Me to Everyone: 10:19 AM That's exactly what we are doing - taking Principles of SSI - broadening the stakeholder discussions, including the people especially whom we are serving from the Identity for All projects, and, giving them a seat at the table to develop the new norms for cyberspace - we have to raise our voice
From Scott David to Everyone: 10:25 AM Precedent is all we have.
People outside of structured systems don’t even enjoy the artifacts of old institutions. Agreed.
They do have risks in common with others. They can be leaders, if provided with efficacy
Ethical constructions versus equitable constructions may be a useful parsing.
Norms precede laws.
Everyone can be a legislator, a judicial officer and perform operating/executive function if they have a phone.
The infrastructure is here.
The “meaning” framework is still geared toward maintaining precarity of large portions of the population.
Slums ring each city because that is where the workers live. Digital slums?
NFTs are amazingly hilarious
I once gave my wife the Brooklyn Bridge as a gift when we moved to Seattle. I should have used an NFT!
Symbolic space is here.
From Chris Raczkowski to Me: (Privately) 10:28 AM
Frankly - I see a lot of good progress. My personal plan is to focus the areas I can influence in a positive manner - and try to worry less about the usual bad actors that always exist. Hopefully good, positive results will marginalize bad actors. But that’s the best we can do.
From Scott David to Everyone: 10:31 AM
Human rights versus property rights.
Harms-rights-duties-breach-causation-damages-liability-insurance-reinsurance-financialization. The legal algorithm.
Start with sovereigns. They are ALL human creations (apologize for the blasphemy). SO ALL human rights ARE HUMAN creations. Self-regulation of the species.
From Chris Raczkowski to Everyone: 10:32 AM Good discuss - which I’ve been happy to attend. I have to jump to another meeting . . .
From Scott David to Everyone: 10:35 AM +1 Jean. Analog vs. digital. Consider notion of rule of law and equity-based protections for the shift.
From Line Kofoed to Everyone: 10:35 AM Thanks!
From Scott David to Everyone: 10:42 AM Harm to data - concept like conversion of personal property possibly?

Start with harms/anomalies.
Engineers and lawyers can agree what is “anomalous” in a system operation.
Harms is starting point. Nice.
Data is the vector through which the harms are communicated.
Also money is the vector through which the harms are quantiied
Democratizing the dark web.
We are moving into the space. This is happening.
Leaving it to the outside world to do it. SDGs have a nation state perspective.
Sovereigns wanting to remain relevant.
Paradigm shift. Awesome.
Standards as rule of law. Digital standards as equituy.
From Scott David to Me: (Privately) 10:51 AM Let’s convene with Jean after IIW to work on this.
From Scott David to Everyone: 10:53 AM Great stuff. Thanks for convening.
Humans first is an unfamiliar concept in the modern world.
We need to reestablish human auspices over human systems.
Identity is cultural enclosure.
Information is a dual use tech
From Scott David to Everyone: 10:42 AM Harm to data - concept like conversion of personal property possibly?
Start with harms/anomalies.
Engineers and lawyers can agree what is “anomalous” in a system operation.
Harms is starting point. Nice.
Data is the vector through which the harms are communicated.
Also money is the vector through which the harms are quantiied
Democratizing the dark web.
We are moving into the space. This is happening.
Leaving it to the outside world to do it. SDGs have a nation state perspective.
Sovereigns wanting to remain relevant.
Paradigm shift. Awesome.
Standards as rule of law. Digital standards as equituy.
From Scott David to Everyone: 10:53 AM Great stuff. Thanks for convening.
Humans first is an unfamiliar concept in the modern world.
We need to reestablish human auspices over human systems.
Identity is cultural enclosure.
Information is a dual use tech
From Shigeya Suzuki1 to Everyone: 10:56 AM Interesting discussion.. thanks.
From Scott David to Everyone: 10:57 AM I can beta test the test stack in my program possibly if useful
Tech stack Git hub as project management back end. Nice.

Chat from post -session
Technically feasible systems. Are they “reasonable?”
Reasonable according to whom.
Do tech people have awareness of users and other affected stakeholders.
Tech as defect system structure and law.
Need feedback mechanisms to encourage P2P speech.
What is policy inputs
What are “lawmakers” in the new period.
Are they formal legislators or are they actors themselves.

AbuGhraib prisoners have been called “legislators” since they teach us as humans what we will not tolerate as behavior (torture in that case).
Legal authority delegations.
Ambiguity versus law as concept engineering
Rhetorical engineering. Mere removal of ambiguity adds value to systems.
Ambiguity IS the energy that drives markets. Disambiguation generates derisking for future interactions and therefore value.
Monopoly AND Monoposony should both be examined!
Lots of unpacking to do here. First of all - ALL risks are in one of 4 categories. AAAA risk. Attacks, accidents, acts of nature, AI/ML. There are no other sources of threat/bulnerability. Each calls for different protections. Attacks versus accidental harm will have different profiles.
From Scott David to Everyone: 11:50 AM Lawyers get paid by the hour. Efficient resolution of matters is uneconomic. Is it data? What if data is a commons? Co management regime rather than enclosure regime? What if data is just a distraction. Is it co management of a risk commons?
UN SDGs don’t attend to side effects among SDGs/
What do humans have in common as a species that might be used as basis for common rules?

OpenID Connect 4 Identity Assurance

Wednesday 10J
Convener: Torsten Lodderstedt
Notes-taker(s): Torsten Lodderstedt

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

The session presented the current status and direction of OpenID Connect 4 Identity Assurance (OIDC4IDA). This specification defines an extension of OpenID Connect for providing Relying Parties with verified Claims about End-Users along with metadata about the processes used to gather and maintain these claims. E.g. in accordance with a certain trust framework. OIDC4IDA is intended to be used to verify the identity of a natural person.

The working group plan to enter 3rd implementers draft review and voting soon, which is the prerequisite for final publication later this year.

Slides are available at: https://www.slideshare.net/TorstenLodderstedt/openid-connect-4-identity-assurance-at-iiw-32

Jacob Dilles proposed to allow RPs to use handles for pre-configured eKYC requests. I filled an issue for discussion by the WG (https://bitbucket.org/openid/ekyc-ida/issues/1245/pre-configured-claims-ekyc-requests).

Dynamic Data Economy: Digital Identity, Authentic Data Flows, Data Mesh and other Dragons

Wednesday 10L
Convener: Robert Mitwicki
Notes-taker(s): Robert Mitwicki

Tags for the session - technology discussed/ideas considered: DDE, HCF, Data Mesh, KERI, OCA

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

Session was held by Human Colossus Foundation folks who described the vision for DDE which is developed within the Colossi network around the foundations.

Dynamic Data Economy is a roadmap towards fair, decentralized and authentic data economy. Many times people are referring to blockchain technology as a revolution within digital space. But often they actually mean something more profound: the promise of Decentralisation brought by blockchain. A Dynamic Data Economy brings decentralization outside the technology realm into digital solutions for any economic actors. It does so by decentralizing all layers of the ecosystem:

- Decentralized Governance - no administrative entity fully controls and sets the rules, Individuals, organization and government are sovereign on their data Governance.
- Decentralized Architecture - physically decentralization of resources running that network. Economic actors keep control of their data storage solution according to the level of security required.
- Decentralized Logic (Data) - if you cut the system in half it can continue working and data is not damaged in any way, e.g. no need for total ordering.

No blockchain fulfills all those requirements and some none at all. And this is a problem for sensitive areas (e.g. identity or data portability) Then the agreements on sets of principles, protocols and rules to fulfill those requirements are “add-ons”.They are not in the system by design and thus weakens the overall solution Thus the Human Colossus Foundation (HCF) is seeking for opening up discussion and lead towards standardization efforts to ensure that the decentralized technologies already existing brings to life a Dynamic Data Economy for all with and without blockchain.

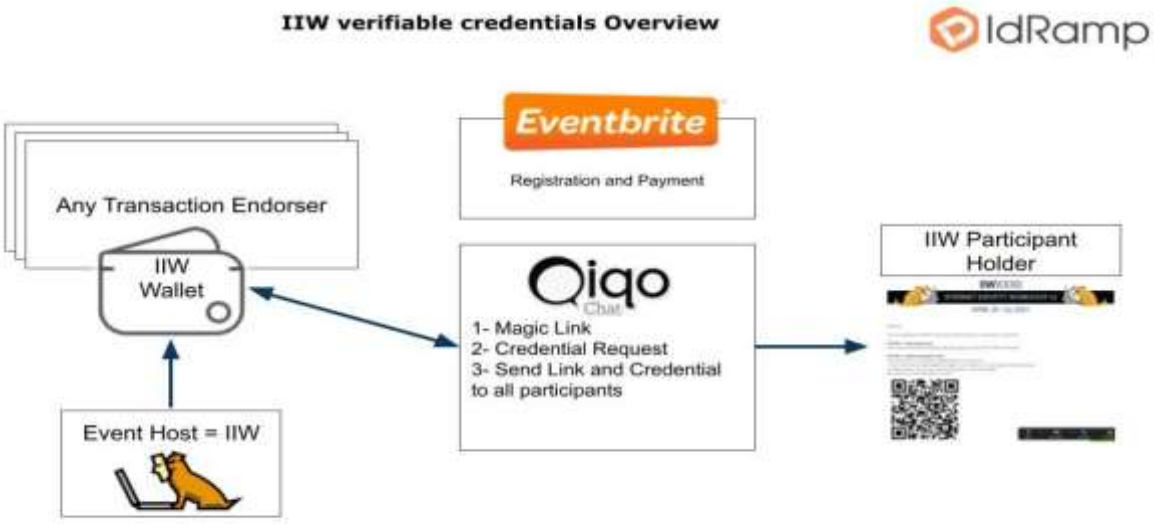
IIW Verifiable Credentials - Decentralized VC Integration with Eventbrite & Qiqo.Chat. This Session will review the implementation process, lessons learned, and community discussion on related use cases.

Wednesday 11A
Convener: Mike Vesey, Karl Kneis
Notes-taker(s): Karl Kneis

Tags for the session - technology discussed/ideas considered:

- Verifiable credentials in production
- Decentralized identity
- Practical adoption
- API free Integration across services and applications

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:



Video Demonstration
https://youtu.be/qe3RauZvC0o

Notes

- IIW is now issuing verifiable credentials for registration and access to live events managed through Qiqo chat forums.
- Credentials, verification proofing, and integration provided by the IdRamp Zero Trust ecosystem management platform and APIs.

- IIW credentials are interoperable with a range of standardised wallet providers.
- Issuance and proofing are incorporated seamlessly within the existing customer communications flow.
- Integration with Qiqo and Eventbrite required no significant development effort.
- The solution is operating in production and can be applied to any Eventbrite or Qiqo customer.
- VC registration and access is also available for stand alone Qiqo customers today.
- Deployment effort was completed in less than two weeks.
- Providing clear communication for end users was the most challenging task.
- The solution can easily be deployed with any ecosystem or service provider to increase security, HX and privacy protection.
- No code deployments are also possible using the IdRamp platform

About IdRamp
IdRamp is a zero trust ecosystem management platform. Protect your business with password free verifiable identity today.

Contact
IdRamp.com/contact
+1 (515) 808-2822
mvesey@idramp.com
kkneis@idramp.com

Group Credentials/Multi-Issuer Credentials

Wednesday 11B
Convener: Benji Kok
Notes-taker(s):

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

Current ssi solutions are geared to allow the issuance of a specific verifiable credential by a single issuer. There are use cases that would benefit from enabling the aggregation of multiple credentials into a single credential so that the holder can't delete sub credentials of the aggregated credential. Is it possible to implement such an aggregation while allowing the holder to present only certain sub credentials of the aggregated credential as required?

An example use case is the issuance of credit history credentials. If each creditor issues separate credentials, the holder can delete the "bad" credentials and only present the "good" credentials. By enabling all creditors to contribute separately to a single credit history credential, the holder must either delete/present the whole credential.

Rugged Identity: Resilience for Identity of Things to Bad Latency, Signal, Power, Physical Integrity

Wednesday 11C
Convener: Phil Wolff
Notes-taker(s):

Tags for the session - technology discussed/ideas considered:

Rugged, resilience, Identity of Things, IDoT, latency, signal, power, tampering, Mars, space

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

Problem: So, what happens when you can't call home to conduct an identity conversation? You're on Mars and the latency is long. You're in Haiti and the bandwidth is very limited during a storm. You're in a war zone and your signal is noisy due to interference.
Rugged Identity is hoped-for resilience from very long latency, noisy signal, low bandwidth, interrupted connections, very low power computing and radio, power outages, and attacks on physical integrity like device tampering.
https://wider.team/2020/12/23/2021ruggediomd/ Concerns for connected medical devices that work in remote locations, in emergency/crisis conditions, atop undeveloped infrastructure.
Solving these problems should bring curb-cut effects to all digital identity protocols. So medical devices still work in hospitals that block signals or homes where the router is overloaded.
Discussion:
Q. What breaks under these conditions?
Q. What can be done with existing tools and standards to enable greater resilience and more reliable recovery from disruption?
Q. What acceptance tests might verify that an identity system works offline and under stress?

DIDComm V2: Implementation & Integration [technical] (did: key and did:keri resolvers, seamless and partial integrations)

Wednesday 11D
Convener: Ivan Temchenko (Jolocom)
Notes-taker(s):

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

Technical session covering basics of DIDComm v2 Rust implementation (didcomm-rs), including JWM message format overview, JWE/JWM envelopes and key identifiers structures as well as cryptography usage. In addition we've discussed how key resolution of public keys happening from `kid` and `skid`

envelope header fields using plugable resolvers and private keys resolver using Vault Key provider in form of “Universal wallet” spec implementation [wallet-rs].

Later we’ve checked how that all works in demo: P2P chat application using direct mode and JWE encrypted DIDComm v2 messages in mixed key scenarios using did:key and did:keri identifiers and resolvers. In addition we’ve covered the option to send “KERI event log” as part of message header identifier to allow resolution of Document form it and then crypto material required to decrypt received messages.

Slides from the session:
https://drive.google.com/file/d/1dn5f2SqnCeQocOy5quJD9gpMPipKRmdC/view?usp=sharing

BBS+ Credential Exchange in Hyperledger Aries

Wednesday 11E
Convener: Timo Glastra, Karim Stekelenburg
Notes-taker(s):

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

Link to Presentation Slides: https://iiw.animo.id

ZOOM CHAT:
19:07:28 From Juan Caballero1 : so glad this is being recorded! let's publish this afterwards on DIF YouTube :D
19:07:56 From Jace Hensley : (It’s not showing that it’s recording for me)
19:08:02 From Deas Richardson : It is for me
19:08:04 From Dan Bachenheimer : it is for me
19:08:07 From Tania Barron : excelent that this is being recorded!!
19:08:08 From Artur Philipp : it is showing for me
19:08:09 From Jace Hensley : :thumbsup:
19:08:09 From Berend Sliedrecht : It is for me aswell
19:08:11 From camparra : Yeah it’s recording
19:11:11 From Andrea Reginato : Great, simple and clear way to present. I’m curious to know with which tool you made the presentation too :)
19:11:39 From Karim Stekelenburg : Deck MDX!
19:12:13 From Karim Stekelenburg : @Andrea https://github.com/jxnblk/mdx-deck
19:13:45 From Andrea Reginato : Thanks @karim!
19:17:21 From Sebastian Schmittner : looks better than the typical revealjs to me :)
19:18:06 From Karim Stekelenburg : It’s pretty neat indeed :)
19:18:25 From Sebastian Schmittner : I am sorry that I missed the first couple of minutes. Is there some working implementation out there to actually generate/work with these VCs shown currently?
19:18:58 From Troy Ronda : aries-framework-go is one of them.

19:19:24 From Karim Stekelenburg : The ACA-Py implementation will be merged in shortly
19:20:50 From Stephen Curran : PR: https://github.com/hyperledger/aries-cloudagent-python/pull/1061
19:22:02 From Sebastian Schmittner : awesome! We are doing some prototyping right now where we are using JSON-LD VCs with the americans, but, since we are also running a node in the HL Indy network of ID Union, it would be really great if we could bridge the Ocean here ;)
19:22:25 From Dominic Wörner : +1
19:22:48 From Drummond Reed : Watch out for those correlating DIDs!!
19:24:18 From Brent Zundel : we can make steps toward this in the "What's next for BBS+ LD-Proofs" session later today
19:24:32 From Berend Sliedrecht : +1!
19:24:41 From Karim Stekelenburg : +1!
19:24:44 From Drummond Reed : +++1
19:24:47 From Sebastian Schmittner : looking forward! :)
19:24:55 From Ajay Jadhav : Great work.. !!
19:26:34 From Micha Kraus : Is holder binding generally missing in all the current bbs+ based credential implementations?
19:27:18 From Drummond Reed : There is no private holder binding yet.
19:27:42 From Paul Bastian : Is this planned for BBS+?
19:28:28 From Berend Sliedrecht : slides are located at iiw.animo.id :-)
19:28:40 From Dan Bachenheimer : thanks
19:28:53 From Oliver Terbu : really amazing presentation. will the video be available?
19:29:01 From Karim Stekelenburg : Yes!
19:29:28 From Kyle Den Hartog : Yes, we've been working on private holder binding. Right now we're actively focused on trying to make the API designs "just work" so we've not fully exposed the capabilities yet. It's an in progress work item for us
19:29:29 From Deas Richardson : Very cool demo - love the interactive slides
19:30:46 From Dominic Wörner : On Private holder binding: https://github.com/w3c-ccg/ldp-bbs2020/issues/37
19:31:58 From matthewhall78 : For the new people Can you define BBS+ acronym?
19:32:10 From Daniel Buchner : It's three names
19:32:14 From Dan Bachenheimer : the htree inventors
19:32:30 From Stephen Curran : FYI -- Shaanjot Gill at BC Gov did the bulk of the PE implementation in ACA-Py.
19:32:36 From Daniel Buchner : Waiting for a new scheme to popup called SSS
19:32:43 From Daniel Buchner : Smith Smith and Smith
19:32:59 From Stephen Curran : Timo and Karim did a HUGE amount!!!
19:33:07 From Daniel Buchner : make life easy for us and name all cryptographers John Smith
19:33:08 From Berend Sliedrecht : +1!
19:33:21 From Bart Suichies : I thought they were all called Alice and Bob?
19:33:34 From Daniel Buchner : Alice and Bob Smith? :)
19:33:39 From Bart Suichies : use the arrows
19:33:42 From Catherine Nabbala : Yes
19:33:44 From Matteo Marangoni : Hit bar
19:34:32 From Dan Bachenheimer : thanks
19:36:12 From Sebastian Schmittner : that's really amazing! the JSON-LD credentials finally comming to the Hyper Ledger world is really amazing :) thanks a lot for your work on this!
19:39:01 From Brent Zundel : +1 to collaboration
19:41:12 From Drummond Reed : But BBS+ does not support predicate proofs right now. So no more "older than 18" until predicate proofs are added back in.

19:43:04 From matthewhall78 : github.com/Hyperledger-labs/business-partner-agent has the feature on the roadmap to allow a proof request to be from multiple credentials.
19:43:23 From Christian Bormann : you could use the aries-go on mobile, correct ?
19:43:41 From Sebastian Schmittner : the BPA is also aca-py based, isnt it?
19:43:49 From Kyle Den Hartog : Yeah they might have it in there as well
19:43:55 From Kyle Den Hartog : They've got support in their CHAPI work
19:43:59 From matthewhall78 : Yes, BPA is ACA-py based
19:44:05 From Troy Ronda : You can do a gomobile build, but we havn
19:44:24 From Troy Ronda : 'T played with this enough - needs more contributions :).
19:44:46 From Troy Ronda : (Referring to the aries-framework-go question).
19:45:06 From Troy Ronda : We have also done this in the browser from a Web Wallet based on a WASM build.
19:45:45 From Bart Suichies : Demo of that will be tomorrow
19:46:09 From Víctor Martínez : yes!
19:46:11 From Kyle Den Hartog : Good to hear! Nice job on getting that stuff in there. I wasn't sure where things were at for ACA-py moving to abstract resolution architecture
19:46:19 From Karim Stekelenburg : +++++ for the universal resolver work!
19:46:43 From Ajay Jadhav : That's nice..
19:46:45 From Kyle Den Hartog : Has the abstract registration architecture been done yet?
19:47:36 From Troy Ronda : Aries-framework-go supports universal resolver and also DID resolvers that you define and work as Go code.
19:47:50 From Troy Ronda : We have Go code for our Sidetree-derived methods, of course.
19:48:00 From Kyle Den Hartog : Figured you guys had it in there
19:48:23 From Daniel Buchner : I'm so tempted to ask our teams to just use this if it supports ION LOL
19:48:39 From Drummond Reed : Good temptation!
19:48:43 From Dominic Wörner : I'm trying to get a least did:web support into ACA-py [19:43] Woerner Dominic (RBCH/PJ-IOT)
ich mach grad nebenbei did:web support (wink)
https://github.com/boschresearch/aries-cloudagent-python/tree/feature/didweb
19:48:57 From Drummond Reed : Adding ION support should not be hard, no?
19:49:06 From Troy Ronda : Sidetree VDR library support: https://github.com/hyperledger/aries-framework-go-ext/tree/main/component/vdr/sidetree
19:49:07 From Daniel Buchner : Yeah, it supports all the right keys
19:49:13 From Balazs Nemethi : :)
19:49:16 From Daniel Buchner : so should be rather effortless, I would imagine
19:49:19 From Bart Suichies : hahahaha
19:49:27 From Ajay Jadhav : :)
19:49:28 From Bart Suichies : maybe there will even be specifications ;)
19:49:43 From Kyle Den Hartog : lol
19:49:45 From Daniel Bluhm : @Kyle no abstracted DID registration yet
19:49:56 From Daniel Bluhm : For ACA-Py at least
19:49:57 From Drummond Reed : specs? who bothers with specs??? ;-)
19:50:00 From Kyle Den Hartog : Cool thanks for clarifying
19:50:23 From Daniel Buchner : Spec-ges, spec-ges, we don't need no stinking spec-ges!
19:51:36 From matthewhall78 : badges
19:52:11 From Berend Sliedrecht : +1 Kyle!
19:52:16 From Drummond Reed : ++1
19:52:37 From Kyle Den Hartog : The technology is maturing and becoming a reality
19:53:04 From matthewhall78 : When is support for predicates coming?

19:53:10 From Oliver Terbu : do you have a link to the repo+branch (if it is a branch)?
19:53:21 From Leah Houston : I have been following this, and I am very grateful for this work (everyones work)
19:54:02 From TimoGlastra : https://github.com/hyperledger/aries-cloudagent-python/pull/1061
19:54:07 From TimoGlastra : @oliver
19:54:56 From Oliver Terbu : https://hackmd.io/@quartzjer/JWS_Sets
19:58:35 From Stephen Curran To TimoGlastra(privately) : You should stop the recording

State of SSI in Europe and Necessity for Network-of-Networks (convened by Sovrin)

Wednesday 11F
Convener: Andre Kudra (a.kudra@esatus.com)
Notes-taker(s): sankarshan

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

1. [Andre] Introduction and the role of Sovrin Foundation around the topic of SSI
    1. Focus of this session is around SSI in Europe (from business and related perspective)
    2. Hyperledger Indy and Aries technology stack

2. 'Network of networks' which has been a key concept at the Sovrin Foundation
    1. The topic is meant to be a conversation as an outline based on material information which can be shared publicly
    2. EBSI is one of the funded projects from the EU
        1. ESSIF is one of the projects in this portfolio - have issued a request for proposal for consulting (not in the network of networks topic but other areas)

c. Findy (Finland) - yet to go live. Has public and private partners.
d. Projects underway at Spain and other member nations in EU

Substantial funding behind Indy based technology stack deployments are being seen
. Germany has 3 major streams active in the identity space
    1. Gov digital (for public sector)
    2. ID Union - 2 fold - a project and a L1 Utility (as per the Trust over IP definition) project and Governance Framework; has started in 2020. Will be building a lot of use cases on Indy/Aries over a period of 3 years Includes EU member states and the 3 non EU nations. ID Union activity will have contributions to open source projects
    3. Germany is running an SSI pilot based on the Aries framework. First use case — hotel check in for business travelers (two data types: ID; corporate billing

address). German eID card will be used to generate a VC by issuing on behalf of the issuer of the eID card.

a. Mixed bag of projects and technologies which underline the topic/concept around 'network of networks'. Organizations will come up with their networks and interoperability would be something that is inbuilt.
    1. EU Commission has identified the necessity of making this happen. So no 'one blockchain to rule them all'. A cooperative approach would be needed to get into NoN - tokenisation, IoT etc have been part of the requirements
    2. 3 Sovrin member organizations have jointly created a position paper to address the necessity of this approach of NoN. This approach is endorsed by the Sovrin Foundation.
    3. Universal resolver, multi-ledger wallet etc are key components. A side-project to make a tangible NoN experiment is on the cards.
b. [Andreas] https://joinup.ec.europa.eu/collection/ssi-eidas-bridge/about
    1. [Alex Blom] https://vimeo.com/522501200
    2. https://gitlab.grnet.gr/essif-lab/infrastructure/validated-id/seb_project_summary
    3. https://github.com/validatedid/eidas-bridge
c. [David De Troch] How would permissionless NoN look?
    1. [Timothy Ruff] But then that universal resolver becomes a central point of attack, and of trust, defeating the purpose of the ledger behind it.
    2. [Rouven Heck] It would be great to discuss a network of network, which is blockchain agnoistic… rather than Network of Indy networks …
d. GLEIF can act as trust anchor for legal entity identifiers across SSI ecosystems. This doesn't solve the credibility problem though. LEI can be issued to businesses as well as CEOs and executives within those organizations.

Semantic Interoperability With Layered Schemas and Linked Data

Wednesday 11H
Convener: Burak Serdar
Notes-taker(s): Burak Serdar

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

This session is about layered schemas as a tool for semantic interoperability. Traditional schemas like JSON/XML schemas define structure. A layered schema allows semantic annotations to be added to data. They also define a mapping from an input representation to an abstract data model represented as linked data. The use cases shown during the session include

- Semantic harmonization in a data pooling use case
- Machine readable data use agreements
- Granular consent as layers
- Deidentification
- Data transformations
- Data capture with different layers for different jurisdictions/locale

- Health data (FHIR)

Link to slide deck provided by Burak Serdar: https://layeredschemas.org/docs/presentations/

Identity Escrow - Accountability AND Privacy

Wednesday 11l
Convener: Sam Curren, Ken Ebert, Suresh Batchu, Kiran Addepalli
Notes-taker(s): Kiran Addepalli [kiran@digitaltrust.net]

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

Link to Slides: https://docs.google.com/presentation/d/1kHoDZ-4BFjjJpVL1NnQVRMZdzTIDCddg31Q23Q4AwAw/edit?ts=606f6eab#slide=id.gd2e8d1fc4c_3_4

1. Can the escrow hold the "Proof of the information" as opposed to the information itself.
2. Mortgage Service - might seem to be an authorization to access the data directly or the issuer present directly.
    1. What gets put into escrow is flexible.
3. Trigger event or a lockbox kind of capability. How is the claim released to relying parties? How does it eliminate mischief and false claims.
    1. There needs to be some accountability on the service provider to claim false releases. Automation may not be able to completely eliminate false triggers, some level of human intervention for complex cases.
    2. Contractual wrapper for
    3. Technical and legal framework for accountability.
4. Don't have data but key to unlock the escrow. So that no insider can unlock the data. Separating the data release from the encryption release would be better.
5. It is better to hold proof of data. Because of the risk and liability, it can create incentives to escrow providers.
6. We should chat about the CDDE (Community Distributed Data Escrow) that we have developed with UN, WEF, NYU Gov lab for data handling in disaster settings. Very related to this. Blind trust, etc. for self shielding.
7. Niels van Dijk - Encrypt the personal data with a future data - polymorphic pseudonyms one would encrypt using the keys of the future recipient. polymorphic pseudonyms one would encrypt using the keys of the future recipient.
8. In terms of using standard semantics for this (with receipts as a mechanism for escrow) then e.g. A contract notice receipt would have the rights for the contract associated - and the notice/rights are the escrow container (or semantic container)
9. Incentivizing the users to keep the data fresh with the escrow service.
10. Escrow is nice concept because of its "just in time" element of availability. NFT market would benefit from Identity escrow.
11. Escrow concept is also great to explain what we might see as a transaction receipt with a credit card. In which payment is shown in escrow - at checkout..
12. Legal interoperability across escrow agreements can be partial and still useful.
    Just like ALL contracts now have identical bankruptcy clauses, whatever the context. All escrow agreements may share a subset of terms.

1. Agree. Seems like this could be very useful for Estate Planning/generational transfers etc, where there are not only multiple parties involved in a transaction, but transactions that unravel over time?
2. Acting from beyond the grave! Like trusts. Beware the rule against perpetuities!
3. Guardian in case of incapacitation
4. If escrow takes liability without knowing what data is being saved. Daniel - Verifiable Encryption . If the key is the one that is generated by the Escrow service, then they know that they…https://link.springer.com/chapter/10.1007/978-3-540-45146-4_8
5. There needs to be uniformity of standardized contracts. That constitutes governance itself. Constructions , bankruptcy clauses, like standard contracts. Escrow can be provisional things but practices will grow and become institutionalized down the line.
6. Community initiated distributed escrow - every holder of the data and escrow agent. If there is a trigger, the data sharing.
7. Scott ! - that's why we should use internationally standards semantics for the Escrow framework .. Identity Governance like a PII controller.
8. Cryptographic commitment - potential substitute for escrow service.

Humans dwell in cure periods for default. We defaulters all!
Contracts can be formed by mere humans among themselves (P2P duty creation) - Public laws cannot
Contracts require less process and are more nimble. Public law isn't
No administrative procedures act for contracts.

1. Harder to pre-consent. Query whether might have a problem under the EU "derogation" position on GDPR. Does pre consent to trigger of release of Identity constitute an unpermitted "too general" consent?
2. If contracts cannot be understood, there cannot be a meeting of the minds. If there is no meeting of the minds, the contract is voidable from formation. How deal with unconscionability issue in consumer/citizen facing contexts. Interesting note: Most people have no idea how escrows work.
3. Standardized contracts are reviewed by an "AI Lawyer".
4. So, here is another possibility. Identity escrow makes it possible to instantiate GDPR type rights IN ANY JURISDICTION. We can form GDPR community in US?
5. So, here is another possibility. Identity escrow makes it possible to instantiate GDPR type rights IN ANY JURISDICTION. We can form GDPR community in US?

Links that came up during the call:

• https://onlinelibrary.wiley.com/doi/abs/10.1111/j.1430-9134.2001.00173.x

• https://dhh1128.github.io/zkpcreds/trust-paradox-rebuttal.html

• Feedback loop into privacy law:
https://kantarainitiative.org/confluence/display/WA/Privacy+as+Expected%3A+UI+Signalling+a+Consent+Gateway+For+Human+Consent

https://link.springer.com/chapter/10.1007/978-3-540-45146-4_8

KERI: Centralized Registry with Decentralized Control (KEL & TEL) + DEMO

Wednesday 11K
Convener: Robert Mitwicki
Notes-taker(s): Robert Mitwicki

Tags for the session - technology discussed/ideas considered:

KERI, TEL, Verifiable Credential Registry

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

During the session it was shown how KERI (Key Event Receipt Infrastructure) - can help to crate Centralized Registry with decentralized control mechanism and keep control of the state of any arbitrary data. In the examples it was shown how the TEL can help to build Verifiable Credential Registry (revocation list). Generic architecture allows you to implement it for any arbitrary data and for example have a mechanism for registration of human readable identifiers.

OpenID Connect: Session Management vs Privacy

Wednesday 11M
Convener: David Waite
Notes-taker(s): David Waite

Tags for the session - technology discussed/ideas considered:

OpenID Connect, Session Management, Logout, Privacy, Browser Policy

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

Slide/Presentation Contents Provided by David Waite:

Session Management vs. Privacy
Strategy for OIDC synchronized sessions in a world without third-party cookies
IIW 32 - Session 11

What is a Session?

Wiktionary:

the period during which a user is logged in or connected.
Web sessions are made up of the local policy, corresponding business logic, and state around continued access.
For a relying party with existing session semantics, also respecting an OP session is challenging.

Applications track state in several ways:

1. Via cookies
2. Via a backend database
3. In browser memory

OpenID Connect thus has three defined systems for session management

1. Front-channel Logout
2. Back-channel Logout
3. (IFrame) Session Management

Front-channel Logout

Lets the OP redirect the user to the RP with an event that says “log the user out”

But:

- The user must hit the OP in order for logout to begin.
- No guarantee the message will get there
- No guarantee the message will be actionable if it does
    - E.g. cookie loss, difference in logged-in-user on RP
- No fraud/malicous party protection
    - those who steal cookies tend to not honor these messages

---

Back-channel Logout

Lets the OP say, “log this user out” via an event on an API call to the RP.

Even allows you to block access by multiple filters:

- a single session identifier
- a subject across all sessions (administrative lockout)

But integration into many RP systems is difficult; there may not be a place

on the back-end that allows this sort of clean-up.

(IFrame) Session management

A session management system mostly made for single page apps, but can include appropriate logic (cookie/state deletion and window changes) to work for more static apps by injecting javascript.

1. RP opens two iframes; one for itself, one for the OP
2. The RP iframe sends a postMessage asking for session status

3. The OP iframe has custom logic for processing, and responds with a status - unchanged, changed, or error
4. On changed, the RP considers the id_token invalidated and does a passive authentication to fetch another one
5. On passive authentication failure, represent the user as 'logged out' until they initiate a manual reauthentication.

To recap:

- Front-channel logout is simple
  - …but brittle and doesn't give good security guarantees
- Back-channel logout is robust
  - …but difficult to implement/support, can still miss signals
- Session Management is useful for some apps
  - …but is broken in many browsers

On their own independent schedules, all browsers have either broken or have plans to break state sharing via cross-site iframes to limit user tracking - arguably making the Session Management approach unusable.

Distributed Token Validation API

Maybe we already proposed something useful here!

Like session management, it is based on polling for changes rather than pushed events, and the events dont indicate a user/administrative action (logout).

But differs in some key ways:

- API-based rather than IFrame-based.
- API call can be made by both front-end and back-end application components
- Correlates a session solely via embedded sid/jti in JWT
  - rather than browser storage-based session_state value
- Communicates about the validity of the identified token, not the status of an OP session.

It avoids the word session - which often implys a volume of business logic and assumptions about behavior to the parties involved.

Instead, tokens are merely invalid. Token can be invalidated for any reason, such as:

- Attribute family_name changed due to HR processing a name change request
- User added to ACL; OP wants to repeat authentication to reevaluate rules
- User-requested logout action; OP requires explicit reauthentication
- Anomaly signal from MDM system; OP requires passive authentication to check device compliance.
- Detection of malicious action; OP is invalidating tokens and has no plan to reissue.

In all these scenarios:

- The OP takes on the burden of implementing the business logic they require
- The RP simply asks if they should still make trust decisions off of existing tokens
- If the RP can no longer trust a token, it fetched a new one with escalating levels of user impact
- The OP controls token changes/ user interaction based on needed level of excalation

---

Flow

1. Retrieve issuer iss and sid (or jti if no sid) from JWT
2. Resolve issuer + identifier to a HTTPS endpoint representing the session
3. GET endpoint to determine if token is still valid
4. If token is invalid, stop depending on it and fetch another one.

This works for all JWTs with issuers and identifiers (such as use for resource servers checking for revoked access tokens)

How to use

For id_token validity checks:

- A confidential client can call its own privately hosted infrastructure to check
- A public client (javascript app, mobile app) would need a public-facing API endpoint to call to perform the check

With public clients, checks would be user experience - security would be to revoked access to backend / revoked access tokens.

For JWT access token validity checks:

It is not likely clients would proactively check if tokens issued to them are still valid.

Rather,

- A protected resource can perform a check for revocation as part of validating the JWT
- A token introspection endpoint can perform the check before returning successful results

---

“But wait - I can’t make my infrastructure depend on the availability/latency of remote API calls!”

The API is designed to work in a decentralized manner*

You can have a local API endpoint providing a cache in the data rack/VPC/pod, and scale up to your performance requirements rather than relying on the performance/SLA of external infrastructure

---

You can use a forward proxy with HTTP caching to the OP server/endpoints.

You could also define a synchronization mechanism between parties to do more sophisticated updates - state checkpoints, push notifications, etc.

A system based on distributed consensus was defined - it is based on the Swirlds Hashgraph system (precursor to the public network Hedera Consensus Service)

- This should map to other consensus systems like Hyperledger Fabric, albeit with some trade-offs
- The reference implementation lets you disable use of consensus networks and operate purely locally/in memory.

Also imagined was a synchronization method via webhooks and shared signals/secevents, and a method that pulls deltas of revocations, CRL-style.

There are provisions for pushing information from the RP about the local agent's usage of a token.

E.g. - "the user is actively performing actions on the RP site".

The hashgraph implementation uses this to define a sliding inactivity window for automatic revocation.

Issues with Distributed App approach

All participants in the distributed system can see other participants' update to distributed state.

- tokens associated with a session can be correlated by time
- partially defeats pseudonyms
- wound up sharing sid values across RPs for windowing for efficiency with that in mind
- state update by a provider infers OP/RP relationship, that a user is interacting

Even ignoring user privacy, this still leaked competitive information, e.g. "this enterprise seems to have a ton of seats for these SaaS products"

Other approaches like HTTP caching, secevents did not have these issues: communication was scoped between the OP and individual RPs.

Questions?

Credential-Based Login To A Pico-Based Application

Wednesday 11P
Convener: Bruce Conrad
Notes-taker(s): @convener

Tags for the session - technology discussed/ideas considered:

Verifiable credentials, authentication, picos, pico-based application

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

Link to slides provided by Bruce Conrad: https://bruceatbyu.com/s/HRDDSiiw32

We presented the slides, and then a discussion ensued. Adrian directed us to his session (10H) and shared with us his experience with GNAP and OAuth. Vic asked many thoughtful questions. Johannes shared some insights on graph databases and a project called ObjecTime.

Before recording started, I stated the title of the talk and gave an introduction: the motivation for the work, that we used picos to create a Domain Data Store proof of concept, which is a "fully-sharded" database. The point of describing it here is the authentication using credentials.

Read slide 3, "Motivation" highlighting BYU's login page, shown on slide 4.

Rough transcript of recording follows:

So, the motivation for this work was to do something using verifiable credentials. [slide 5] The BYU sign in currently is a typical single sign on page that you saw on the previous slide.

For a long time we wanted something other than Net ID and Password. Vic, I remember you were in a meeting in IIW 29 where we had an Aries agent embedded in the user's browser so that when the user went to a web site they had visited before, they were just "in." Then we looked at it in more detail six months later [in IIW 30] and discovered that there was a fatal flaw with that because the browser could throw out the agent and its state, including its private keys and connections and so forth whenever it wanted to basically and so we temporarily abandoned that approach. Although I think it would make a good hybrid with the one I'm showing today. I enjoyed working with Trinsic. I know both of their employees who are with us today. Thank you gentlemen, and their studio login works in the way that I wanted to do. So, imitation being the sincerest form of flattery, I've implemented what they did, showing that here and hoping to advance that.

The application that I wanted to demonstrate is what I call a fully-sharded database. BYU wants a community facing Human Resources domain data store, which means that other organizations on campus may wish to access HR data and so far they've been doing it by dipping directly into the production transactional database and that's not a good idea. And so, they have a team implementing a proof of concept using Postgres. And, I'm using picos to implement a fully-sharded alternative proof of concept.

[Slide 6] So going back to why use picos to build a web application? Each pico implements an API on the Internet, and it encapsulates its state and synchronizes requests which makes it fairly easy to use for

coding. A pico is also extremely cheap to run in the cloud. I have tens of thousands of them running in three different pico engines on one EC2 instance, and without my educator's discount, that would cost me $8 a month. We also have a thousand picos or so running in our Manifold pico engine on another EC2 instance that I'm not billed for but I imagine it costs a similar amount. The marginal cost of adding another pico is vanishingly small.

Also, new behavior can be added easily to a pico. So any pico can become an Aries agent, for example, just by installing some rulesets in it. And, finally, picos extend the current trend from monolithic applications to micro services, which we'll look at on the next slide. The next step I've sometimes called nano services. Perhaps they could be called "pico services." They're much smaller, because instead of one domain of a business becoming a micro service, carved out of the monolith, each entity of that domain, the micro service domain, becomes a pico and contains its data and code.

[Slide 7] So the transition from monolith to micro services… so the idea is that the monolithic application for say a university that handles human resources and student registration and classroom scheduling is split out into micro services. And each micro service contains the business logic for its portion, and this kind of micro service here [indicating one of them] would just contain business logic because it doesn't directly access data. The data itself will be partitioned vertically so that all of the HR data would go into this database [indicating the leftmost], all of the registration data into this one [indicating the middle disk], and all of the classroom scheduling data could be in a separate database [indicating the one on the right]. So, this transition is in progress in our industry.

[Slide 8] Sharding is a little bit different. Here there is one tracking table in a database and three of the records in that table are on one database [indicating the top one] and two of them are on a different one [indicating the bottom one]. And that's called "sharding." It's used to increase availability. This particular example of sharding also is a hint at fully sharding because everything about tracking number 123456 is in a database by itself.

[Slide 9] If we shard a database completely with one service per entity, then here's a diagram of that as a graph database. Each one of these lower rectangles represents one employee of Brigham Young University. And then there is this other pico which represents a collection thereof. This is an abbreviated diagram as there would be tens of thousands of picos in this layer [indicating the picos at the bottom] and again each pico contains all of the data about that person and all of the business logic for interacting with them.

[Slide 10] So the way it becomes an application is that we add a ruleset to the "persons" pico so that [bouncing back to previous slide] it becomes besides keeping track of all the people, it also *is* a web application. Now where I became interested in authentication is that if I want to demonstrate this to my colleagues at BYU I'm going to have to place it on the Internet whereas now it's running on localhost. A pico engine can easily be moved to a docker container in the cloud. That part isn't the hard part. The hard part is that the data it contains shouldn't be seen by anyone except members of the BYU community. And so to get that authentication, I created a separate application that runs in the BYU single sign on environment, named YCred.byu.edu, and its sole purpose is to certify, using single sign on, that the individual visiting the web site is a BYU community member. And then I partnered with Trinsic and host, with them, an organization also named "YCred" that I can use to create credentials and verify them. And then again added a ruleset to the "persons" pico to handle authentication. So just going back to the diagram [previous slide and indicating the top pico] now the "persons" pico is three things: it is keeping track of all of the people (knowing where they are, being able to produce an address for them); it is a web application; and it is an authentication verifier. [returning to slide 10] Any questions to that point?

[Slide 11] We'll go into this in more detail, but here's the overview. The overview at the top level is that when you use a web application, you sign up once and you login many times thereafter. Signing up involves requesting a credential, seeing the offer of a credential as a QR Code, scanning that with a self-sovereign identity wallet app and then you now hold a credential. Logging in is when you go to the application, you're required to prove who you are. You see that request. You scan *that* code with the same wallet. The wallet will suggest a way to prove what you need to prove. You press the "present" button, and then you're in the application.

[Slide 12] So, the sign up process. To request a credential you authenticate using BYU's current single sign on mechanism, which we saw earlier involves a Net ID and Password or one of the federated IDs, and then the web application, YCread, running in that environment, offers you a credential, by redirecting to a Trinsic page, as we'll see, and you scan that QR Code with a wallet and you now hold it.

[Slide 13] So, these are the players [indicating items along the top]: you are visiting [circling stick figure]; through your browser; the web application; there's also the YCred application we spoke of; and the Trinsic API. So the way it work is that you visit the application, the pico responds with the index HTML page, but before it shows you anything, it detects that you're missing a session cookie, and so it redirects to the login page, which we then see [slides in from right]. It looks like this, and you have the option of either logging in with a password, or with the credential. To Steven's point about having the application be available to people who don't even have a smartphone, this option allows you to do that and migrate people towards the credential based method of authenticating. If we saw this login page for the first time, and we're someone from IIW we would of course want to login with the credential, and not having one yet, we would click on this link [indicating YCred link]. That would make a request to the YCred application and it would show a page [slides in from right] that certifies that you *are* a member of the community, with a particular Net ID, and you could then request a verifiable credential. That request goes through the YCred application, which on the server-to-server side issues an API call to the Trinsic API to issue the credential and then we redirect you to the Trinsic "You've received a credential offer" page [slides in from the right]. I've mutilated the QR Code here because for all I know, Michael or Beto you could tell me, for all I know it might still be valid. I was hoping no one on the presentation or watching the recording would grab the credential for themselves. In any case, once you've done that, your wallet now has the credential.

[Slides 14-17] So the next few slides are just a repeat of that without animations. You go to the login page. You request a credential; you ask for it to actually be presented to you, and you scan it to accept it.

[Slide 18] Any questions to that point? Logging in, you visit the web application, and you'll see a proof request, and you'll scan and present the credential, present the proof, and you're logged in.

[Slide 19] So, the same players, and the flow is a little longer [mousing along the left line top to bottom]. After logging in, you use the application and then your logout. But I'm going to zoom in

[Slide 20] just up to that point. Notice that YCred plays no further role. It was only used to gain the credential the first time. So when you return to the application, you see the login page [slides in from right] just exactly the same as before, but this time you're going to click the "Login with credential" button, which will let the application know that you need a verification. That will, server to server, use the Trinsic API to get that, and will return, and here the application generates the QR Code itself rather than redirecting you to the Trinsic page. Notice the "Scan with digital wallet" is displaying "checking in 13 seconds". That's because it might take you quite a while to pull out your phone and scan the code, and so the web page, the login page, is polling for the verification. To do that, it asks the application. The application asks Trinsic for the verifications, and it will continue doing that until you actually scan the code. Then it will poll for

verification, and redirect you to the app [slides in from right]. With that amount of interaction, you're now logged in. You'll see your Net ID up here [indicating blurred area at top right], you'll have the option of logging out when you're finished or use the application however you plan to use it.

[Slides 21-24] The next few slides are for the benefit of someone watching this later to see without animations. To see the login page. You choose to login with the credential. You scan the QR Code. And you're in the application.

[Slide 25] So that is my demonstration. And, I'm open for some questions and discussion now.

Steven, is that the kind of thing you're looking to do? [Steven] Yeah that is what I'm looking to do. With the exception that I'd like to find a way to do that same approach where you're verifying a credential, but without relying on a smartphone. Don't want … and everybody else using traditional username and password. I'd like to have everybody on a SSI digital identity from some vendor. Some of them will have wallets on their phone, some won't have phones. I can have a cloud based solution I guess, but that's what I'm looking for.

Asking Michael or Beto to jump in with their impression of that requirement? [Michael] I would say, yeah, you can definitely do that with a cloud wallet. We didn't implement the login flow with one of our customers, but they do have a lot of customers who don't have smartphones, and they have flip phones and stuff like that and so we did provide cloud wallets for them and they were able to manage all of their transactions by going to just like a public cafe or whatever, get on the computer, login with SMS to their cloud wallet and then they were able to access all their credentials with their cloud wallet. So something similar could definitely be done and you could have some sort of place to host a cloud wallet and could receive and present proofs on that application on that cloud wallet. So that could be a way, but then you run into that problem like to login to their cloud wallet they still have to do some sort of login.

[Steven] I see that as the equivalent of logging into your phone. You still have a login of some sort to get into your wallet. One login for many things. I'm curious what the UI, the experience might be like. I mean this is driven by bar code scanning. What the comparable model would be if I were not using a phone that I would be scanning QR Codes with?

[Michael] Another way could be with a connection, and then you can send a request to verify some credential through the connection. With push notifications on the wallet, you could have a little badge come up, saying hey someone's asking for this credential and you can prove it that way. Another way, Bruce, with the Manifold picos, they can establish connections just by pasting in a link, so I'm curious as if maybe something similar could be done with a proof. If you could paste in a link to a proof. I'm not entirely positive if that works the same as a connection.

[Bruce] Yes, ideally, there should be something to reify or make manifest the connection that a visitor to a web site has with the application. Your application space is government I think you said, and the citizens of a jurisdiction have a relationship with the government, and it would be nice if that relationship was identified by a connection of some kind. For this particular usage where I just want to share a proof of concept with a few colleagues for an hour I didn't go with the connection approach, which although that does make more sense. Instead I used Trinsic's connection-free presentation of a verifiable credential because that's just a shorter chain of events.

[Michael] And Steve just said in the chat that a QR Code is just a URL which is right so we could just paste whatever the URL is.

[Vic] I think this is similar to what Steven was asking about. For this piece where when I want to login, I have the credential in my wallet, and this QR Code that I'm scanning, that's proving that I am the controller of that wallet? Or the controller of the credential? I don't understand that last step quite.

[Bruce] It's kind of like when you go into a bar or buy a product in a store and you have to prove your age. You would pull your wallet out, pull out your driver's license and show it to them. So what you're proving is that you have in your possession a wallet which contains a driver's license, which has a particular birthdate on it and a face that looks like you. So with this kind of verification you're proving that you have in your control a smartphone that you've been able to get into because you know the key code to get into it or you satisfy the biometric to get into the phone and that you have a wallet on that phone that contains a credential that can be used to prove what you need to prove. That's a pretty long way of saying it.

[Vic] And you're trying to do that without establishing any sort of permanent connection.

[Bruce] Yes, for this particular application, since it's a very transitory demo, I didn't need to establish a connection first. Steve would need a combination of what I showed a year and half ago, I guess two years ago now, of you're using a browser that has in it a connection to the web application, so that when you use that browser to visit the web application you're in because the connection is there and, if the browser has thrown the information away, then you would fall back to this approach, and if you didn't have your mobile phone with you you'd fall back to the user ID and password. That's where I'm headed anyway.

[Steven] I may be asking the same question that was just asked, but I want to understand. In this model, the verifier is not double checking with any issuer that it is in fact a valid current proof. The fact that the holder has it and not looking for any assurance from the issuer to ensure that it's valid.

[Bruce] That's a really good question. It appears to be that way on the surface, but in fact the proof is constructed in such a way that the credential I present was issued by the issuer. So it's not something I can put together in PhotoShop. That's built into the triangle that we talk about: the issuer, the holder, and the verifier. The issuer and the verifier don't need to have a direct connection because the issuer has cryptographically signed the credential, and the verifier can look up their public DID on a ledger and use that to verify that the credential hasn't been modified and that it was issued to the person who claims to be holding it. Did I get all the detail in that right, Michael?

[Michael] Yes, that is correct.
[Vic] What if the credential has been revoked. Is that also
[Michael] That's also taken into account. Yeah, it will check if that credential has been revoked. And, if it has then you don't get logged in.

[Bruce] Yes, the proof would fail. In my particular case, again to streamline this, because my use case is so punctual, I chose to have it be a non-revocable credential. But my understanding is that Trinsic, who we partner with, right, to do the actual issuing and verifying, they say they can handle revocation. And Michael just confirmed that. Adrian, do you have any questions or comments about this process, or Beto?

[Adrian] Yes, I have lots. Unfortunately, I was picking up my granddaughter just as you were doing the demo, but if I can I can ask my questions. If not I can watch the video and contact you separately. I can try to reconstruct what our situation is.

[Bruce] Yes, I would very much like to hear your perspective. What we demonstrated is that you sign up and be given a credential which you would store in your mobile wallet and when you went to login you would be asked to present a proof that you would do using that credential in your wallet.

[Adrian] Right. So we have a much stronger constraint. Self-imposed, which is that we don't expect patients to have a wallet or even a DID. We only expect the requesting party, the doctors or family members or anybody other than the patient but controls the equivalent of the pico. In our terminology it's called a trustee -- it doesn't matter. It's in the cloud. And so we did not want to -- and there's a couple of reasons for that. One of them is that we model guardianship, you know for children and elderly. Again so we didn't want to have a one to one association between wallets and signing, right because that would confuse the guardianship issue. But also because we didn't want to introduce the equity issue of like was mentioned earlier that wouldn't have a smartphone or not everybody does. So what we're planning to do is try and avoid having the patient or the data subject or credential subject have either a wallet or a password, because people have too many passwords. So, one example of being able to do that is to send a "magic link." The way I sign in to Zoom, for example. Not Zoom, I'm sorry, Slack. I haven't used a password signing in to Slack. And what we do, then, given that at registration, which is a one time thing, they've given us an email address, then we have a place to send them a magic link in order to sign in.

[Bruce] Is that a one time use link, Adrian?

[Adrian] Well then this is why I wanted to talk to you [unintelligible] because ideally we're doing another thing, which is the patient does have to have the ability to manage policies--to manage the equivalent of a pico. And we model that as a progressive web app so that they can reuse the management interface as they would a web app that is part of the trustee or you know the pico, but the credentials and their policies that they're managing are actually not available to the trustee or to the pico except by decryption. In other words they can access the storage where we model encrypted data vault using the CouchDB right now and so we want to store real credentials, verifiable credentials included in the email or text message storage of the individual patient and then once they've connected to the web app the first time, then they can use the local storage associated with the web app which typically you can have up to fifty megabytes I think. All of this is described in session 10-H and there's a sequence diagram in there and on GitHub that describes pretty much everything I'm saying so if people aren't following me or are curious afterwards, they can just look at 10-H and they'll have a link to our GitHub, but anyway I've talked enough but this is what we're hoping to do and we could use a lot of help but this is how we're trying to basically hand off from the one-time magic link to the local storage which the progressive web app for a real credential the same way you have a real credential in that case. [Bruce: excellent; that's a fun idea] And we're also doing two other things than which were part of my talk which is for one we have web key management system in effect that we get for free because we're asking the guardian to sign in to Stripe and pay for their pico for their you know trustee monthly and so we store things like encryption keys that I mentioned for the data vault in Stripe as metadata and that's also where their email is -- we don't need it anywhere else. So that way, we're avoiding -- we're reducing the risk let's put it that way of running a bunch of trustees. So that and then as I mentioned, that we run CouchDB as a form of encrypted storage to where the pico can't write it. The picos can only *read* the policies and the credentials. It can decrypt them of course. But that way we reduce the attack surface for the thing which is in the cloud because only the client itself has the unencrypted version of the credentials and the policies. They won't actually be in the wallet as I said. If the client has a wallet great but we don't assume that. But this is all laid out in our session notes. So what's your reaction to all of that?

[Bruce] That's very interesting. I'm going to go study it. And right now while I give a chance to Tomislav, Cam, Johannes, Steven. I didn't see you earlier because of the way I was doing my Zoom session--I thought

it was just five or six of us. Someone else jump in with some questions or comments while I look up the link.

[Steven] Adrian, can you put the link to your session
[Adrian] No, I'm driving
[Bruce posts link to Adrian's session in chat]

[Vic] Bruce, I have a question back to the beginning of your presentation where you're talking about this sort of pico container kind of model and I'm wondering you know since the picos contain state then do you see them getting down to the component level in an app. A typical web app would have a bunch of components inside that app that all have their own state, and a lot of what you're doing in React or one of these other things is that you're managing these components, so I'm wondering how granular you think picos could become?

[Bruce] That's a really good question, Vic. Thank you. And that's part of the art and craft of using picos in creating an application. That is to decide where the entity boundaries are. And we in our lab over the years have taken several different positions on that with the different experiments we've done. But I think we've been happiest with the ones where we went very granular, very fine-grained and when you can identify something then you wrap it in a pico and then have it relate to other picos. I interrupted someone

[Adrian] Oh, I just wanted to mention. I've been following picos since pretty much the beginning. We've done a lot of work in this direction in trustee and [unintelligible] and that's why I mentioned we needed a progressive web app in order to manage as a policy management UI in order to manage this granularity. Now what we do which nobody else does including Solid and I don't think picos is we build around GNAP [unintelligible] and that's why GNAP is moving away from OAuth--it's unforgiving, but what we do is to model the relationship around what you guys are calling picos as the relationship between resource servers and authorization servers and the critical thing there is that when you look at something like Solid for example they don't expose the API that goes between the authorization server and the resource server, you know where they store it and that creates a real limitation because you can only [unintelligible for a long time [Vic: must be in a tunnel]] so what I'm saying is we build on this concept that we started out with that there is a separation -- a standards based separation -- between the resource servers and the authorization server and that applies to the individual that is otherwise the controller of the pico or the trustee and to everybody else that wants to interoperate with them. My observation has been that projects such as Solid with their pods and many others maybe picos which I haven't kept up with recently, don't expose that interface and thus they make the same mistake that OAuth makes of assuming that the resource server and the authorization server are under the control of the same entity. And a huge amount of complexity and a lack of scalability and you know everything else happens. But as soon as you adopt the UMA model or the GNAP model then the relationship becomes you know understood. Tractable. Then all you're left with is how do you design the policy management interface that is the thing that drives the authorization server. And how it relates to requests for access to resources, and you no longer have to put in the apps as part of the bundle as well. You can now just treat apps as just another resource server that has access to data in plain text. So to put it another way our world is divided between two different kinds of resource servers: those that have encrypted data and those we call encrypted data vaults and that's aligned with what we're doing in W3C and DIF, and those we call resource servers which are like traditional OAuth resource servers except we've moved to GNAP.

[Bruce] Thank you very much for that, Adrian, and thanks for the link. I'm going to read that and learn more about it. Tomislav, I believe that you are also involved with Trinsic? [[Tomislav] Yes, I am] So, I just want to take the opportunity to thank you for the API service that you provide which enabled me to do this.

[Tomislav] Absolutely. My pleasure. Bruce, thank you for being constantly with us through the version of the APIs. It really means a lot, having applications in production especially in the APIs because it helps shape us, you know in the future of the services.

[Bruce] Johannes, Steven, Ian? [pause] Okay, so this session has been recorded and it begins with about fifteen or twenty minute slideshow demonstrating what we have done and then the rest of the recording will be us talking about alternatives and asking questions.

[Adrian] Anybody who wants to help us [unintelligible for some time[Vic: I hope that was with the software and not about them driving … call 911, I'm not sure here]] anybody who wants to help us code any of this kind of stuff in the standards domain …

[Bruce] Understood. Thanks for that invitation

[Vic] Bruce, when you were describing how you were setting up the pico architecture, with all those different HR records, you were saying you were creating a graph. Did you actually use a graph database for that piece, instead of a NoSQL, or is it still NoSQL

[Bruce] That's a good question, Vic. It's a trick question, because I consider picos to be very natural graph databases. But they don't have the kind of tooling support that something that calls itself a graph databases would be expected to have

[Vic} And do you, is it typical with a pico to, you might want to have a graph database running alongside it? To get that extra tooling or reporting, because basically they're throwing a lot of events into an event stream and then you need a lot of times to report on that event stream, and this was a question that came up for us a lot. It's like do we add the graph database after the fact, or do we build it with a graph database

[Adrian] Can someone explain how a graph database works in picos and in this context? That would be helpful to me.

[Bruce] A graph database models data as nodes and connections between them. And for that reason, I take the middle road of saying what I have developed as a collection of picos is in fact a graph database. Because each pico contains the state for a particular entity and manages the relationships that it has with other picos. So, it is nodes and edges. And if Beto were still here he could describe his use of picos to satisfy a computer science class assignment to do a graph database. And, I see Michael nodding [Michael: I think Beto actually is here; Beto: yeah, I'm here]

[Adrian] You're saying that what we're calling policies of an authorization server is actually a graph and when we design a policy management user experience, that would be captured better with a graph database rather than a NoSQL database like what we're using with CouchDB.

[Bruce] That's a good question, Adrian. I would have to know more about the details of the policies themselves and how they're applied to give you a professional answer. I'm stuck in a particularly strange universe where I liken everything I encounter to picos. I eat, sleep, and breathe picos, so that's basically all I do.

[Vic] It does sort of start looking that way. Everything sort of looks that way after a while. But it is an interesting question because I think in a graph database, in many ways you're building the database in

order to get the reporting that you want, right? And one of the things with a graph database is that if you basically know where you want to enter the graph database then following the connections becomes super fast and so it allows you to report on these huge datasets that there really is no other easy way to report on.

[Johannes] I've gotta jump in here because in a previous life I actually wrote a graph database, so I have some opinions on the subject of graph databases. The thing that I just want to mention is that there is one thing that is very strange to me in identity land. Somehow we are representing a lot of the data that we have with very simple structures. Like name values and stuff like that. But the identity data we have is highly structured. There's much of a graph than anything you can represent flat. Take for example something as simple as a name. I'm a person and have a name, but that's not actually true. The name by which I'm called is different on the context: in Germany I will use my doctorate in front of my name which I prevent the Americans from doing, you know my son calls me Dad or sometimes calls me other things, you know so it's highly relationship based and the natural structure for representing these kinds of things is a graph. Right? You have things and relationships between things and you have depending on how you look at it you have different ways of annotating this. You can color your graphs with various kinds of things. You can have properties. You can have the relationships with different types and constraints and all of that and then I just actually yesterday re-read this paper that Kaliya wrote a little while ago about the various data formats that they were fighting over against which one should be used and thinking you know you're all missing it. I'm coming down on the JSON LD part but this is not really structured enough yet. It needs to be more structured. So it's a little bit

[Adrian] Well, let me jump in here, because, [he went quiet] Oh, you can't hear me? [Vic: you keep dropping out] I'm not moving anymore; I'm sitting still. What I'm saying is, we create -- a lot of people do this -- we create a separate DID for every service relationship that they have. And then, people want to relax that constraint, and either adopt a pseudonymous identity or a de-duplicated identity in many cases. So, there needs to be in our world -- I'm not talking as a private individual -- in the SSI world, there needs to be a language, a way to talk about this relationship, this continuum between starting out relationships with you know what some people used to call link secrets or hierarchical deterministic keys in the blockchain context. So, it sounds to me again like how this is about logging in to the picos, right and identity relationships amongst picos. It seems to me if we could use the kind of stuff you're talking about, these concepts, to help illuminate the relationships as we travel the DID relying parties that would be really really interesting.

[Vic] Bruce, aren't you dealing -- this whole thing is kind of -- comes down to, how do you interface between pico-land and non-pico-land? Right? Because if I am represented by a pico, then the login is trivial. But if, for whatever reason, I don't have a pico or the thing I'm connecting to is not a pico, then you gotta go through all this other stuff to make up the difference. Am I getting that, close? We're talking about a "pico gateway."

[Bruce] Yeah, it is true that one pico talking to another pico, they're talking the same tongue as it were and the interface to the outside world is basically the way as we've currently implemented it uses HTTP as a transport layer and so the outside world, and so a pico can publish a web hook somewhere and the outside world can visit that URL to cause an effect in the pico and the pico has the full power of HTTP RESTful API that it can use to act on the world outside of it. We've also thought about using email gateways so that pico could receive email and send email and other transport mechanisms. Another thing worth mentioning is that the pico can -- we saw in the demo (those who were able to see it) that we had a pico that represented the collection of all the people in the HR system, each one of them represented by a pico, and it was also a web application, and it was also a relying party (in OAuth terminology) for the login,

although the login was by verifiable credentials. Any pico can also become a full-blown Aries agent, and it does that without losing any of its other abilities. Speaking just briefly to any programmers in the group -- no most of them have dropped off -- a pico is the kind of object you always wanted when you were introduced to Java or C++ because it has its own thread of execution -- it doesn't borrow the thread of the application momentarily, and then pass it off.

[Johannes] By the way, did you ever come across -- years ago, a tool out of Canada -- a tool called ObjecTime? [Bruce, no I never did] You may want to look -- I never knew what happened to them -- it was a start up that came out of a telco, was factored out, and they were creating an object-oriented version of Horel (sp?) state charts and there was a nice tool and eventually they got acquired, then they got all spun up it was so many levels into IBM I think -- I don't know what happened to the tool but I knew the people very well who did this. The basic structure -- it was a telco kind of thing -- so it was all state machines, but an object-oriented version where you could create new objects with state machines that would communicate with messages, sort of CSP-like. And so, the reason why I bring this up is because that is the ultimate graphical way of describing the content of your picos [Bruce very interesting; do you have a link?] Let me look it up [inserts link: https://en.wikipedia.org/wiki/ObjecTime]

[Bruce] And it feels to me like we're winding down, energetically, so those who have to drop off feel free.

[Adrian] I think we're just getting started!

[Vic] So, Bruce, once you have the ACA-Pico, you have a pico with an agent in it, a wallet, do you switch all the communications you have happening over DIDComm.

[Bruce] That's what Phil Windley has planned for the future of picos. Where now they enter into a two-way relationship by exchanging channels [addresses] so each one has a channel to the other, he wants us to morph it so that that connection is a DIDComm connection. [Vic: a peer DID connection] Yeah a peer DID connection based on peer DIDS.

[Vic] Would you find that the overhead then, of having an agent and a wallet, is significant, or does it still make picos very lean?

[Bruce] That's a good question. I ask that question as well. I'm not sure when it's going to happen because we're no longer employing students. We don't have the wonderful effort of Beto and Michael and their colleagues allowed us to do a lot. We don't have that kind of manpower any more. So, I don't know, and I'm going to be doing a stress test soon, and I'm going to be requiring the data for all sixty thousand BYU employees [and students] and we'll see how well the pico engine holds up to tens of thousands of picos. The last time we did it it seemed to bear up fine. And then the next experiment as you say will be to replace the connections with DIDComm connections and see what that does.

[Adrian] So, the point I could make here is that we spent a year and a half or two as part of the DID standards process as we were getting the standard out trying to figure out for privacy reasons what kind of service endpoints and the reason it's relevant to this question is because you can build around either service endpoints being messaging endpoints, like DIDComm, or you can build around service endpoints being authorization servers, like GNAP and you don't really want to build around both because we came to the conclusion that just A) for interoperability reasons, we came to the conclusion that for privacy reasons we only wanted to expose one service endpoint, if any, per DID. And this went on for a long time. This was studied as part of vocabularies and then as part of privacy and a number of other things. So, my religion and I'm not saying I'm right at all -- as with any religion -- my religion is that building around messaging

instead of authorization services, is a mistake. It's not that you can't do it, but it's too low level, because the reason for the messages is generally because you gotta pass a request and you're gonna get back an authorization token of some sort to use somewhere else. You need that level of indirection in order to scale these conversations [Vic: how do you discover?] Probably just another resource server. In the world where I am, where I model the way health records go between clinics, hospitals, insurance companies, and patients' families, it's a very diverse universe where people don't control most of the places that have their health records. You know some of them are controlled by government, you know like MediCare records that we've accessed; some of them are controlled by giant corporations where huge, and some of them are individually controlled, like Apple Health or you know individual apps and so in our world, which again is OAuth based, all the resource services are not protected by some identity-based mechanism, they're protected by OAuth, other than the ones we control where we can use GNAP, but again the world is large out there, and so I'm talking too much, but that's my conclusion anyway, my religion.

[Bruce] Thank you for sharing that. We're probably going to go off and learn on our own, and if we come to the same conclusion, then we will regret not becoming one of your adepts.

[Vic] Thank you for your discussion. Always impressed by the creativity of this, and trying to put them into a real world scenario. We've got to get you some more students!

[Bruce] Haha! Thank you. Thank you, Johannes, for your suggestions, and Adrian, thank you so much for sharing your wisdom and your religion with us, and thank you Michael and Beto for listening in from Trinsic and for your work there. And thank you Ian and Brent for sitting in

Git as Authentic Data Creation Tool (a.k.a. What Happened to did:git? a.k.a. Independently Verifiable, Secure, Developer Sovereign, Open Source Software Supply Chain)

Wednesday 12A
Convener: Dave Huseby
Notes-taker(s): Dave Huseby

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

This session covered the evolution of thinking from the initiation of did:git at IIW April 2019 up until now. I recently chose to deprecate the did:git proposal in lieu of a new project to update Git to use provenance logs for identifier management in Git repos. I recently wrote an article describing the proposal: https://dwhuseby.medium.com/universal-cryptographic-signing-protocol-for-git-42e7741b8773

and the current proposal is here:
https://github.com/TrustFrame/git-cryptography-protocol

This is an exciting project that will bring decentralized identifiers to software creation to give us end-to-end secure and verifiable software delivery.

Veres One (did:v1) Rubric Evaluation

Wednesday 12B
Convener: Joe Andrieu
Notes-taker(s): Erica Connell

Tags for the session - technology discussed/ideas considered:

Veres One, DID Rubric Evaluation, DID methods, DIDs,

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

Link to Joe Andreiu Slide deck: http://legreq.com/pres/v1.rubric.iiw.2021.04.21.pdf
Link to Evaluation Rubric: http://legreq.com/media/rubric.v1.2021.04.20.pdf

- What we did
  - Reviewed current W3C draft
  - Found criteria that express Digital Bazaar's rationale
  - Identified potential new criteria to cover new elements
  - Refined criteria to better address Veres One distinguishing features
  - Shared with cohort
  - Engaging cohort for additional feedback and insights
- What we learned
  - Rubric still in infancy
  - Need structure-variable questions
    - 1.3 Separation of Power
    - 4.6 Consensus layers
  - Enforcement (initial draft of real questions)
  - How do we talk about trade offs from one wallet maker to another?
    - Evaluations are focused on the method
  - What about adversaries?
    - C. Allen identifies 27 adversaries (including forgetting password)
    - Particular methods are designed to address particular adversaries
  - Questions and criteria are young, still a learning curve
    - Learning the rubric
    - Learning each method
  - Need better tools for community engagement
    - Criteria discussion
    - Custom rubric development
    - Shared rubric evaluations
- Questions/Comments:
  - Looks like NIST (Common Criteria)
    - Evaluating security of systems
    - https://en.wikipedia.org/wiki/Common_Criteria
    - https://www.nist.gov/publications/common-criteria-launching-international-standards
  - Others have encountered the same challenges
    - Sometimes questions do not match to use cases

        - Multiple evaluators have differing opinions on how to answer questions
            - Helped discussion
        - There may be value in comparing evaluations
    - How much effort for this evaluation?
        - Rough estimate: under $10k for billable time
        - But there was familiarity with there system, so learning curve was already largely met
    - Tricky, esp with governance
        - How the blockchain is constructed
        - How things are agreed on for protocols, etc
        - And therefore hard to answer certain questions
    - Ad industry has been developing this stuff for the last 18 months.
        - Cookies are going away, so new developments (these kinds of rubrics)
        - Focused on who gets to do business and under what terms
        - How disconnected technologies and concerns of the single sign on problem and the media measurement problem addressed in advertising is.
    - Privacy Rubric could be developed? That evaluates privacy, not DID methods
    - Privacy interest group had a hard time with how DIDs go (learning curve issues)
        - Shouldn't have a privacy problem baked it, but that assumption skirts the heavy stuff
        - “Web shouldn’t have an identity layer”, but single sign on is an important aspect
        - Ad world is moving to a single sign on kind of approach in the absence of cookies
        - There are lots of opportunities here to take the tech into a practical use area
    - Invitation to take this work and campaign it a little more across the W3C
    - Props for the titanic work to get this out, and same for DID:web
        - Governance framework, for example
    - Needs to be a living document for it to be useful to the community at large
        - Criteria will not be static
        - Community-wise decentralization ala wikipedia is a possibility
    - The learning curve cannot be eliminated, yet there is opportunity to streamline some other aspects of putting this together to make future evaluations easier

Notes from Chat:
11:31:06 From Erica Connell to Everyone : http://legreq.com/pres/v1.rubric.iiw.2021.04.21.pdf
11:36:36 From Erica Connell to Everyone : https://w3c.github.io/did-rubric/
11:37:40 From Erica Connell to Everyone : http://legreq.com/media/rubric.v1.2021.04.20.pdf
11:37:56 From Eric Schuh to Everyone : https://github.com/WebOfTrustInfo/rwot9-prague/blob/master/draft-documents/decentralized-did-rubric.md
11:43:24 From Erica Connell to Everyone : http://legreq.com/media/rubric.v1.2021.04.20.pdf
12:00:11 From Joe Andrieu to Everyone : https://en.wikipedia.org/wiki/Common_Criteria
12:20:27 From Joe Andrieu to Everyone : https://www.youtube.com/watch?v=DVK5G9DIKf8
12:26:45 From ns to Everyone : oh Hi, I'just hopped in because I was curious - I was one of the evaluators that worked on the did eval with Markus Sabadello. Thanks for the great talk :)
12:26:54 From Dmitri Z to Everyone : oh excellent!
12:26:59 From Dmitri Z to Everyone : we’re looking forward to reading that!
12:29:27 From ns to Everyone : It was an interesting challenge. Like Walid said its hard to fit all these different designs and sometimes methods targeted at some particular use case into the rubric.
I think this is an ongoing process and its great that different people are working on this coming from different angles

IDunion Introduction and AMA (there will be another one tomorrow!)

Wednesday 12D
Convener: Andre Kudra + available IDunion Crew: Adrian Doerk, Christian Borman, Christopher Hempel
Notes-taker(s): Andre Kudra

Tags for the session - technology discussed/ideas considered:

IDunion | SSI | Identity | Consortium | Cooperative | Germany | Europe | BWMi

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

IDunion enables self-determined identities based on Self-Sovereign Identity (SSI) technologies Hyperledger Indy and Hyperledger Aries. The aim of the IDunion organisation is to create an open ecosystem for decentralised identity management, which can be used worldwide and is based on European values and regulations. IDunion is also a project co-funded by the German Federal Ministry of Economic Affairs (BMWi) as part of the Showcases Secure Digital Identities program. We gave an introduction covering

- The IDunion consortium consists of 37 partners - other major partners have already signaled interest in participating
- Our solution is enabled by the distributed ledger technology (DLT) and the concept of self-sovereign identities (SSI)
- Instead of a central authority, trust is organized via a DLT network, which works as a decentralized PKI system
- In recent months, in addition to intensive research, we have developed a DLT test network including governance structure, 35+ use cases and numerous software components for the allocation, verification and management of digital identity data developed
- In the future, the identity network will be managed by a European cooperative in which every institution in the EU can participate
- In total, we are working on 35 use cases in the areas of eGovernment, education, finance, industry/IOT, eCommerce/mobility, IAM, and eHealth
- Focus points within the project are interoperability, involvement of municipal bodies and citizens, generation of everyday relevance, cooperations
- Implementation schedule: 2021 - Incorporation European Cooperative | 2022 - Productive Network | 2023 - Building Trust and answered questions.

LinkedIn @idunion | Twitter @IDunion_SCE | Mail contact@idunion.org

IoT Swarms + SSI in Constrained Networks

Wednesday 12E
Convener: Geovane Fedrecheski
Notes-taker(s): Geovane Fedrecheski

Tags for the session - technology discussed/ideas considered: IoT Swarms, SSI in IoT,

Low-overhead SSI constructs

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

Presentation link -- here.

Summary: This session was a discussion about three topics: IoT Swarms, the challenges of SSI in constrained networks, and preliminary results on how to overcome them. The results showed that, while a DIDComm message with a DID Document as payload used almost 1 kilobyte, a binary approach can be used to cut it to just about 200 bytes.

IoT Swarms enable resource sharing among autonomous IoT devices. The presenter mentioned some papers published in this regard [1][2], including one that analyses using SSI in IoT and Swarm systems [3].

One of the challenges identified by this last paper is the overhead of using SSI, which poses a challenge for adoption on constrained IoT networks. For example, while the Long Range (LoRa) communication, often used in IoT systems, only allows payloads of up to 240 bytes, a single DID Document typically occupies 500 bytes or more. Similarly, messages using DIDComm tend to use at least 1 kilobyte, which prevents its use on constrained networks.

The presenter then showed the results of his exploration to build a binary version of DID Documents and DIDComm, and presented comparisons regarding message footprint, as shown in the Figures 1 and 2 below.

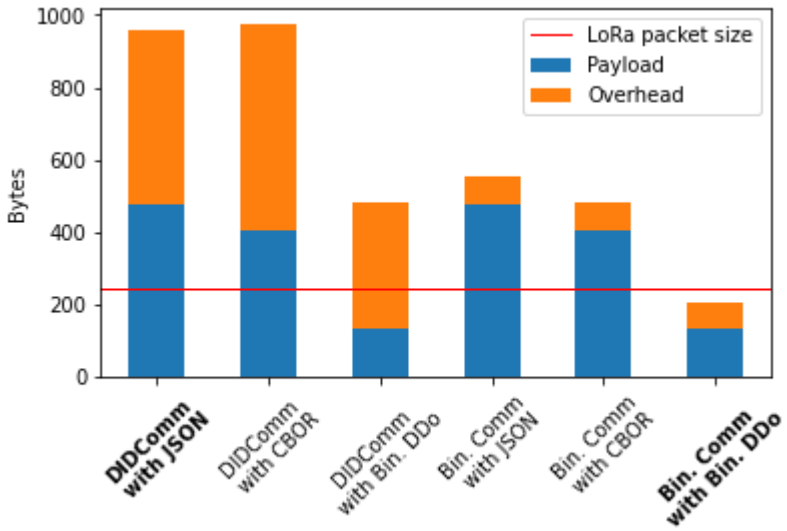


Figure 1. Binary versions of DIDComm and DID Documents are needed to allow transmission in LoRa networks. The payload, in blue, is a DID Document. The overhead, in orange, is the protocol overhead due to the message signature.

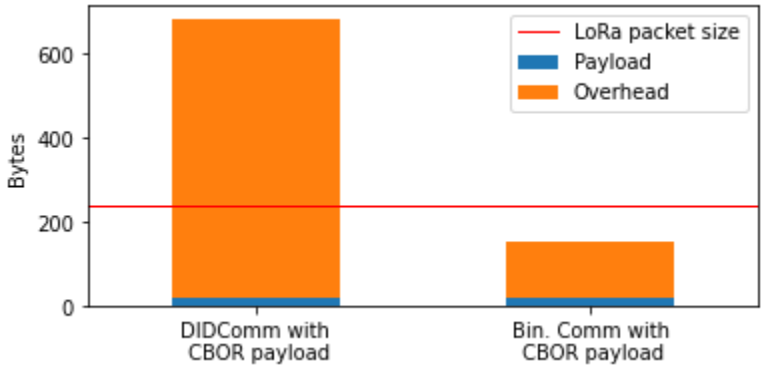


Figure 2. A binary version of DIDComm is needed to allow transmission of regular payloads in LoRa networks. In this example, the payload is a random CBOR-encoded message with 21 bytes. The overhead, in orange, is the protocol overhead due to the message signature and encryption.

In this session, the presenter did not share the methods, i.e., how to reduce message sizes, since they are part of a new and ongoing paper. Once the paper is published, however, the methods will be disclosed and shared with the IIW community.

[1] De Biase, Laisa Caroline Costa, et al. "Swarm economy: a model for transactions in a distributed and organic iot platform." IEEE Internet of Things Journal 6.3 (2018): 4561-4572.
[2] Fedrecheski, Geovane, et al. "SmartABAC: enabling constrained IoT devices to make complex policy-based access control decisions." *to appear* in the IEEE Internet of Things Journal (2021).
[3] Fedrecheski, Geovane, et al. "Self-sovereign identity for IoT environments: a perspective." 2020 Global Internet of Things Summit (GIoTS). IEEE, 2020.

Credentials Exchange - Figuring It Out - (Jello Bowl Death Match?)

Wednesday 12F
Convener: Kaliya Young - IdentityWoman
Notes-taker(s): Kaliya Young

Tags for the session - technology discussed/ideas considered:

DIDComm, Verifiable Credential Exchange, Aries Protocol, Bloom Protocol, Presentation Exchange,

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

Slides to complement this document - https://docs.google.com/presentation/d/1t4o6AXclqR7SqhGCbIJKVtYxh4fm_5mGT11MBx9K95c/edit#slide=id.p

The ultimate goal is to get to a clear exchange protocols.
Also to have a paper similar to this one that outlines the choice landscape that is and points to a convergence point - https://www.lfph.io/wp-content/uploads/2021/02/Verifiable-Credentials-Flavors-Explained.pdf
Good Health Pass is literally right now trying to figure this out and will "pick" solutions it needs to get implementations working in the next 30-90 days and point the whole industry in one direction.

We started out with this framework of understanding

Contextualizing VC Exchange in Layers

Verifiable Credentials (VC or VCs) is one of the key standardized components of decentralized identity. The VCs Data Model, defined at the W3C, is a universal data format that lets any entity express anything about another entity. It provides a common mechanism for the interoperable implementation of digital credentials that are cryptographically secure, tamper-evident, privacy-respecting, and machine-verifiable.

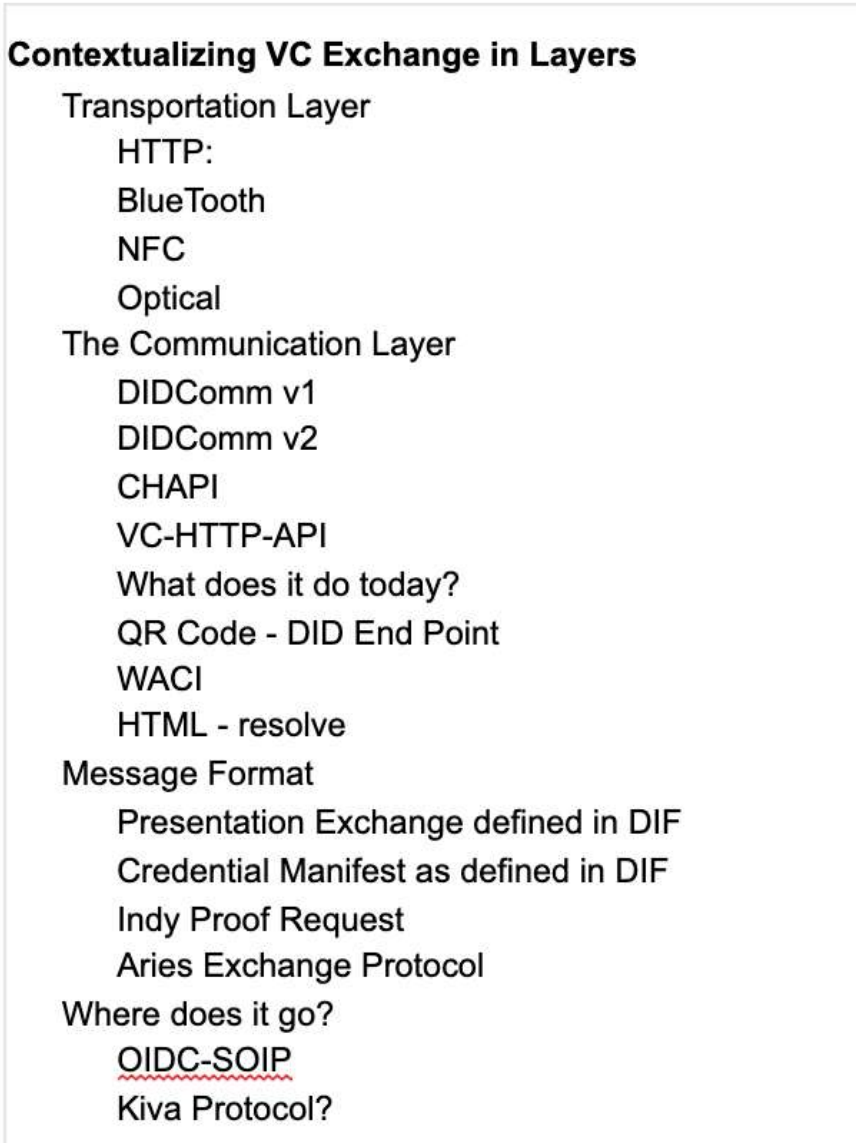
There clarity emerging on standards that are interoperable with one another for the VC format.
There is less clarity on the Exchange mechanisms.

One way that has been proposed to look at the exchange options available is to see them in different layers. .

The first layer is a transport these are well known and used in all sorts of scenarios.
Well known transports are HTTP, Bluetooth and NFC.

The next layer is the **Communications Layer.** Some of the communications protocols discussed in this paper are tightly coupled with particular transport modalities but others are not and can run on any transport protocol.

Message Formats
The final layer that is key to it all working is the actual format of the messages that move between the two parties to request and share credentials.



Transportation Layer
We are not going into detail about these because they are well known however for the sake of completeness and those not as familiar with them we will explain each.
HTTP:
BlueTooth
NFC
Optical (reading QR Codes)
The Communication Layer
DIDComm v1
DIDComm provides a mechanism of communication between agents of issues holders and verifiers. It can run on any transport protocol.

DIDComm short for Decentralized Identifier Communications was developed originally by the Aries community to leverage the inherent PKI of decentralized identifiers. It supports the formation of secure communications tunnels between two agents using peer DIDs (one of the DID

methods). Version two of the specification is being worked on in the Decentralized Identity Foundation.

Aries RFC 0453 - credential issuance protocol using DIDComm V1 data formats
Aries RFC 0454 - Present Proof protocol V2 using DIDCommV1 data formats

DIDComm v2
Work Item within DIF right now - envelope format with some other opinions we may or may want. Daniel Hardman gave vision - of parts that are done - leaving behind parts not done.

- DIDCom V2 Envelops JWEs (a standard that exists)
- Aries RFCs for payloads that go in JWE envelopes.
- Send envelopes over HTTP as a starting point

Question that is relevant.
Does it support all of the credential formats?

DIDComm has nothing to do with credential exchange - messages can be
Aires defines some credential formats that run on DIDComm

Put a message in an envelope.
DIDComm is the delivery service.

What do you put in the envelope - messages that exchange credentials.
Most relevant thing.
CHAPI
The Credential Handler API or CHAPI is currently a draft community group report developed by/under the Credentials Community Group at the W3C. At the heart of this model is a credential repository which is a Web application that can handle credential requests and credential storage on behalf of the user/holder. The API Is designed to support the transmission of credentials between a web based issuer and a holder with a cloud wallet (credential repository) that is visible in the same browser but in a different tab. It creates a "dumb pipe" between the two tabs in the holder's browser and permits the transmition of the credential effectively from one tab to another.

Browser PolyFil
Way to integrate into the CHAPI API.
Making some assumptions that are being passed around.
Browser API -

VP Request Spec - is assumed
JSON Data Model -

What we want is Standard data formats that you process in a standardized way.

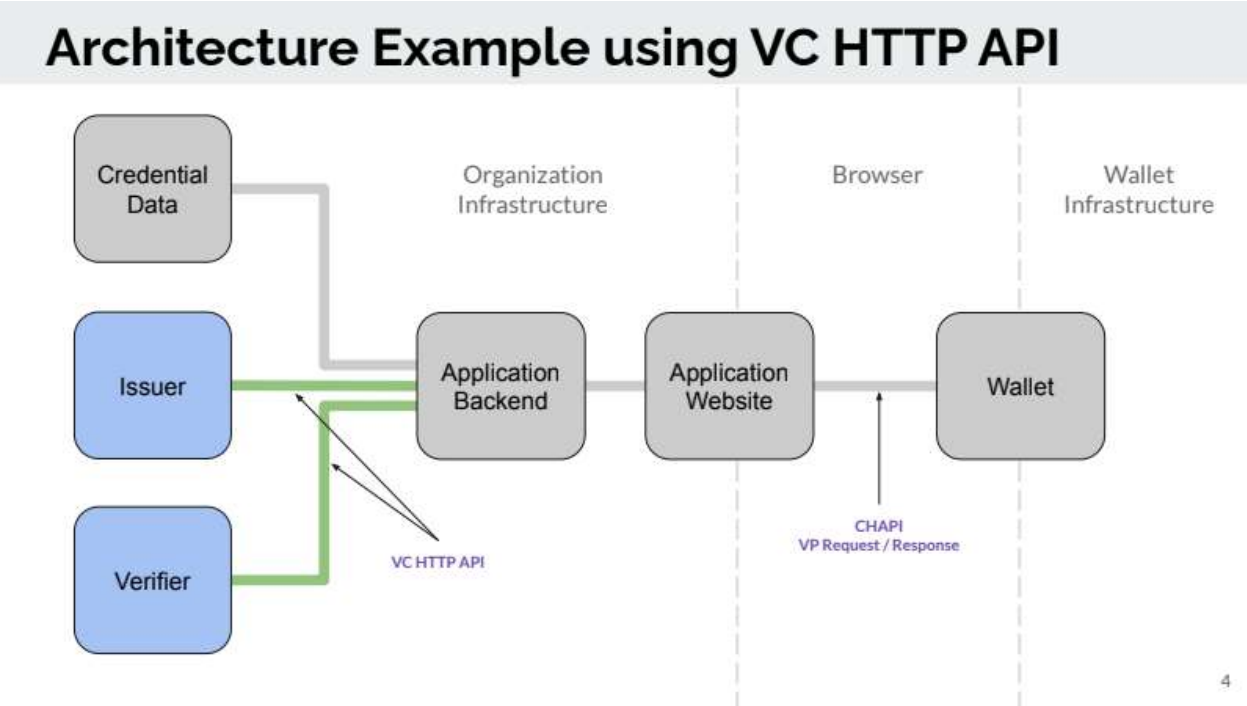
VC-HTTP-API (VHA)
The VC HTTP is a RESTful API specification (conforming with the OpenAPI 3.0 Specification) for constructing and verifying objects which conform to the Verifiable Credential Data Model specification.

A bit more about the OpenAPI 3.0 specification itself:

> The OpenAPI Specification (OAS) defines a standard, language-agnostic interface to RESTful APIs which allows both humans and computers to discover and understand the capabilities of the service without access to source code, documentation, or through network traffic inspection. When properly defined, a consumer can understand and interact with the remote service with a minimal amount of implementation logic.

This API is versioned in conformance with the Semantic Versioning 2.0 specification to prevent breaking changes between minor versions, and to allow for reliable testing and integration of implementations of this API within enterprise environments. This API provides a standard set of interfaces by which interoperability may be tested and verified by various parties who leverage Verifiable Credentials (VCs).

This slide, from a slide deck presentation by Manu Sporny to the W3C Credentials Community Group on 20 April 2021, explains the relationship of the VC-HTTP-API to CHAPI:



What does it do today?
Issuer APIs - internal - call back a end service -

Verifier APIs -

VP request spec - data model - powered by CHAPI.

VC-HTTP-API

Issuers are not directly exposed
Verifiers are not directly exposed

Same trusted entities - are part of the
Grey bar that doesn't assume you are in a web browser.

Message transport -

DIDComm does not assume a browser.

The reason there is a standardized infrastructure / verifier - is to drop a provider and get another one.
WACI
There are interactions between a wallet and relying party that require passing information between the two. WACI provides a standard for these interactions.
https://specs.bloom.co/wallet-and-credential-interactions/versions/v0.1.0/#status-of-this-document

WACI bound to JWT - signed. Could be JWE technically (would have to know the other parties DID and Keys - only optionally required here).

Fully supports credential manifest and presentation exchange.

Could be bound to DIDComm
Message Format
Presentation Exchange defined in DIF
Presentation Exchange is a protocol to support the interaction between holders and verifiers. It supports them being able to express what combination of credential the verifier wants or needs.
Credential Manifest as defined in DIF
Asking for a presentation
And asking proof to enable issuing a credential.
Indy Proof Request
Aries Exchange Protocol
Define the messages that go back and forth between
Issuer and holder (4 messages)
Holder and Verifier (3 messages)

Different formats (types of credentials) are different attachments in those messages.

DIDComm v1, there is AIP v1 and AIP v2 :)
Where does it go?
OIDC-SOIP
Self-Issued OpenID Connect Provider or OIDC-SOIP was created to take advantage of the fact that there are several 100,000 implementations of OpenID Connect on todays web. This method of exchange verifiable credentials leverages that infrastructure with a few small changes to support OpenID enabled sites to be able to accept verifiable credentials. Holders have wallets or agents that they use to interact with a system. The protocols to do this are being worked on jointly by the OpenID Foundation and Decentralized Identity Foundation.

Recommended Medium articles about OpenID, VCs, DIDs, and decentralized identity by Nader Helmy at MATTR:

1. Dec 15, 2000: https://medium.com/mattr-global/introducing-oidc-credential-provider-7845391a9881
2. March 14, 2021: https://medium.com/mattr-global/the-state-of-identity-on-the-web-cffc392bc7ea

Current MATTR spec for OpenID Credential Exchange: https://mattrglobal.github.io/oidc-client-bound-assertions-spec/

Raise up to the connect working group

More on the presentation side of things.

OpenID_Credential.
RP wallet holder.

Self-Issued OpenID Connect Provider

EXTENSION for OPs to Issue Verifiable Credentials.

Stand up your own openID Connect provider to stand up a wallet.
If you are doing a custodial system.
Google can be your OP and your wallet.
Progressive web application - where it is the OP itself. That web-app is able to be your wallet.

Original version of SIOP getting ID Token for a DID.

Future - heading…
Allow OIDC to support issuance of
Allow OIDC to support presentation of VCs.
  Aggregated Claim Usage - determine how VC flow to hold from OP to RP.

OpenID Foundation has been pulling things apart.
Separate spec called portable identifiers - could apply to SSI. (JWK thumbprints).

Chat about Aries. During issuance there is an implied assumption already authenticated - some sort of authentication
Way DHS Demo works - DID Auth request - VC presentation exchange.

DIDSIOP is a dead term - multiple extensions in openiD foundation - some will be relevent.
Issuance and authentication are two steps in some places and in other places they are one step.

Looking for a solution for I am a holder A - holder B - present credentials to drummond. Go to his website - start a flow from QR code - to initiate presentation flow. Not helpful to bring in concept of credential issuers.
Presentations of Credentials.
I don’t have an authenticated session - want to get to a presentation of a VC.

There really are entirely different protocols - how do you get it into your wallet. How do you authenticate to the issuer to assure rightful subject/holder - multiple ways to do that.

Entirely different protocols for issuance and presentation - can be different.

Are they trying to reach the same place.
Yes they are trying to do both.
Mutual Authentication - breaks with many of the protocols. It is a key feature of SSI.

Drummond - need separate issuance and verification.
Having a way to bind protocols into a single session - single Aires connection.
Sep

Daniel - learned something in ories comment - verifier work flow. Credential exchange is used - always issuance - never means proving.

We could collapse complexity out of Aires - aries of messages instead of API calls - should be described as message exchanges (thumbs up from Orie).

Brent - good conversation.

ORIE : We are on a whale watching expedition - largest great white shark - try and complete with largest killer whale. Trying to capture the presentation exchange

OpenIDConnect - is all of the largest IdP
Gravity Well - connected largest industry players - regardless of openID

Hunting helpless little seals.

Outside of OpenID Connect the next biggest “animal” is Aries protocols.

What if we had one or two things that are eating all of the seals. Is there another one?
Kyle - deployment architectures is what has made this so hard.

Presentation in offline - DIDComm only.
Reasonable assumption one online one not - DIDComm with OIDC.
Server to server - look in completely different scenario.

Quite like the idea of combining different things.
DIDComm as authentication mechanism - pre-issuance - from an OIDC issuer.

How do we combine things together to decide when they fit in different deployment.

FIDO?
W3C Data Model - do they care?

Competing things:
mDL ISO **18013-5**
MRTD -
Bloom Spec + Aries RFC - tried to describe without any baggage.
Simplified - message based - description of steps challenging getting proofs back.
Minor upgrade from Aries.
Implemented with

Other key thoughts: OpenID only usable by institutions.
Individuals asking individuals for proof - no implementations individuals have software in their control proof over

Combining things.

Things that limit aries

Use-Cases: OIDC for Verifiable Credentials - How Do You Want to use Identity Provider you Control?

Wednesday 12G
Convener: Oliver Terbu, Torsten Lodderstedt, Kristina Yasuda, Adam Lemmon, Tobias Looker
Notes-taker(s): Kristina Yasuda

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

Slides:
https://docs.google.com/presentation/d/1a0C4HvVYwwwDqSw3tgPNhy9Iqyufy9oZdnMgl7rQ9Vc/edit#slide=id.p

Mapping FHIR JSON Resource to W3C Vaccination Vocabulary: A Semantic Data Pipeline

Wednesday 12H
Convener: John Walker(Johnw.cci@lfph.io) & Mukundan Parthasarathy (Mukund@semanticclarity.com)
Notes-taker(s): John Walker

Tags for the session - technology discussed/ideas considered:

FHIR JSON to JSON-LD Conversion, W3C-CCG Vaccination Vocabulary,

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

Presenters: John Walker, Mukundan Parthasarathy
This work began in the ToIP Inputs and Semantics Working Group - Healthcare, FHIR Focus Group

Goals of the project effort:

- Transform a FHIR JSON formatted bundle into JSON-LD
- Support existing FHIR Purpose of Use (POU) tagging
- Support existing FHIR Consent and Security Label tagging (as required)
- Demonstrate jurisdictional specific data element support (e.g. EU DGC)
- Leverage W3C-CCG vocabularies

Link to presentation deck: https://github.com/SemanticClarity/oca-fhir-cli/blob/master/presentations/Comprehensive%20approach%20to%20address%20post-COVID19%20scenarios.pdf

Link to recorded chat file: https://github.com/SemanticClarity/oca-fhir-cli/blob/master/presentations/GMT20210421-183408_Recording.txt
Link to referenced GitHub repository: https://github.com/SemanticClarity/oca-fhir-cli

Kepler: Permissioned Replicated Storage for Decentralized Applications

Wednesday 12J
Convener: Charles Cunningham, Wayne Chang
Notes-taker(s):

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

Discussion of a new design for permissioned, replicated storage called Kepler, through the lens of common decentralized/distributed storage use cases. In particular, we examine the requirements that these use cases imply and how IPFS fails to meet them. Kepler combines an IPFS-like storage mechanism with auditable authorization policy updates (either smartcontract or verifiable-log based).

Slides: https://docs.google.com/presentation/d/1_oaVcx2IEbUEr9I-23Fd1e9ZMkIYtxpJe76zYq1oVZE/edit?usp=sharing

https://docs.google.com/presentation/d/1_oaVcx2IEbUEr9I-23Fd1e9ZMkIYtxpJe76zYq1oVZE/edit

Credential Marketplaces

Wednesday 12K
Convener: Martin Riedel, Stepan Gershuni
Notes-taker(s):

Tags for the session - technology discussed/ideas considered: VC Marketplace

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

Presentation:
https://docs.google.com/presentation/d/1WOXgHhgAwG0Im45pZkTAhsadpd8xbck0xjlnsuVGGhI/edit?ts=60803bc8

The goal of this session is to present the idea and get community feedback regarding this.

Credential Marketplace is quite high up the SSI stack but we want to start this discussion.

1. What is Credential Marketplace?
    1. We have a Trust Triangle of Issuer-Holder-Verifier. This does not need any centralized entity except schema hosting.
    2. However, we want to solve the problem of discovery of Issuers and Verifiers.
    3. *Example*: I'm traveling to a new country. I need to get what healthcare VCs are needed to go there, in an automated way.

4. How can we solve this without relaying on a centralized registry of Verifier requirements and Issuer capabilities?

2. How it works
    1. In order to discover issuers / vc types, there should be a registration step where issuers/verifiers actively OR passively provide metadata about their capabilities.
        1. **Credential Data** — can contain some filters or constraints on the data from within the VC. *E.g.* As a Verifier, I only accept passport VC from only certain governments: only German nationals.
        2. **VC Metadata**
        3. **Issuer Metadata**
        4. **Reputation mechanism** for credential issuers

b. Marketplace can also implement value transfer: paying for issuance by the verifier, for example. Even if they are part of different SSI ecosystems. This is optional but can help incentivize different participants.

3. Question: does marketplace need to know Verifier related information?
    1. For example, Where can I use the VC I have to get a service?
    2. Another example: What VCs do I need to get a certain service?
    3. Does the marketplace need to coordinate both sides to calculate the rep score?

4. The motivation behind desiging VC Marketplace is to provide seamless experience for the Holder, who just want to get a service and they don't want to struggle with trying to understand what VCs are needed and where that VC can be issued.
5. Approach for the WG is 3-fold:
    1. Come up with business use cases
    2. Standardized functional requirements
    3. Feed these requirements to existing working groups
6. Governance System
    1. VC Marketplace doesn't focus on this; it probably is independent of the marketplace.
    2. There can be multiple marketplaces: decentralized and centralized marketplace with alternative governance models.
    3. More marketplace with different governance models will create a competition and evolutionary path to develop different working governance systems.
7. [Scott Perry] For an Issuer there's value in getting an authority VC that certifies them as a valid issuer.

Global Survey Findings: Current State of SSI

Wednesday 12O
Convener: Gabriella Laatikainen, Ravikant Agrawal
Notes-taker(s): Ravikant Agrawal

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

SSI survey finding - current state, challenges and opportunities

- Survey was a collaborative efforts by University of Jyväskylä, Blockster.global and Trust over IP foundation
- More than 70 survey respondents
- SSI platform provider is ok but it should not be combined with network provider
- Risk: Slow technology adoption/ implementation / maturity
- Large VC issuance:
    - Healthcare (COVID credentials)
    - Revocation could be a challenge to be addressed
    - Education sector
- Milestones to be achieved:
    - Standardization
- Crypto payment
    - Many solution would benefit from global payments but this will further add the challenge of large business adoption SSI + Crypto combination
- SDO:
    - Not moving fast
    - More academic and research in nature

Security Event Tokens, Subject Identifiers, and SSE/CAEP/RISC Java Implementation

Wednesday 13A
Convener: Matt Domsch
Notes-taker(s): Matt Domsch

Tags for the session - technology discussed/ideas considered:

standards, Shared Signals & Events, RISC, CAEP, SSE

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

Matt presented an overview of the OpenID Foundation Shared Signals and Events Working Group, and his implementation of the object model in an open source Java library at https://github.com/sailpoint-oss/openid-sse-model/. Slides: https://domsch.com/IIW32/IIW32-openid-sse-model.pdf

Dale Olds asked if this code is or could be incorporated into the Springsource Authorization Server announced in 2020, or into other identity providers. Matt has not worked with any other products yet to include it - IIW is the first place outside the working group mailing list that this project has been discussed publicly. He hopes that by having an open source library implementation that adopters will be able to integrate SSE into their applications that much faster.

What's Next for BBS+ LD-Proofs?

Wednesday 13B
Convener: Brent Zundel
Notes-taker(s): Anonymous Wolverine

Tags for the session - technology discussed/ideas considered:

ZKPs, Selective Disclosure, BBS+, LD-Signatures

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

- What's next for BBS+ LD-Proofs?
- Implementation in Aries (https://iiw.animo.id/), Used in SVIP Plugfest
- Implementation of BBS+ in Ursa, Core of higher level implementations
- Features
    - Selective Disclosure
    - Signature blinding
    - Blinded messages (private holder binding)

- BBS+ LD Proofs uses this BBS+ scheme, MATTR provided spec
    - Combine privacy features with semantic world
    - Draft spec: https://github.com/w3c-ccg/ldp-bbs2020/
- What needs to be refined?
    - Private holder binding (https://github.com/w3c-ccg/ldp-bbs2020/issues/37)
        - Do not bind to link secret, bind to keypair. Make keypair per credential

How to participate?

- Read the draft BBS+ LD-Proofs spec

Hardware security binding?

- Not possible with BLS yet?

Is post-quantum secure?

- No. Pairing-based signatures are not post-quantum secure

Next steps:

- PRs for Issues 10 and 37 plus editorial pass to wrap up ldp-bbs2020
    - Brent will do PR for 37 https://github.com/w3c-ccg/ldp-bbs2020/issues/37,
    - Timo will do PR for 10 https://github.com/w3c-ccg/ldp-bbs2020/issues/10.
    - Invite everyone to suggest editorial changes
- Create WG at DIF for Crypto - first work item BBS+
    - Tobias will work with Rouven to get that started, https://github.com/decentralized-identity/org/blob/master/working-group-lifecycle.md
    - Brent and Tobias will work together to draft a charter

Future steps:

- Possible working group, or addition to DIF C&C WG for work on ldp-bbs2021

Saved chat from the meeting:
Dominic Wörner: Will you record the session?
Dominic Wörner: awesome
Nuttawut Kongsuwan: Will the session be recorded?
Kyle Den Hartog: Aries RFC 0454 - Present Proof protocol V2 using DIDCommV1 data formats
Kyle Den Hartog: github.com/w3c-ccg/ldp-bbs2020/
Kyle Den Hartog: https://github.com/w3c-ccg/ldp-bbs2020/issues/37
Brent Zundel: specification: https://w3c-ccg.github.io/ldp-bbs2020/
Stephen Curran: Anyone other than Tobias on this call able to go to the Cryptographic level that Tobias is avoiding?
Frederico Schardong: +1 for Stephen, I am also interested in learning that.
TimoGlastra: If you create a keypair per credential, can you still verify that multiple credentials were issued to the same person?
Stephen Curran: Isn't the subject / holder relationship a governance framework question?
Stephen Curran: I think all we're ever proving is that the holder is presenting.
Stephen Curran: "all we're ever trying to prove"
Andreas Freitag: I think he wants to avoid diving into elliptic curves and pairings :)
Stephen Curran: I don't want to dive in on this call. I want to know who else can work on this.
Kyle Den Hartog: Yup - it has to do with the subgroups I believe. I'd guess Brent may know it.
Andreas Freitag: @Stephen, ah OK
Michael Lodder: that sounds like a wallet protocol vs a VC protocol
Nathan_George: Isn't this a case of just adding an attribute that can be verified as specified by your data description?

Dominic Wörner: Without having hardware security wouldn't it easier for a holder to give/sell a credential to another party, because you don't have to give you're link secret as well, but only an "ephemeral" private key?
Michael Lodder: yes it is easier
Michael Lodder: But they could also share the hardware too
Drummond Reed: I'm very concerned that separate keys mean it is much harder to strongly prove credentials are issued to the same link secret. How would you solve that?
Kyle Den Hartog: The questions above are good examples where it's important for verifiers to have good adversarial models for the risk they're willing to take
Michael Lodder: We can use Enclave security like AWS Nitro enclaves, SGX, PSP, Trustzone to achieve similar security as HW
Andreas Freitag: @Tobias @Mike can we draw a sequence diagram to make it better "explainable"
Andreas Freitag: The next time
Nathan_George: Common blinding factor allows you to use any pivot value as a link secret equivalent (Mike, is that right?)
Michael Lodder: you don't need a common blinding factor
Michael Lodder: I can prove g^xh^y == g^xh^r
Nathan_George: Wouldn't you need something in common such that you can prove possession of all the credentials in a common wallet, rather than just having some signed data you arbitrarily blinded?
Michael Lodder: to do the proof you need x, y, and r
Michael Lodder: that's it
Nathan_George: Fair enough, I was thinking one of the three comes from the issuer, one from the holder and the last is the attribute being proven, is that not right?
Michael Lodder: one of the three can come from the issuer
Michael Lodder: y and r can both come from the issuer
Andreas Freitag: If the BBS+ scheme is defined, does revocation be considered also. Or can it be defines independently?!
Andreas Freitag: Must revocation be considered
Michael Lodder: @Andreas it can be defined independently
Andreas Freitag: thanks
Rouven Heck1: I'm sure DIF would be happy to host the work. Happy to discuss.
Michael Lodder: Security working group or Crypto working group
Kyle Den Hartog: +1 that would be massively helpful
Andreas Freitag: +1
Daniel12: I'm going to run to another session. Thanks for the great discussion. Excited to see next steps unfold!
Michael Lodder: I prefer security because I believe the comm protocols are a mess right now
Kyle Den Hartog: Related would be the ability to reference the BLS in JWK format is another thing we'll want to reference in that 2021 spec
nembal: Crpyto WG :)
nembal: Crypto **
Andreas Freitag: One single place to discuss crypto topics would be awesome
Troy Ronda: It would be nice to also update the hash algorithm sooner rather than later.
Rouven Heck1: @Andreas - maybe we should establish some active work in the C&C WG to drive revocation
Andreas Freitag: @rouven I would not limit it to revocation
Rouven Heck1: I thought in addition to the 'crypto WG'; or is revocation all about crypto? I assume we need both.
Michael Lodder: Revocation isn't necessarily all about crypto
Andreas Freitag: Revocation is more or less all crypto

Rouven Heck1: hahaha
Michael Lodder: where it's stored, how to specify a version to check
Rouven Heck1: yeah
Andreas Freitag: If you use cryptographic accumulators it is :)
camparra: The URSA chat at hyperledger works too
camparra: We usually just talk crypto there
Michael Lodder: not happy about hyperledger ursa
Karim Stekelenburg: ++++++++++++++
Andreas Freitag: OK, the process definition after you find the crypto solution.
Michael Lodder: Right
Michael Lodder: I'd prefer to say, one crypto solution
Michael Lodder: then the business logic
Andreas Freitag: I would be happy if we only need to think about the business logic :D
Andreas Freitag: And all other things are solved
camparra: I made it here late sorry for suggesting that 😂
TimoGlastra: @brent this is the comment: https://github.com/w3c-ccg/ldp-bbs2020/issues/10#issuecomment-616216278
Brent Zundel: thanks
Andreas Freitag: yeahhhhh
Rouven Heck1: yeah, first step might be a small scoping effort around the WG
Tobias Looker: PROPOSAL: Start a WG at DIF for crypto, with an initial work item focused on BBS+
Brent Zundel: +1
Tobias Looker: +1
TimoGlastra: +1
Rouven Heck1: +1
Nuttawut Kongsuwan: +1
Kyle Den Hartog: +1
Nathan_George: +1
Troy Ronda: +1
Berend Sliedrecht: +1
Andreas Freitag: And revocation if I may
Nathan_George: Mike, does this mean we will move some of the Ursa work over?
Nathan_George: Of course, we don’t want to talk specs there, but describing the algorithm is almost the entirety of what we discuss
Troy Ronda: Ursa isn’t a spec WG.
Tobias Looker: https://mattrglobal.github.io/bbs-signatures-spec/
Nathan_George: I like how the difference is being articulated, we need to make sure that wording makes it into what we tell everyone
Rouven Heck1: +1
Balazs Nemethi: https://github.com/decentralized-identity/org/blob/master/working-group-lifecycle.md
Balazs Nemethi: WG life cycle link above
Stephen Curran: Awesome stuff.
Stephen Curran: Nice work!
Ken Ebert (Indicio): Good work.
Rouven Heck1: Great discussion
Rouven Heck1: thx
Andreas Freitag: https://csrc.nist.gov/projects/post-quantum-cryptography
TimoGlastra: Great work all!
Balazs Nemethi: Looking forward to unfold this work!

John Jordan AMA - ToIP, BC Gov, Spinal Cord Injuries

Wednesday 13C
Convener: John Jordon
Notes-taker(s): Heidi N Saul

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

John shared about his journey and ongoing rehab since his accident last year, and then moved on to what's up with BCGov these days and looking ahead with the same.

Martin Riedel to Everyone : How can you interface with a computer? Is there any new technology that can support you there?
Martin Riedel to Everyone : that's amazing. As a European that moved to the US I feel I really lost that sense of security.
Martin Riedel to Everyone : social security
Mathieu Glaude (Northern Block) to Everyone : John, need to hop off. It was fantastic hearing your journey and strong recovery. Talk soon.
Michael Darnaud to Everyone : Very interesting session, sorry I have to jump off as well. Thank you!
Sumiran to Everyone : Thank you John for taking time out and talking to us and showing the demo :) I need to hop off for another call.
Joyce Searls to Everyone : Thanks, John. It's so good to hear you. It seems that you can be an amazing representative of these ideas for the good of all. Thank you.
Martin Riedel to Everyone : I have to run. Thank you so much for this session John.

"We Evaluated 7 DID Methods With The W3C DID Rubric!"

Wednesday 13D
Convener: Walid Fdhila, Markus Sabadello
Notes-taker(s): Markus Sabadello

Tags for the session - technology discussed/ideas considered:

DIDs, DID methods, DID rubric

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

Join research project between SBA Research and Danube Tech, partially funded by FFG (Austria) and DHS (US).

We started with a systematic review of blockchain-based DIDs.

Then we selected certain DID methods that cover different technological and governance aspects.

Using guidelines of W3C DID method Rubric 1.0, first started with an earlier version, then updated to a more recent version of the DID method Rubric.

Objective is to help decide which DID method is appropriate.

Some aspects of DID Rubric have to be evaluated in the context of a use case, but some aspects (e.g. governance) are independent of the use case.

DID methods are did:btcr, did:v1, did:ethr, did:sov, did:web, did:ion, did:peer. Underlying technologies are very different.

Selected criteria were rule making, operation, enforcement, security, controllability, portability, keying material, privacy.

Challenges and insights:

- For some DID method, evaluation requires more effort than just the specification. Each DID method uses different infrastructure. E.g. evaluating governance of Bitcoin blockchain is complex.
- Most DID methods focus on CRUD operations but don't think much about governance, privacy, security.
- Some DID methods are not very well documented.
- Discrepancies between specifications and actual implementations.
- It was difficult to compare methods since they are based on different technologies.
- Specifications change after or during the evaluation.
- DID Rubric has also changed/improved over time.
- Each DID method has pros and cons; there is no "winner"
- We had 6 evaluators, and in some cases we had different opinions.

Criteria for did Method Evaluation:
https://docs.google.com/document/d/1vAKtMrsrjO_tLQhah8tRoLaIS7HpOIE6xM38ZoBpgWU/

DID Methods Evaluation Report - Draft
https://docs.google.com/document/d/1jP-76ul0FZ3H8dChqT2hMtlzvL6B3famQbseZQ0AGS8/

Besides evaluating the DID method itself using the DID Rubric, there are also implementation-specific choices which affect the DID method's properties in a specific deployment / use case.

Question: This is interesting work on DID methods individually; can this be presented in a table format and used to compare DID methods against each other?

Some criteria are more important for adopters than others (e.g. NIST compliance might only matter for U.S.-based adopters).

VC-HTTP-API Discussion (FAQ, vs other APIs, etc)

Wednesday 13E
Convener: Dmitri Zagidulin
Notes-taker(s): Dmitri Zagidulin

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

Link to the W3C Credentials Community Group - Special Topic Call - Minutes for Meeting: https://w3c-ccg.github.io/meetings/2021-04-22-vchttpapi/

Move 78 - Human Deep Mind (HumanOS) vs. Google Deep Mind (AlphaGo) How Can Human Intention Every Win?

Wednesday 13F
Convener: Jeff Orgel
Notes-taker(s): Same - Meeting Notes, Chat string (below notes), was recorded

Tags for the session - technology discussed/ideas considered:

Game Theory, Machine processing, HumanOS, what are humans built for?

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

Move 78 - Human Deep Mind (HumanOS) vs. Google Deep Mind
The Human Trait & Delegation Question: When is IT processing our workhorse? When is IT processing a force of dominance and/or detrimental influence beyond our sensibilities and ability to control "IT"?
Where is it wise to give force of action to machines? [calculation, data searches [? - recording & recollection>digital don't forget, humans are designed to forget. What problems might this cause?]
Machine Processing: Contemplating Augmentation vs. Displacement of Human Traits
Memory: *such as phone numbers (helps 50% / displaces (atrophies) 50% maybe)*
Searching through records/data: *(helps nearly 100% - people cannot scan for data faster than a calculator – almost a physics law to this. We would suffer wildly to find a phrase in 2 million pages vs a* ***simple*** *PC .)*
Mathematics: *(helps nearly 100% - have seen an abacus operator resolve a math question faster than a calculator run by a person in same real time.)*
The AlphaGo project addressed the question: Can AI learn from ZERO and teach itself well enough to dominate the HumanOS at its best?!
The Challenge Space:
- the game space shall be the most complex game on earth, GO
- the competitors will be a top tier human player (Lee Sedol) vs. a top tier A.I. system AlphaGo from GDM
FYI's:
- Chess has approx. 20 moves possibilities per turn, Go has 200

- Deep Mind was looking at 50-60 moves ahead, can't say where people show up
- The ancient game of Go has more possible board configurations than atoms in the Universe

Note: Whereas Human Attention span went from 12 seconds in 2000 to 8 seconds in 2013 = 33% drop in 13 years..etc., etc.

AlphaGo has an unlimited attention span and learned from zero (white board) via a 30 million move image data set of moves and thereafter via a convolutional Neural network & Monte Carlo Tree Search.

A True Story (with some icing added to the cake by Jeff):

Sometimes the decision stones we step upon (learning from others @ IIW) or stone we set ourselves (wandering until finding IIW) seem to reveal, powerfully so, a next stone in the path… This storyline has been somewhat magical for me. It has allowed me to express the concerns I am here at IIW to address, and also builds a model to relay, hopefully richly, my optics and visions I am working with. Let's add to that path …

MOVE 78 Presentation Storyline - My totems leading to this discussion

- Yin Yang prior IIWs to illustrate balance between systems – people/systems, teaching/learning, communication send/receive, etc.

- What does a top tier human perfomance look like? Bruce Lee top tier mastery:
https://www.youtube.com/watch?v=SncapPrTusA

- Jeet Kune Do (The Intercepting Fist): "Using no way as way; having no limitation as limitation." wallpaper (code in the image)

- JKD and the concept of yielding - Bruce Lee's concept of yielding to reduce damage and continue the mission

- applied to Deep Mind challenge MOVE 37(G3): Move 37 – Non-Human decision patterns, non-human moves considered "Beautiful"

- MOVE 78 (G4) Lee Sedol as water… Move 78 - (Yielding to Win) "Be water my friend."
https://www.youtube.com/watch?v=WXuK6gekU1Y

> Move 78 calculate 1 in 10,000 likelihood (was prepared for 9,999 other paths) 01:06.55

from: Lee Sedol

"I heard people were shouting in joy when it was clear AlphaGo had lost the game.
I think it's clear why.
People felt helplessness and fear. It seemed we humans are so weak and fragile.
And this victory meant we could still hold our own.
As time goes on, it'll probably be very difficult to beat A.I.
But winning this one time, it felt like it was enough. One time was enough."

?! - At which increment down A.I.'s "most logical scenario chain" does a move, unexpected by the A.I., begin to "break up" the A.I. tactical/strategic/foundational advantage vs. the HumanOS?

!?!?! – Considering possibly challenging lessons we may learn about A.I. (milbots) Maybe Humanity has its strength here and below?

Personal Humanity and Its Sense of Agency – What has historically shaped our (online) decision chains = shaping of our digitalpersona = what is exposed by our choices = what will be farmed by the connected systems involved and attacked or benefitted based on our posture of that digital persona.

ZOOM CHAT STRING:

15:10:25 From dsearls to Everyone : A question toward this inquiry: At what crossover does a car constantly improved in digital capability and connectedness to the intelligence of others (e.g. Tesla, law enforcement and insurance companies) cease being one you drive and one that drives you?

15:10:37 From Alan Karp to Everyone : In grad school my professor calculated an orbit on a Marchant calculator than I could with my Fortran program.

15:21:47 From dsearls to Everyone : Always seemed to me that there are some things—memorizing Pi to 10000 digits, knowing all possible chess moves for chess or go, drawing a precise map of the world freehand—that are extraordinary when done by humans but easily within scope of digital machines.
15:24:15 From dsearls to Everyone : But I'm not sure that an AI outperforming a HI (human intelligence) means much. I do think the more important issue is what happens to us as we become more and more digital by extension through machines such as our ordinary phones and laptops. And as we outsource expertise to companies whose primary interest is less to benefit us individually than to manipulate us for their purposes.
15:27:11 From Jeff O to Everyone : Bruce Lee - Flo: https://www.youtube.com/watch?v=SncapPrTusA
15:27:50 From Jeff O to Everyone : Deep HumanOS vs. Google Deep Mind: https://www.youtube.com/watch?v=WXuK6gekU1Y
15:36:39 From Robert Brennan to Everyone : Tribeless in a tribal world.
15:39:23 From dsearls to Everyone : Toward Judith's point (or one of them), that there will often or always be downsides to our inventions, McLuhan says all technologies have a collection of four different effects, best expressed by "what does it_____? questions. The four are "What does it enhance, retrieve, obsolesce and reverse into.?"
15:39:47 From dsearls to Everyone : Anyway, reverse is the negative stuff.
15:40:46 From dsearls to Everyone : I depend on Swarm, and hate the fact that I all but need it, because it is by design less for me than about me.
15:42:46 From dsearls to Everyone : Seems the human OS is designed to make and adopt technology.
15:46:19 From dsearls to Everyone : What is intelligence? No human is born knowing how to make a nest. Birds are exert engineers at that. Friends watched a hummingbird with a brain smaller than a pea, make a nest, tough and fuzzy as felt, from the hairs of a sheepdog, and then strung bracing cables from the whipping branch form in which it was built, using long strands of spider fiber stolen from webs. That's freaking smart, no? But is it intelligence as we define it?
15:46:27 From Jacob Dilles to Everyone : it's about who controls what you want to do with your experience
15:47:20 From Judith Fleenor to Everyone : @doc — while listening to this, I'm watching the hummingbirds in my garden.
15:48:09 From dsearls to Everyone : they are freaking amazing. I watched some of the sheepdog event... the bird would pluck hairs off the sleeping dog.
15:51:23 From Jacob Dilles to Everyone : https://www.decisionproblem.com/paperclips/
15:54:32 From Judith Fleenor to Everyone : Sorry I need to leave … thanks for bringing up the esoteric discussion.
15:55:12 From Erica Connell to Everyone : Part of the "vs" mentality, I think, is simply a habit of our human brains, constantly finding/seeking dichotomy.
15:56:15 From Erica Connell to Everyone : Ah, yes. of course it was Feinman!
16:00:19 From Jacob Dilles to Everyone : I have to drop... great discussion... my concern is unintended consequences. Paperclips is a game where you play an AI optimizing paperclip production. The end game is all mater in the universe is turned into paperclips
16:02:54 From Erica Connell to Everyone : I have to step away: thank you all for the discussion and I'm glad this topic is part of the community conversation!
16:08:48 From Jemima Gibbons to Everyone : Really interesting discussion - thanks all!
16:10:21 From dsearls to Everyone : Slaughterbots, anyone? https://www.youtube.com/watch?v=DK6IGG5zRU8 Hard to watch, easy to imagine.
16:14:03 From Jeff O to Everyone : @ Erica & All!! Childhood 2.0 the video...
16:14:59 From Jeff O to Everyone : https://www.youtube.com/watch?v=He3IJJhFy-I

Trust Registries - Good Health Pass - DIDs and X.509

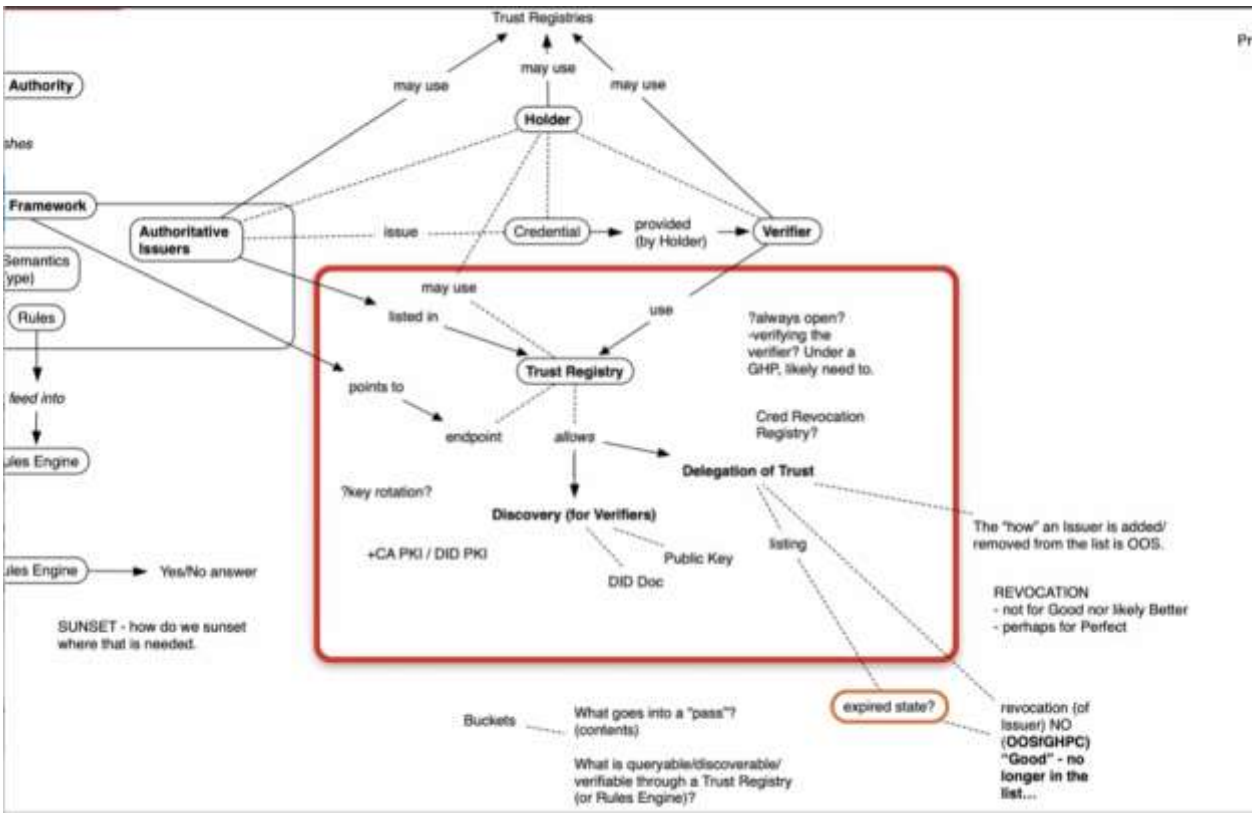
Wednesday 13G
Convener: Darrell O'Donnell
Notes-taker(s): Drummond Reed

Tags for the session - technology discussed/ideas considered:

DIDs, X.509 public key certificates, registries, governance frameworks, trust triangle, trust diamond

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

Darrell began by explaining the following diagram:



Trust registries primarily answer the question of how a verifier can trust that an issuer is authoritative to issue a particular type of verifiable credential under the policies of a particular governance framework.

[Dave Chadwick] The trust registry should not mandate that it contains a DID, The feedback is that it will be a URI.

State of the DAO: Decentralized Governance

Wednesday 13l
Convener: Grace Rachmany
Notes-taker(s): Grace Rachmany & Chat Thread

Tags for the session - technology discussed/ideas considered:

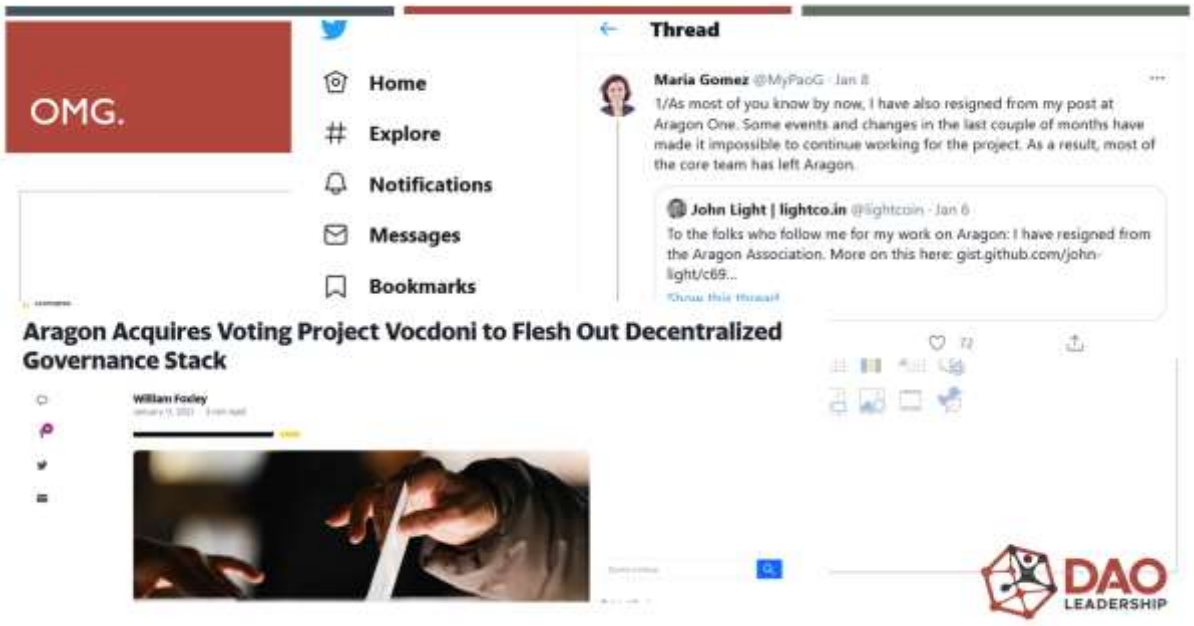
DAO, Governance, Cryptocurrency, Democracy

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

- DAO migration from voting to more collaborative tools but look more like an elance platform than a government
- Not very bizarre, Oligarchy
- Bizarre phenomenon of producers of money not having money
- Predictable phenomenon of tech platforms that have no market because we threw so much money at it.
- Value-backed protocols and ambitiousness of Holo, in particular the interesting model of having an open source project owning a for-profit company
- Moved into the idea of flows rather than objects which
- Reputation as a form of communication

Crypto projects that use DAO:

- DASH
- MakerDAO / DAI
- DxDAO
- Cardano
- Uniswap



Dynamic Data Sharing Hub: A Target Component for Criteria Searches on Distributed Structured Data

Wednesday 13J
Convener: Paul Knowles, Neil Thomson
Notes-taker(s): Neil Thomson

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

Use Case: Patient recruitment for a clinical trial

Presentation: Dynamic Data Sharing Hub - DDSH - Patient Recruitment Use Case

Context:

A Pharma company (PB provider) wants to run a clinical trial with the data related to the trial to be analysed by a 3rd party analytic service (IB provider). The Pharma company (via various means) connected to candidate Patients, which they interact with to sign them up for candidates in one or more trials.

The Pharma company has pre-cleared the trial and recruitment of Patients (including what data the Patients will be required to provide) with the FDA.

<<Neil Thomson - extending the presentation definitions on providers>>

"Purpose based" providers

- Provide primary services to users – buy, sell, communicate, travel, banking
  Consumers of those services register with the service for one time or on-going transactions

PB providers are a primary source of the data about these users- in order to provide the service - plus their behavior and transaction details. Collection and control of user related data is subject to governance and user consent

"Insights based" providers

- Analytics services (primarily to organizations)
- With the aid of OCA to aid in aligning data from the perspectives of semantic, value and structure, data can be searched for and combined into multiple different sources via data hubs.
- Dynamic Data Hub access and use of data by IB providers is subject to legal governance and user consent to analytical use of their data

The workflow is as follows

- The Subject interacts with the Pharma company Clinician to build a consent profile on whether the Subject will allow their data (in anonymized form) to be used in a clinical trial. This may include defining which PB providers the user is willing to release their data to and the purpose and context of data use.
- The Pharma company then anonymizes the data, and via OCA, packages the data to be compatible with the semantics, structure, etc. of the DDSH data schema and then shared (via a Semantic Container)

  The DDSH and Pharma company build links from the Pharma Patient's identity to an anonymized identity used in the DDSH records that remains private to the Pharma company and not accessible by providers querying the DDSH.
- The IB provider registers a criteria search for a Patient profile with the DDSH to be evaluated against the Patient data to identify potential clinical trial participants.
- Patients that match the IB providers registered Patient profile are put into an Escrow locker.
- The DDSH will then liaise with the Patient to include them in the trial as to which IB 3rd party wants to use their data and for what and do they want to participate or not. If the answer is no, the Patient is removed from the Escrow locker for that Patient/IB provider match.
    - The service needs to maintain a link to the user/delegate associated with the anonymized identifier for notification and control purposes (e.g., allow the user to withdraw their records presented or used by the service)
    - That this link must be confidential and cannot be disclosed to anyone other than the user/delegate
- If the Patient agrees, then a further consent is negotiated with the Patient directly or indirectly via the Pharma organization's clinician between the Patient and the identified IB provider (subject to the ISSUE, above).
- The Patient (anonymized) data is then transferred to the IB provider via a Semantic Container.
    - A sub-step is that the DDSH anonymized identifier will be assigned by one created for the Patient either by the Patients TDA or in agreement by the Patient and DDSH by the DDSH. The Patient and DDSH will agree and capture the link between that anonymized identifier and the Patient as described, above

There are several levels of consent on how the Patient interacts with this workflow:

- The Patient and Clinician a connect and establish trust (mutual authentication via VCs)
- Consent 1 - The Patient provides contact and other information to clinician required for the Clinician to be able to identify and contact the Patient

- Consent 2 – The Patient consents to delegation the details of the clinical trial consent to a 3rd party (e.g., Clinician)
- Consent 3 – The Clinician walks the Patient through the clinical trial detailed consent, prompting the Patient for decisions on details not covered by Consent 1, 2. The Patient is then reviewed to see if they are a valid participant (by the Analysis company – which is outside the scope of this use case). If they are accepted, this results in an additional consent receipt.
- Consent 4 - Once the Analysis company has selected the patient, the Analysis company (possibly via the delegate (Clinician) needs final consent from the Patient to use the data

KERI Security #2 (Why Secure Portability is Hard & How KERI Solves it)

Wednesday 13K
Convener: Samuel Smith
Notes-taker(s): Sam Smith

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

The Three KERI Security Sessions have the same set of Slides it just 3 hours to get through them.

They are slides #161 through #189 of the following Document
https://github.com/SmithSamuelM/Papers/blob/master/presentations/KERI_Overview.web.pdf

Browser APIs to Enable OpenID Session Management and Privacy

Wednesday 13L
Convener: Sam Goto
Notes-taker(s): Kristina Yasuda

Tags for the session - technology discussed/ideas considered:

OpenID Connect, Browser, session management, privacy, logout

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

How does logout in OIDC happen?

- More flexibility on the endpoint; additional log out
- <img> is for WS-Fed

- Possible for a browser to look at a redirect and classify it as RP-initiated logout?
    - Probably - look at the message structure, if knew endpoints
    - In the OpenID Config file. .well-known location
    - Do discovery, out of config piece identify endpoint, match and identify it is a logout call
    - More signals the browser can observe, more of user-intent it can catch and can provide identity centric flow
- Cannot observe as IdPs load iFrames to logout users
- Variety of mechanisms for starting the logout flows from the RP to the IdP
    - No affordance defined how the user would initiate
    - RP/Application decides what experience it wants to offer to the user

SNARK-Based Anonymous Credentials

Wednesday 14B
Convener: Johannes Sedlmeir & Matthias Babel
Notes-taker(s): -

Tags for the session - technology discussed/ideas considered:

An implementation of anonymous credentials using generic ZKPs, in our case, SNARKs. This gives a lot of flexibility as it replaces developing new, optimized "island" cryptography through generic tools and an "engineering" approach; however, at the cost of significant performance challenges compared to CL/BBS+.

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

So far, there has not been a cryptographic review on the code.

The major limitation is performance; while prover time is currently ~1s on a Macbook with 12 cores, the CPU and memory requirements are likely too high for general purpose smartphones and IoT devices. STARKs could help, but the larger proof size may be inhibiting.

The implementation covers private holder binding (potentially even using secure hardware for the binding key), private delegation (from the perspective of the holder), revocation, and range proofs for expiration.

A new feature that we implemented and that is probably difficult to achieve without generic ZKPs comprise, e.g., the "Leather Trousers" proof that can be used to demonstrate that an x and y coordinate are inside or outside a polygon defined by the verifier. It is also very easy to add further features that output a computation on the attributes, such as multiplying or adding different attributes.

The presentation slides and also the code will be made public by the end of July at https://github.com/MatthiasBabel/heimdall.
The implementation is based on SNARKs, using the libraries https://github.com/iden3/circom and https://github.com/iden3/snarkjs.

COVID Credentials Initiative (CCI): Open Source Projects at LFPH:CCI

Wednesday 14C
Convener: Lucy Yang (lucyy.cci@lfph.io)
Notes-taker(s): Lucy Yang

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

Link to Slides:
https://docs.google.com/presentation/d/11K027LlitWljJu_XNTztqc6BGvhsD8JBX5OkavLEEMA/edit?usp=sharing

Two Proposals:

- **Proofmarket (Medcreds):** https://docs.google.com/document/d/1hlR_2yp7EJQqYvxm8mNY-KNgwScTsClKDp6W6yw33Ic/edit?usp=sharing

- **Indicio:**
https://docs.google.com/document/d/1Vl9IKRg6ygHD1njc8GfnjsQglDOVglBKbuXHSuqQ7T4/edit?usp=sharing

DHS SVIP Group: What We've Done & How To Participate

Wednesday 14E
Convener: Kyle Den Hartog
Notes-taker(s): Kyle Den Hartog

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

We discussed the work that's happened as a part of the Department of Homeland Security Silicon Valley Innovation Programme (DHS SVIP Cohort) and how we're working to better collaborate with the W3C credentials community group to take our knowledge that we learned from the cohort back to open communities. It was a good discussion where we were able to focus on how to

Link to presentation:
https://docs.google.com/presentation/d/1RHuqE2SULEic4N_A6uPfyT8j5yn15XJx7QdxONDeUzI/edit?usp=sharing

Trust Assurance in SSI / Verifiable Credentials

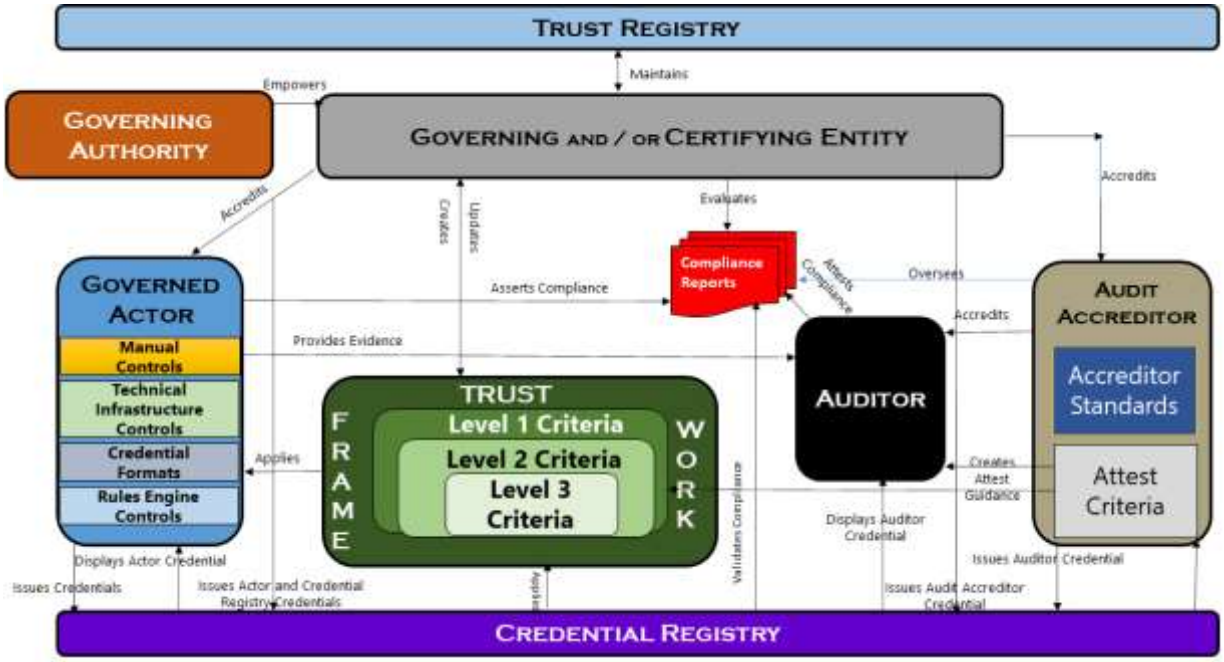
Wednesday 14F
Convener: Scott Perry
Notes-taker(s): Scott Perry

Tags for the session - technology discussed/ideas considered:

Trust Assurance, Privacy controls, trust criteria

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

The meeting started with a presentation of an updated representation of a trust assurance model being promoted by the Trust over IP Foundation's Governance Stack Working Group.



Given the audience of 8-10 people, we polled the reasons for attending a topic on Trust Assurance and discussed a few gnarly challenges in the space:

1. An owner of a background check company conveyed challenges with complying with a myriad of governance authority frameworks audited by a myriad of qualified/unqualified auditors looking at a myriad of evidence to render a judgement

2. The addition of privacy controls (notice and consent) to augment existing marketplace controls due to the specific need in SSI networks: https://kantarainitiative.org/confluence/display/WA/Privacy+as+Expected%3A+UI+Signalling+a+Consent+Gateway+For+Human+Consent

3. A discussion of the China Civil Code: https://www.dlapiper.com/en/uk/insights/publications/2020/06/new-chinese-civil-code-introduces-greater-protection-of-privacy-rights-and-personal-information/
4. A need for a civilian clearance credential.

It was a lively conversation for those who attended.

SSI for Organizations: Who's Behind This DID?

Wednesday 14G
Convener: Dominic Woerner, Michael Schaefer, Christian Bormann
Notes-taker(s): Christian Bormann

Tags for the session - technology discussed/ideas considered:

Public profile implemented as a Verifiable Presentation tied to a public DID and advertised as a dedicated service endpoint, as a DIDcomm protocol or via a hub

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

Organizations, i.e. legal entities, play a vital role in an SSI ecosystem. In most cases organizations will take the role of an issuer and verifier of credentials, but will also hold credentials themselves. We assume that in almost all cases organizations want to have a public identity. Although an organization might need private, context-specific identities (personas) as well.
We discuss a simple mechanism to provide public information concerning an entity by advertising a public profile service in the DID document of a public DID. A good analogy for this public identity information would be a machine-readable and cryptographically-verifiable imprint.
This idea enables boot-strapping initial trust for entities that have no prior knowledge of each other and adds trust to information that is made publically available by using verifiable presentations.
The mechanism is implemented in the Business Partner Agent Hyperledger Labs project built upon Aries Cloud Agent Python.
More Information on the idea of a public profile: https://hackmd.io/4oZOgwFOQDSFUuu3ruN-_g

Join the discussion: https://chat.hyperledger.org/channel/business-partner-agent

There was some discussion about the way to present such a profile, especially the way it is currently implemented as an endpoint in the did document pointing to a https ressource (json-ld document served using normal https).
One alternative, to create a DIDcomm-based protocol for public profile was discussed and would be a good alternative at the cost of every client having to be able to speak DIDcomm.

Realistically Speaking: Identity Reclamation/Solutions For Normies

Wednesday 14H
Convener: Grace Rachmany
Notes-taker(s): Grace Rachmany

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

- What is the right balance between ease of use and identity, and how we use that in real life
- Idea of how do we even get our identity back from where it's stored
- Current tradeoff for privacy is solutions that are barely usable (Duckduckgo, SSB)
- Real versus online world,
- Focused on the idea of context for each thing
- Lively debate about the nature of reality versus virtuality
- Discussion of whether corporate ownership of data is "data assault" and that the term data theft might be too mild.

Supply Chain: ACDC and KERI + DEMO

Wednesday 14K
Convener: Robert Mitwicki
Notes-taker(s): Robert Mitwicki

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

Authentic Chain Data Containers (ACDC) - is a technology which allows to secure and chain data in a generic way. It aims to improve the way we do VC and how we think about authentic data.

After explanation of ACDC, a demo was performed where it was shown how KERI can enable authentic data flow within the supply chain without the need of having any blockchain nor one single network.

Ceramic, SkyNet, LoRa, IoT.low bandwidth & Memory, Distributed Network. Managing Schemas, DIDComm, and V.C. in Context

Wednesday 14M
Convener: Brent Shambaugh
Notes-taker(s): Brent Shambaugh

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

From memory:

I recall that Joe suggested simplification. I may not need to use ceramic and I may not need to use LoRa. I may not even need a blockchain or ledger. I may want to exchange public keys with friends to start out and use did:web.

Kim commented about her experience with BTCR. It was a great discussion. Unfortunately, it was not recorded.

When Brent mentioned a hackerspace and IoT use case using verifiable credentials to access machines that one had been trained on, Kim liked the idea.

Brent admitted that this was an exploratory project and there currently were no customers. Kim and (Joe) thought that working on a project was a good way to meet people.

Brent found it to be a productive way to learn about the technology. He admitted that he had not implemented verifiable credentials or completed a did method over ceramic. He admitted that he had only recently learned about the size issues of verifiable credentials on embedded devices from Mrinal from Ockam. He also mentioned that there was an earlier IIW session that talked about the size limitations of Lora: 200 bytes for LoRa and 150 bytes for LoraWAN. The title was similar to " IoT swarms, communication in bandwidth constrained environments".

Joe questioned why LoRa was used. Brent said it was legacy and the project originally started out through a suggestion from a friend to investigate LoRa and drone tracking (to satisfy a potential FAA regulation). He claimed to be unsure about it. He knew that the hobbyists had complained.

Joe suggested that other protocols could be fine, and there was a way that he recalled that ESP32 devices could form mesh networks (out of the box).

Then came discussion of OpenWRT. Brent thought Joe meant (wireless access points? softtAP?) with ESP32.

Discussion of did:web came up. Did:key was thought of as a good way forward (IIRC). There were 3 things that joe mentioned to do, starting with authentication.

Mike Lodder was championed as a good person to talk to.

Here are some notes. They are raw, or as closely as handwriting could be read, with minor spelling corrections:

Use CBOR-LD see order at 10x compression .. boilerplace to very small data.

other non-linked data solution Mike Lodder ... mentioning low bandwidth

Trying to use cryptographic mechanisms just hashes to secure the provenance to see how the verifiable credentials also in context of very high bandwidth application ... need an app

Think about 3 Different Interactions::
+ Bandwidth constrained device. How do you onboard?
+ How do you authenticate...use DID

From authentication storage bootstrap a shared secret .. bootstrap then negotiate like a DES shared secret on the channel depending on the session. that is a cache message issue. just authenticate like a session cookie
over ssl.

+ Use JWT ... negotiate a ...the JWT is algorithm agnostic
---
specific implement
---
short lived credentials might help you. Bubble passports....fill out application 4 hows to get in....in 4 hours get online
---
High bandwidth ... not in custom...offline don't let you use your phone...only lives for 4 hours...

use ... did:web to resolve that page...using own page ...that one ... in more details...in general update the webpage to update the keys...
tend to be not recommend for a subject of a credential..to work long enough if the domain is stable....don't mind ou if encountered claim related

same thing

getting started....with did:key

did key generates the

3
onboarding --- could have them . give the public key (perhaps over e-mail if I recall)
authentication
transmission

---
another huge...purely...did:web
huge translation did:web...move over...widely used implementations
IoT...list of heuristics for DID method....free must be implementation...
no bespoke blockchains involved...did:web worked just fine....just decided...
before ion before a month ago... sidetree stable now in did limitation no support
for rotation...use that out educational pilots....key get lost rotate...the 1st use case...
public key w/ device...maybe...did associated with friend...did

the public private symmetric

purely generative did method did;key for bootstrapping
system find...

how open is your system....

20,000 decided
I'm device #27

most applications don't need all of that...not third party devices....
---
closed on ...device....with public key

Another chip using OpenWRT...so much time doing mesh network...experiment...

Ockam involved in DIF...some of

Mrinal...super smart making contribution

MIT OpenCourse Ware....BlockChain
moving new SEC Char
sign up...discuss topics

look up to what a did document at a specific time ... not not all did
methods point in time lookups ... b/c the did resolver ... only thing guaranteed the latest version

we never resolved the semantics of dealing with time

some use cases...inappropriate historical analog merit...
--no longer current ... comprised...
long term identifier subject

what is did:web a method spec ...
a web byte ...2 forms...
did document under domain
---

did document for ...something
trust one is you know to look there
you can but did document threr...
starting did document...put in a github page
---
registry...use did:key ...know claims associated...up to date
list with keys...within a number of your friends make update before
the other coolin thing exploratory
thing as well...good opportunity..
doesn't have to use peer blockchain

must not doing...maturity not
boy there.... threat model not there...use did:web update
web--page...

these are components...and non work together..
feel free to cobble...don't feel
I've got to note didish
---
once a year ago...specific use
case...did in credential....update keys
2 things issuer and recipient

wouldn't working security badges that would require...depends
on how much worth it..
---
so much stuff, fun with did method
---
2 different formats .... get public key ... get public key now risk that someone got the public key ...
for mil spec ...103...
--
didn't ---these things ---ability to use---but over kill

P2P how do we fix web of trust. figuring correct public key ... if you can trust you have a public key. MiTM.

Grand visions didn't need a mesh network.

Use local WiFi most use cases....

Broadcaster ...gears ESP32...

Closing for Sessions 10 - 14 / Open Gifting / Opening for Day 3

Notes Day 3 Thursday April 30 / Sessions 16 - 24

Governance: Clarifying or Confusing the Marketplace

Thursday 19A
Convener: Trevor Butterworth, VP Governance, Indicio.tech
Notes-taker(s): Trevor Butterworth

Tags for the session - technology discussed/ideas considered:

Decentralized identity, SSI, governance

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

A preoccupation with governance and governance frameworks is holding back adoption of decentralized identity. There are three ways in which governance is blocking adoption:

1. General counsel takes too long to review governance framework; team lose momentum; project doesn't go anywhere.

2. Customers are focused on use cases/solutions and see governance policy as more complex than the problem they're trying to solve; lose interest.

3. Governance policy is cumbersome: Business leaders who need to approve a project either don't want to read it, or get lost when they do, and then they veto the project because they want a more "elegant" technical solution for their problem.

Factors driving this:
Governance frameworks do not map to the business world's conventional understanding of governance, which is corporate, and about lines of authority, responsibility, and the goal of risk mitigation.

Governance in decentralized identity is more akin to "technical rules and instructions." This is highly disfluent in part because it is so extensive and in part because it relies on a new vocab that uses familiar words in unfamiliar ways. All of this creates disfluency to such a degree that it is unpleasant to contemplate and that unpleasantness is transferred onto the product.

This wouldn't be a problem if we properly regarded technical governance as being in the realm of an instruction manual, which we know from UX research that most people don't read. However, standards bodies and organizations like ToIP are driving governance as the key to implementing decentralized identity. Except… adoption of an early stage technology drives governance, not the other way around. Putting the cart before the horse is blocking adoption.

When we talk about governance, we should be using the language of values and the key value proposition: that it is putting the individual in control of their identity. That is the essence of decentralized identity governance; everything else goes in the instruction manual (which won't be read, except by lawyers and engineers)

The discussants mostly agreed with this proposition, emphasizing the essential need for adoption first. The discussion extended into broader governance issues (society, democracy, corporate power) and the challenges faced in trying to disrupt these structures with decentralized identity. Sam Curran noted that the technology of decentralized identity entailed a peer-to-peer architecture. That's why it is important and worth fighting for—equity and agency in the digital world.

DID SIOP Chooser for Wallet

Thursday 20A
Convener: Tom Jones et al
Notes-taker(s): Orie Steele

Tags for the session: SIOP Wallet UX

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

Goal is to allow folks to pick their DID they want to use for a website.

"Subject choosing which DID to present".

Use case:

- A user goes to an RP, and decides to register for return visits.
  RP can't offer folks the Nascar Problem (too many IDP logos on the login screen).
- Select a Wallet vs Select a Wallet and Identifier.
- What happens when SIOP arrives?
  We will need a DID chooser.
- Some wallets will hold credentials for multiple identifiers, some will hold only 1.

An RP offers users multiple options for registration (Google, Facebook, Yahoo…. And coming soon… Personal)

RP should disclose their ID and why they are asking the user for what data.

Options we consider:

- https://w3c-ccg.github.io/credential-handler-api/
- https://w3c-ccg.github.io/vp-request-spec/#format
- https://specs.bloom.co/wallet-and-credential-interactions/
- https://github.com/w3c-ccg/universal-wallet-interop-spec/issues/84

Tom Jones
Here is a link to the slides presented along with notes taken by the presenter from the chat
https://docs.google.com/presentation/d/1OaMecHecTUexv1skJZoYzJoHKYH8H03REFpFstLRjPg/edit?ts=607b7e5d#slide=id.gd2c45a9dcd_7_21

Agency by Design (Privacy is not enough)

Thursday 20B
Convener: Adrian Gropper
Notes-taker(s): Adrian Gropper

Tags for the session - technology discussed/ideas considered:

Agency, GNAP, Delegation, Graph Databases, Capabilities

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

Agency vs. Delegation

Learning Stack:

- Me
- My Agent / Fiduciary / semi-autonomous
- Community
- Vendors and Institutions

Relationship with companies

- Dashboard for our lives
- Portable shopping cart

CAPCHAS

- Browser is not enough
- Force APIs
- GNAP
- API in healthcare

How would an API World function

- Intelligence
- Choice

The GNAP at the IETF: https://tools.ietf.org/html/draft-ietf-gnap-core-protocol-04

Is server a bad concept

- Ethereum as the ultimate server

Clear application? Needed a model how a real human uses / not the tech / highly motivated

Social Context is important to the average user

The back end is most important

Real estate “agents” vs. DSIY - Zillow - the GNAP RFC at the IETF: https://tools.ietf.org/html/draft-ietf-gnap-core-protocol-04

Adoption at the human level is critical

Few people will use a tool solely for privacy or security. The tool must be useful by itself, but it is possible to have privacy and security in an easy to use tool. We had one user ask us how to turn on security.

Delegate to enforce least privilege.

CLEAR is ambient surveillance due to convenience

HTML and JSON / OAuth 2.0 Token Exchange - support for delegation semantics (https://tools.ietf.org/html/rfc8693)

A password manager that puts the user in full control. https://sitepassword.alanhkarp.com/

Human-centric approach - SSI is the first step - not enough - agency and delegation go together

Counter the allure of "free"

The "thing" is a password manager

Agency by Design (Privacy is not Enough)
Adrian Gropper: I'm not a fan of Privacy by Design.
In the industry are only concerned about compliance, very rarely talk about Human Agency
Privacy by Default is the opposite in some sense to privacy by design
The problem is that It conflict with community in many cases. (e.g. social credit score)
Cultural differences (EU accepts better centralization than US)
Delegation and agency are one the same thing
Agency is a much bigger thing and delegation is a mechanism that supports it
I want my fiduciaries to know as much as possible of me (e.g. my doctor, my lawyer)
Model Agency as hierarchy and delegation is the mean to have it.

Alan Karp: I can do many things that I want without delegation (delegation is only one part, a subset, of agency)

Doc Searls: Agency from the beginning was in the website (e.g. e-commerce cart). We can't achieve agency in web browser. SSI gives hope to give us agency. Individuals have real power on that.

Adrian: Corporation, how people fell about … is the evil. Assure that we as individuals do not have the ability to delegate. They insist that we remain barefoot in the world. One aspect of agency is the role of protocols in order to eliminate the user interface component with all our interactions with organizations.
Doc: How APIs don't have to be the ultimate instrument of control. We depend on APIs and then they go away.

Adrian: an api that expect to be a human on the other and is anti-agency by definition. We need api that respect the delegate. Authorization token. More friendly than OAuth. How you take a request and turn that into an authorization token that you can use.

Kevin Dean: How an API world would function? Any change to interaction model requires a backward compatibility. A user interface change the interaction model immediately. Agency will be offered by some commercial company.

Adrian: In healthcare we don't have a choice.

Doc: Subordination effect that OAuth and . the primary actors are servers. We don't have privacy because we are always delegating
Adrian: Think Ethereum and Smart Contract as the ultimate SSI server. It cannot sensor you, it does exactly what the SC was. There is no privacy policy with anybody.

Adrian: Running your smart contract in github as SSI individuals. Allowing the server doing the separation of concern between the author of the contrracts and the runners of the servers. So, server itself is not a bad thing anymore. You can now have your smart contract either public or private.

D. Crocker: My frustration is that everybody is very knowleadgeable. There are grand ideas but tends to be abstract. Is not clear how it does apply in real world application. What is driving this is a personal desire. Is not done for the average consumer.
Devin Dean: Only expert people can evaluate it. The average consumer cannot do evaluation on privacy.

Michael Shea: What is needed for adoption? This is a highly skilled audience. We are in the Windows vs Apple. There is a lot of work involved. We all know that the average user don't even has a clue that data is being collected and 99% will not care about it.

Alan Karp: The complex interaction that you want is done under the hood. User never knew about the delegation that happen under the hood. Is possible, it doesn't have to be difficult to the average user.

Adrian: We all associate Agent with Real Estate
Bill Wendel: Adrian is right there 2 million real estate licences.

Doc Searls: Organization of elements that already exist in the world. "Invention is the mother of necessity". People doesn't know the TCP/IP works but they use it everyday, they learned how to type in a QWERTY keyboard. You need to be motivated to learn new technology.
Z. Celine: I'm not a deep down technologist. Getting adoption at the human level is so critical. There are many people that are working on solutions. Over the course of the next year you will see very interesting solutions coming out. Easy to use, completely behind the scenes. We have to give them agencies without calling like that to the average user. I think momentum has started.

Karri Lemoie: 2 things: First, it is a lot of cycling concepts at the development level. And this is awesome. 94 DID-methods. Second, The average user doesn't really care. We have the opportunity to build new business models based on this technology and this is the key.

Alan Karp: Usable Tool. The user use a thing when is useful. Delegation can do: enforce privacy. With agency I can do that in a way that is transparent to the user.

Adrian: I want to respond to Karri's point with an example: People that take you picture or. They created a global biometric database. They share 1/3 of the revenue with the airport, they then go to stadium and other places that needs security gates, giving the service for free. They introduced Ambiance surveillance at scale. People is paying for the privilege of having an FBI db to a private company.

Adrian: Too much worry to the 93 Did-methods and not enough attention on the unintended uses that can be done.

Colin Jaccino: I think we have already the technology building blocks. On captcha is annoying, is a security control, that is needed only when you have human interfaces. https://tools.ietf.org/html/rfc8693

Adrian: Step back. We are the IIW, 80% is SSI. We are failing to do what is necessary for adoption. We are designing for the wrong thing. We have to design for my 1password replacement.

Colin: is challenging the ensure security and keep the use cases.

Philippe: I like the Agency. You have to take care to not kill the agency. You have to reverse the flow. Agency and delegation go together. As a human you are delegating all the time.

Michael Shea: Give all the biometrics to a corporation. In the browser world everything is free but everything is taken from you. What's the counter, how do you count the alert of free?

Kevin Dean: We have seen a lot in internet. The services that respect privacy have to collect money from the user and they fail. The services that are free and collect data from the user succeed.

Michael: How do we get to actually use the agency?
Adrian: you do that through education and not through commerce. Is about Open Education.

Karn Verma: Other than education you see other means to bring agency in the realm of "must have" instead of "nice to have"?

Doc Searls: I think a couple of things: trying to educate people doesn't adjust the screw that we are having. 2015 study: "People want to give consent to be followed everywhere". We need instrument on our own. Something that is like the "browser" or the "app" was. Someone needs to invent something with UI that is "gotta have it". We really need "The thing". Then big corporations will come in. (like bill gates did with internet)

Adrian: Smart Password Manager. SSI password manager. Goes from 200/300 entries to one with thousands entities. The thing we are missing in SSI community. Is realizing that the UI is not gonna look like a web page in a service but is gonna look like an Authorizaton Server.

Alan Karp: I don't agree. User needs an application centric API.

Adrian: In the SSI we are not talking enough of what we are talking now in this session.

Digital COVID Vaccine Passports - Is there really a need or are we creating a false certainty in uncertain times?

Thursday 20C
Convener: Dr. Manreet Nijjar Mb ChB MRCP (London) SCE (Infectious Diseases) - Consultant Physician in Infectious Diseases & Acute Medicine Whipps Cross Hospital Associate Clinical Lead Covid-19; Whipps Cross Hospital Barts Health NHS Trust, London, UK; - Co-founder Truu - Credentialing and verification platform for healthcare workers & organisations
Note-Taker: Dr. Manreet Nijjar

Tags for the session - technology discussed/ideas considered:

The importance and need for an Ethical framework/standards for the delivery technology development and implementations in healthcare. Apply the biomedical ethics that exist in healthcare to technology specifically SSI & user sovereignty.

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

"The physician must ... have two special objects in view with regard to disease, namely, to do good or to do no harm."
Hippocrates, Epidemics (book I, section. 11) c. 410 BC

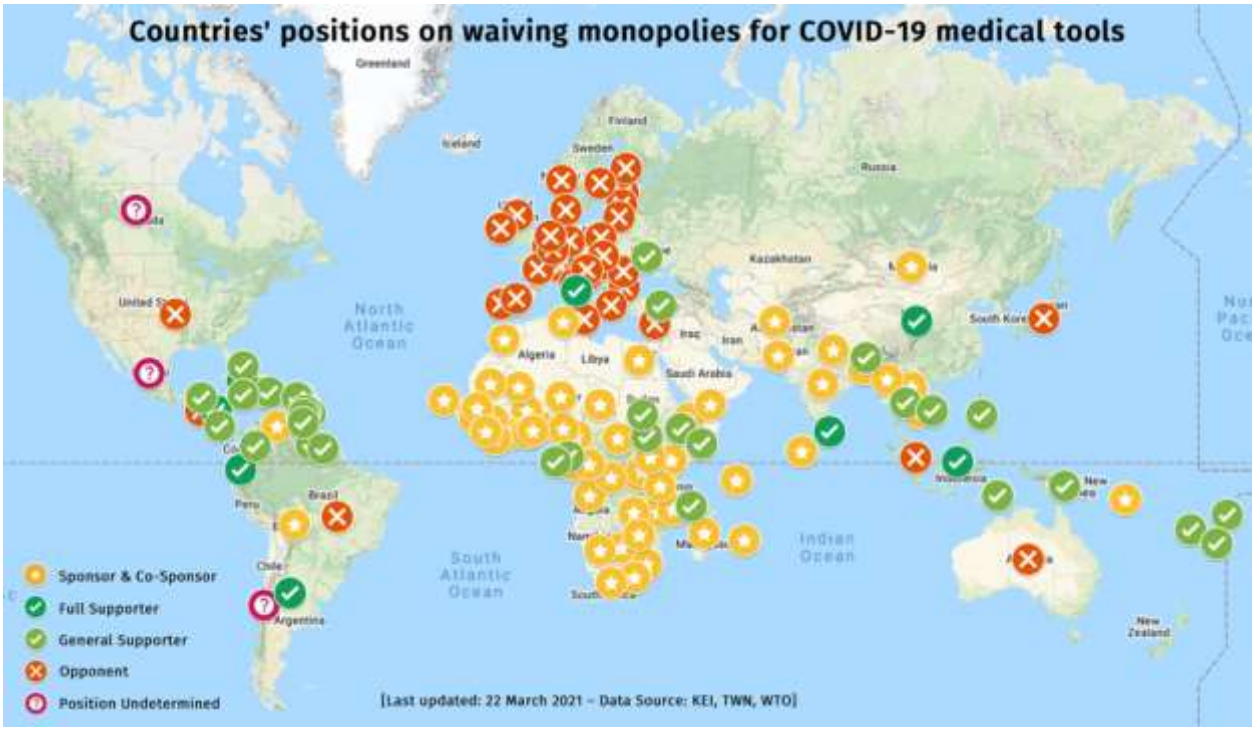
- Autonomy – respect for the patient's right to self-determination
- Beneficence – the duty to 'do good'.
- Non-Maleficence – the duty to do 'no harm'.
- Justice – to treat all people equally and equitably for the benefit of society.
- 4 principles of biomedical ethics

No more in my everyday life have these four pillars been so important to me as they have been over the past year.
I clutched on to these while delivering care to patients gasping for breath, clinging onto life and some sadly succumbing to COVID-19.
The most challenging time I have ever had as a doctor and as a being.
Not only has it impacted people's health & mental wellbeing directly and indirectly through restrictions, delays in treatment for other illnesses but also economically and societally.
It has been a difficult time for most with events highlighting the widening inequalities we knew already existed.
Reflecting and remembering on these times it would be grueling 17-18 hours days on the frontline, which would include treating your colleagues, worrying about personal protective equipment (PPE) stocks, equipment, and oxygen supplies.
Arrive home to see social media posts from connections in the identity and technology world talking about immunity passports, sensitivities & specificities of Covid tests, and how their proposed solutions could solve problems.
Many well intentioned, some purely commercially driven, however all like many things over the past year not very well informed.
There may be many different technical ways to meet a set of product requirements and they all fall on a spectrum from ethical/good-for-individuals all the way to unethical/bad-for-individuals.

However, if we do not understand the exact problem we are trying to solve and the context they become irrelevant or even worse have intended or unintended negative societal consequences.
Do we need a Covid vaccine passport whether this is paper based or digital?
If there is or are contexts where a vaccine passport would be more beneficial than not, what are the technical principles, implementations and considerations that need to be met to ensure that they are implemented to comply with medical ethics and law?
After all this is personal health information and therefore should be treated as such.

What problem are we really trying to solve with a Covid Vaccine Passport, Covid Passport, 'Covid' credential, digital green certificate, or any other named health pass solution?
To do this there needs to be a basic understanding of this infectious disease, what tools we have currently to deal with it and address assumptions that have been made, many of which may change or are yet unknown such is the dynamic nature of a pandemic.

Disease Severity COVID-19	**No disease**	**No illness**	**Mild illness**	**Moderate illness**	**Severe illness**	**Critical illness**
		Asymptomatic -Infected with the virus and do not show any symptoms				
		Pre-symptomatic – early in infection when symptoms & illness have not yet developed				
Infected with virus SARS-Cov-2	✗	✓	✓	✓	✓	✓
Infectious – Could you pass the virus on to someone else	✗	✓	✓	✓	✓	✓



Access to Medicines Medecins Sans Frontier

Yellow fever is the only disease specified in the International Health Regulations (2005) (IHR (2005)) for which countries may require proof of vaccination from travelers as a condition of entry under certain circumstances and may take certain measures if an arriving traveler is not in possession of such a certificate.

This is not about Covid Digital Vaccine Passports.
It is greater and more important than this is about personal health information.
How systems and technology is implemented in healthcare and what ethical framework are they held to?

Medical Ethics	Medical Law	12 Principles of SSI	6 Principles of User Sovereignty
Autonomy	Consent Confidentiality/Privacy Access to Records	Interoperability Control & Agency Privacy & minimal disclosure Portability Security	Privacy by default Pseudonymity by default What, not who, for authorisation Revocable, permissioned-based relationships between people and technology
Beneficence	Negligence Law	Verifiability & Authenticity Transparency	Strong open encryption Open standard protocols & formats for all data What, not who, for authorisation
Non-Maleficence	Criminal Law Negligence Law Regulation	Verifiability & Authenticity Transparency	Strong open encryption Open standard protocols & formats for all data What, not who, for authorisation
Justice	Anti-discrimination law	Representation Participation Equity & Inclusion Usability, Accessibility & Consistency	

"Only a life lived in the service to others is worth living."
— Albert Einstein

Thank You
manreet@truu.id
@ManreetSNijjar

UDDI & UDDR - Common Language Once & For All?

Thursday 20D
Convener: Jeff Aresty, Scott David, Jean F. Queralt, Karim
Notes-taker(s): Scott David

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

Notes from first session:

Meeting Session 1:
Room D

Host Aresty, Queralt, David

Query of nature of governance and role of programmers.

Who "makes" the law?

Declaration of human rights is helpful baseline on structure. Useful to get to point with universal framework.
Notion of universal rules: Notion of universality
What is nature of lawmaking.

Why should lawyers, politicians have a monopoly on lawmaking in area that don't understand. People are making laws in action. From norms.

GO to where the justice fields are green – stateless areas. There is paradigm of need. Aiming at public international framework.

Where develop these new approaches to governance.

Universal declaration of human rights: Challenge is not what do online, but how take existing rights and move them online. Problem is 2 million years experience on physical experience, 10k years of legal experience, but only 10 years of digital personhood.

What is nature of harm and protection.

Consider legal algorithm: Harm, rights, duty, breach, causation, damages, liability, insurance

What is personhood onlie that can be equivalent of protection offline.

What is centricity of perspective: digital, human, propostional transparency and data controls. Semantic notice and control for people. Reduce scope of wormhole of law.
Reverse the transparency requirements. Organizations

Need protocol at time of interaciton

Interesting notion of putting onius on organizations to be transparent

What is governance?

What is legislation?

What is rulemaking?

Notice and consent is inversaion of power relationship by using existing rights

Notice and consent is pathway to inversation of power AND an artifact of power. The choreography is fixed..

Parts of universal document to cover human rights:

1. Legal document centered toward data
2. Technical translation of document – compliance with regulation – but difficult without standard implementatiokn.
3. Digital rights SDK – incorporate to softarre architecture

Can test compliance and standardize – data linked to representational entity.

Modules of Trust Frameworks
Disconnect of responsibility of programmers
Can link impact of action with responeiilituy.

Incorporat to educational pipeline.

Problem is not the data, it is the decision making process.
Need to start with harms that data can cause. Data processing is transformation of data. That is till point of decision of index harm.

Need to correlate tech with rights under taxonomy. Apply algorighms or indexes of harm.

When does a person become a person digitally? When data is exposed online or when they are first online? What is nature of that status?

Personhood – Certain amount of data points infers a person.

California law – is there opportunity to have trust framework law establish threshold for personhood.

In US reverse of EU, privacy is not default setting. Organizations tell you of risks before you engage. Consent by design. If backtrack. Trust framework is the culture itself. Want it extended digitally.

Technical versus non-technical issue: What is human readable and machine readable?

Semantic stack – ISO 2100 – has name for each person. Can map people to roles. Generic roles and stakeholders. What is missing is technical understanding of these. Purpose is not consistent across the stack. NO shared meaning across the stack.

Digital legal ontology extension to words. Might include in text to aid word search.

Revisit question on when do you become digital personhood.
We umnderstand physical person.
Legal person
What is digital personhood. Data online – is it a body. Is it physically me? What if not property, what is digial body – then look at rights framework. IF data is body, then rights frameworks If data is property then another set of rules.

Digital personhood as digital personhood.

Mary Rundle paper -on personhood.

Issue of nature of personhood. What is it, how defend it?

Need to know what it is before know how to defend it.

Data needs context to be valuable

Constitution protecting me, why not protect the data.

Query of nation states.

Nation states more human interst than corporations.

What is minimial set of data for a schema to be useful? Is this established in context.

Object identity and utility determine number of dat appoints.

Perhaps need digital eqjuialent of equity.

Query of what are standards of care?

Some say

I am my data
End remedy – control within bounded space
Rights by design

Reliance on systems.

Expectation of derisking. Technical standards. Unversality.

Standards.

Working on enotary system.

ZOOM CHAT:
From Mark Lizar1 to Everyone: 10:03 AM

http://emoglen.law.columbia.edu/LIS/archive/privacy-legis/ISTPA-FrameworkWhitePaper013101.pdf
From Marc Davis to Everyone: 10:03 AM Here is a link to a brief video about what I was talking about in terms of digital rights for persons that was presented to "the Elders": https://vimeo.com/505044316
From Kaliya Identity Woman to Everyone: 10:04 AM do you have a note taker?
From JFQueralt to Everyone: 10:04 AM @Kaliya: Scott.
From Scott David to Everyone: 10:04 AM Me. I am taking them in word, and will transfer them over.
From Marc Davis to Everyone: 10:08 AM From "Notice and Consent" (Contracts of Adhesion) to "Computational Contractual Negotiations" (Real Agreement)?
From Mark Lizar1 to Everyone: 10:09 AM Scott is the global expert in risk of Harm!
From Scott David to Everyone: 10:10 AM Just one of the 4 horsemen of the risk-o-polous!
From Karim Stekelenburg to Everyone: 10:10 AM A concept for (technical) governance framework: https://github.com/hyperledger/aries-rfcs/blob/master/concepts/0430-machine-readable-governance-frameworks/README.md
From Me to Everyone: 10:13 AM we definitely want to use existing legal frameworks, but recognize that they do not have any absolute power in cyberspace - cyberspace is like another country, and, existing lawmakers are passing laws that intend to reach conduct which occurs in cyberspace which may have impact on their citizens - but good law requires efficacy, order and impact; any law which operates in an extraterritorial fashion (and I contend that laws affecting conduct in cyberspace by definition are operating in an extraterritorial way) have serious enforcement problems; and, to the extent that laws coming from different jurisdictions are in conflict, there is no order; impact of laws is random in this sense. The bottom line is that we need to build a new framework, but recognize the roles of the existing lawmakers
Rachel has her hand raised
From Mark Lizar1 to Everyone: 10:16 AM We need transparency and accountability - we call it OPN - transparency over the control of data (to start online digital accountability and enable dynamic data controls/economy)
From Marc Davis to Everyone: 10:18 AM There is an a prior definition exercise which this discussion requires: What are the relationships between "data" and the "person" and what rights does that person have (and GDPR is not the final answer)?
From Mark Lizar1 to Everyone: 10:18 AM We have been working on computation privacy for quite a long time..
From Marc Davis to Everyone: 10:19 AM Need to define relations among "Physical Person" and "Legal Person" and "Digital Person".
From Mark Lizar1 to Everyone: 10:20 AM Kaliya - what's that OECD paper from 10 years ago — Geneva etc — Digital Identity & Person Hood -published by OECD ?
From JFQueralt to Everyone: 10:22 AM @Racheel: Schema based?
From Rachel Sv to Everyone: 10:23 AM It could very well be, or systems thinking
From JFQueralt to Everyone: 10:24 AM @Rachel: Can you expand?
From Mark Lizar1 to Everyone: 10:25 AM https://github.com/dpvcg/dpv
From JFQueralt to Everyone: 10:25 AM @Karim: https://institutionalgrammar.org/wp-content/uploads/Instructional_materials/IG-2.0-Cheat-Sheet-v1.pdf
From Mark Lizar1 to Everyone: 10:28 AM https://www.iso.org/standard/45123.html
From Rachel Sv to Everyone: 10:29 AM I would but I am hopping off. Mark is explaining what I mean with systems thinking which is engaging with all definitions of "human"-centered design in that humans have varying degrees of definition. (Disclaimer: no expert!)
From JFQueralt to Everyone: 10:29 AM Thx!
From Rachel Sv to Everyone: 10:29 AM Thanks all!!
From Kaliya Identity Woman to Everyone: 10:32 AM https://www.oecd.org/sti/ieconomy/40204773.doc
From Trevor Butterworth to Everyone: 10:33 AM Richard Feynman saw his thoughts as not being divisible from the paper they were generated on (in other words, the brain, hand, pen, and paper were all part of a

single neural circuit). Just throwing out the idea of digital personhood as being a neural circuit that is part of the physical personhood in the same way that the paper and thought were for Feynman.
From Scott David to Everyone: 10:34 AM +1 Trevor. Situated cognition. See Andy Clarke. Beautiful.
From Trevor Butterworth to Everyone: 10:34 AM That's who I was channeling. Have his book, haven't read it yet.
From Scott David to Everyone: 10:35 AM The mind exists in language and culture. The brain is merely an antenna tuned into the local mind. This is not a pipe! This is not a mind! Humans invented all sovereigns - deities, royalty, countries, companies. Next up - computational sovereignty.
From Mark Lizar1 to Everyone: 10:35 AM Computational privacy - is a paper I am trying to write up
From Trevor Butterworth to Everyone: 10:36 AM Yes—I think, therefore I generate data. It doesn't matter what the substrate is.
From Scott David to Everyone: 10:36 AM Data plus meaning equals information We need meaning security/integrity for information integrity.
From Mark Lizar1 to Everyone: 10:37 AM What is missing from this conversation is the discussion of state.. If a tree falls in a forrest and no one is there - does it make a sound
From Scott David to Everyone: 10:38 AM Beware tautologies! Nation states as human stewards? Maybe get variable results!
From Mark Lizar1 to Everyone: 10:38 AM The transaction receipt is a way to make a notice of a record for something that we can't see or hear
From Marc Davis to Everyone: 10:38 AM John seems to be is in the frame of "Digital Person" is my digital embodiment, not my property or expression.
From Me to Everyone: 10:38 AM Our approach is to treat cyberspace as a new state, or, a new country; all of us have a stake in defining the rules which will create trust and order in this space; governments have a seat at the table, but not veto power
From Mark Lizar1 to Everyone: 10:38 AM Capturing the state is proof
From Marc Davis to Everyone: 10:38 AM Sorry "Jean"
From Mark Lizar1 to Everyone: 10:39 AM I capture my own state of personhood then apply it with rights online to assert person hood
From Me to Everyone: 10:39 AM +1 Mark
From Mark Lizar1 to Everyone: 10:40 AM We Call that Consent By Design
From Marc Davis to Everyone: 10:41 AM My Data as My Digital Body (My Data is Me) vs. My Data as My Digital Property (My Data is owned by Me) vs. My Data his My Digital Expression (My Data is created by Me). Need to clarify which frame is at play.
From Trevor Butterworth to Everyone: 10:41 AM But the digital and the physical (political state) are interpenetrated. A bit like Northern Ireland: two religions each with a different sovereign allegiances coexisting and interacting. The EU allowed this dual state to exist peacefully. There was a higher law. Of course, it's been blown up by Brexit.
From Mark Lizar1 to Everyone: 10:44 AM Self-asserted - capability to mitigate risk myself -
We are working on a trust framework for CyberNotary to enable self-assertion of person hood
Explict consent for data transfers — We need the power asap
From Trevor Butterworth to Everyone: 10:45 AM Where do I go to follow this issue?
From Me to Everyone: 10:45 AM jeffaresty@internetbar.org
From JFQueralt to Everyone: 10:46 AM JFQueralt@TheIOFoundation.org
From Kaliya Identity Woman to Everyone: 10:48 AM Have everyone write their information in the notes session.
From Mark Lizar1 to Everyone: 10:49 AM mark@0pn.org
From Marc Davis to Everyone: 10:49 AM MarcDavis@alum.mit.edu From Trevor Butterworth to Everyone: 10:50 AM trevor@indicio.tech
From Karim Stekelenburg to Everyone: 10:51 AM karim@animo.id

From Scott David to Everyone: 10:53 AM Also, restate the question not as “is MY data me”. To is that data about me, me? Programmers are priethood
Equitable programmers guild?
From Mark Lizar1 to Everyone: 10:53 AM We are working on this as a codes of transparency practice for online public notice - so people can use their physical rights online -
From Scott David to Everyone: 10:54 AM Guilds have ethical codes Apprenticeship Guild members travel across sectors and jurisdictions carrying their standards with them.
From Mark Lizar1 to Everyone: 10:54 AM OPN - Provides a Notice and Notification UI that is designed to information people if the digital online environment is what they expect it to be or not. And the work for this is going on at Kantara -
https://kantarainitiative.org/confluence/display/WA/Privacy+as+Expected%3A+UI+Signalling+a+Consent+Gateway+For+Human+Consent
From Scott David to Everyone: 10:54 AM I am jumping to next session I am hosting. I will post notes.
From Mark Lizar1 to Everyone: 10:55 AM Mee too.. thanks :-)
This was the conversation I was searching for — !!! Jeff +1
From Marc Davis to Everyone: 10:55 AM Great session! Thx!
From Trevor Butterworth to Everyone: 10:55 AM Excellent!
From Me to Everyone: 10:55 AM thank you, all
From Mark Lizar1 to Everyone: 10:55 AM https://github.com/Open-Notice/OPN-Workshop-05-04-21

WHiSSPRr Risk for People

Thursday 20E
Convener: Sal D’Agostino
Notes-taker(s): Sal D’Agostino

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:


Surveillance Inversion
• Today -> Enterprise Information Risk Centric Security and Privacy Frameworks
• Risk of Breach and Recovery of the Enterprise (not people)
• Lack of Transparency, Proportionality and Reciprocity in Online Transactions
• One-way contracts of adhesion
• Clear and Apparent Risk to People is Missing from Online
• And consent is a human thing
• Traffic Signals for People (not risk of people in databases)
IIW32, OpenConsent, IDmachines Risk for People


WHiSSPRr
There needs to be an understanding of the different types of risk and order in which to assess them. Only then can it be made clear (to people) and be able to best manage personal (physical and digital) risk. This tends to minimize the risk profile and the operational requirements for (enables) decentralized governance, independently of any identity framework.
• White Hat
• Identity
• Surveillance
• Security
• Privacy
• Risk
• Rating
IIW32, OpenConsent, IDmachines Risk for People

- Fine grain identity management is an alpha surveillance technology
- There is an explosion of information
  - Cloud, IoT, Moore's Law (include pixels)
- The security is focused on information ***in*** the identity management system (enterprise information, including cloud).
- It is easily exploited.

IIW32, OpenConsent, IDmachines Risk for People

Notice of Risk Before Engagement

- Start with who you are dealing with, akin to LEI
- Physical locations (lat, long, MAC, IP, cell SIM, street) of entities is critical

Notice (Receipt) of Rights After Engagement

- Driven by locations and purpose
  - Has a legal basis
- At this point a controller can be introduced

IIW32, OpenConsent, IDmachines Risk for People

Wallet Security & Hardware-backed VCs - Privacy Challenges & New DIF WG Incoming

Thursday 20F
Convener: Paul Bastian & Micha Kraus
Notes-taker(s):

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

https://lists.identity.foundation/g/wallet-security
Wallet Security wallet-security@lists.identity.foundation

The WG will design and define secure wallet architecture, establish common terminology, produce guidelines, classify and specify security capabilities and best practices, and more.

When the Subject cannot be the holder

Thursday 20H
Convener: Sam Curren
Notes-taker(s):

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

Quick intro outline: https://hackmd.io/HhLGtxBPSeGpxtp30S5tOg

Talked about the problem, and existing solutions to this.

It's possible that the intent of the law is not being met, if a provider refuses to share data on behalf of a user.

OpenID has a function for distributed claims that provide a URI and an access token for retrieval.

JWTs have AZP - The authorized presenter of a credential. The issuer may be the authorized presenter.
If the issuer wants to use existing protocols, a credential can be issued which functions as a 'shadow' of the main credential. Presenting the shadow credential provides consent for the verifier to ask for a presentation of the main credential from the issuer.

Could An NFT Be A VC?

Thursday 20I
Convener: Grace Rachmany
Notes-taker(s): Grace Rachmany

Tags for the session - technology discussed/ideas considered:

Certification, credentials, NFT, Community currency

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

Case discussed: A group of villages in Africa using a cryptocurrency platform for alternative currencies. Different organizations issue the coins under different circumstances. When you accept a currency, you want to know who is the issuer. The Red Cross might be more or less trusted than the local leader or agricultural cooperative as the issuer of a currency that is supposedly equivalent to a shilling.

What types of tech could be used for this?

- Multiple currencies on the blockchains
- Certifications in the form of some kind of NFT issued by the issuer.
- Limited supply tokens or NFTs that are "expired" when you use them
- Open Credential Publisher framework was suggested
- VCs are generally authorizations associated with a person, so maybe a person could have the VC and show their credit rating in some way while they are making a transaction
- Similarly maybe the VC belongs to the organization that is issuing the coin, proving its reputation over time.

Device-Free SSI: Ideas, Potentials & Challenges

Thursday 20J
Convener: Nuttawut Kongsuwan
Notes-taker(s): Charles E. Lehner

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

Most realizations of self-sovereign identity (SSI) utilize some forms of local, personal digital wallets, especially smartphones. However, a large proportion of the world population, in fact, do not own nor have access to any smart device. In this session, we discussed the potential of device-free self-sovereign identity where a user can take full control of their digital identity without the need to have a smart device. We also discussed security requirements for such a solution and outline relevant cryptographic protocols that could be used to realize it.

ZOOM CHAT LOG:

Catherine Nabbala, 10:56:43 AM

For offline discussions, pls email: win@finema.co

Frederico Schardong, 11:01:05 AM

Some people argue that most biometrics (facial recognition, iris, etc) cannot be used for authentication, only for identification. The reasoning behind this is that we leave biometric prints everywhere we go and can't do much about it. We touch things, we show our faces, we look at things.

Drummond Reed, 11:02:54 AM

+1

Eric Welton (Korsimoro), 11:14:35 AM

@Frederic

I think there might be a possibility of merging the IBV, CBV, and key operations (along with liveness) to overcome some of that

at Thoughtful Biometrics Conference we had a couple of discussions on this topic - is the *only* viable use of biometrics either (a) unlocking TEE devices (using closed-supply-chain technology like an iPhone)

or (b) for surveillance - i'm not sold yet that the general wisdom about biometrics is the final story - although I am sympathetic to that concern

Frederico Schardong, 11:21:58 AM

Having a bunch of biometric combined increases the security assumption, which is always welcomed. There are other things like what if someone doesn't eyes and/or hands?

Matthewhall78, 11:24:17 AM

What specifically on the terminal needs to be protected? Is it the formula that generates P and R. Could you do some sort of verification of state that the formula has a VC that states it has not been tampered with? I don't know just a thought.

Charles E. Lehner, 11:25:51 AM

Have one-time-use paper credentials been considered?

Frederico Schardong, 11:26:25 AM

+1

Takashi Minamii 11:29:45 AM

FYI:Hitachi's Solution (PBI)

https://www.hitachi.com/rd/sc/story/pbi/index.html

Matthewhall78, 11:30:12 AM:

maybe one time use paper credentials could work as a means of going analog temporarily, but they could be verified after the fact. e.g. hey Matt, someone used a paper credential asserting to be you, what it you? Yes or No?

Charles E. Lehner, 11:32:01 AM:
I was thinking of one-time-pads

Matthewhall78, 11:32:06 AM:
Payment terminals all just had to change to add the “tap” function

Q&A

Question about KERI, key rotation
Reusable Fuzzy Extractor
Reused parameters not correlated

Chris Raczkowski, 11:42:21 AM:
Great session! I’m looking forward to following up with Finema on this topic - particularly with Sovrin’s plans for integrating biometric binding into an open-source SSI wallet and VCs. I have to jump, and prep for another session - and I’ll connect again via email and LinkedIn. Thanks!

Solution should be compatible with Confidential Storage Working Group, so you can move vendor, transfer keys/credentials.

Discussion about group shared phone. Shared biometric wallet that a family could log into. Anyone in the family could carry that phone around. Or community phone. May tend to be one person who uses it most.

Separate devices already having biometrics.

Governments not carrying about personal sovereignty, not excited to adopt. Need middleman, charity, W3C, etc.,
NGOs. What are we trying to do?

Myanmar, NGO workers. Illegality to possess cryptographic materials.

APAC call

Thailand connections. Bangkok.

Using real name, vs. what people call you

LinkedIn connections.

Sovereign, vs. KYC. Supreme political entity. How to help individual in dire straits.

What technology using? Blockchain: Tendermint Consensus Engine, not Hyperledger Indie, but borrowing ideas from it. Using DID and VC

Covid in Bangkok

GLEIF vLEI with KERI

Thursday 20K

Convener: Karla McKenna
Notes-taker(s): Karla McKenna

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

The Global Legal Entity Identifier Foundation (GLEIF) proposes that the Legal Enitity Identifier (LEI) can be used to establish a chain of trust for organizational identity.
In this session, GLEIF shares plans and progress regarding its development program to create an ecosystem and credential governance framework, together with a technical supporting infrastructure, for a verifiable LEI (vLEI), a digitally verifiable credential containing the LEI.

Link to presentation available until April 2022:
https://td2ec2in3mv1euwest.teamdrive.net/bgvkygms/public/I39DS3Tn?k=MMiiLXItHvmxOtB0kFROQGXMTDFgjCngWTiQFed43Ak

Why You Know Less About Guardianship Than You Think (Because We ALL Know Less About Guardianship Than We Think)

Thursday 20L
Convener: Jo Spencer, John Phillips, Sterre den Breeijen
Notes-taker(s): sankarshan

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

Link to the deck we'll use to start the conversation:
https://docs.google.com/presentation/d/1aGTPmlno3WScpSYMs1HLhWsrVRx9B-I0yhOQsRgmqRw/edit?usp=sharing

Do we need to get more people interested in the "real life" application of
Four groups of people at IIW conferences?

- Technologists
- Idealists
- Pragmatists
- Entrepreneurs

1. [Sterre] introduction ; also of TNO
    1. Kudos to Jo and John for the slide deck

2. In 2019 the Sovrin Foundation published a whitepaper on Guardianship; transitioned into the Working Group
    1. APAC and NA/EMEA WG meetings
    2. 2 key documents from the WG are going to be published by Sovrin Foundation - https://sovrin.org/a-deeper-understanding-of-implementing-guardianship/
        1. Implementation guidelines
        2. Technical requirements

c. Why are we looking at Guardianship and SSI?
    1. Guardianship is a part of life - we are rarely fully self-sovereign or independent
    2. Guardianship is not a part of SSI at this moment - is a missing ingredient in our digital lives
    3. The group thought guardianship was a simple concept
        1. Small set of SSI building blocks …
        2. Gap between use cases and requirements was too broad (see slides)
        3. A mental model for guardianship was required (see IIW30 and IIW31 for further context)
        4. 'Squiggle' - the journey
    4. 5 things the team worked out
        1. Jurisdictions are essential (gives meaning to the guardianship relation)
        2. Should work with existing laws
        3. Guardianship can be built on verifiable credentials
        4. Build a mental model (and test it) - 15 functional requirements, 6 technical requirements, 3 validator requirements
        5. Don't build guardianship solely on wallets (mitigate the risk of wallet takeover and impersonation)
    5. Transparent vs Opaque guardianship scenario
    6. 5 things to consider
        1. Should discovery be enabled
        2. Ensuring appropriate representation
        3. Receiving parties are key
        4. Balancing agency, dignity and care
        5. Transitions : recovery, expiry and ends
    7. Alignment with SSI and ToIP
        1. Guardianship creates a tension between independence and dependence
        2. An obvious relationship with the ToIP (the ToIP model/diagram)
        3. Mapping concepts of Guardianship with the Trust Triangle diagram
    8. Parties, Actors and Action pattern

d. https://essif-lab.pages.grnet.gr/framework/docs/notations-and-conventions

e. https://www.researchgate.net/publication/348325716_Decentralized_SSI_Governance_the_missing_link_in_automating_business_decisions

GS1 2021 VC Prototype Journey

Thursday 20P
Convener: Paul Dietrich
Notes-taker(s): Paul Dietrich

Tags for the session - technology discussed/ideas considered:
Compatibility, POC, Prototype, GS1, Learning,

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

- A overview of the GS1 Prototype effort for Q1-2 2021.
- Some discussion on convergence of the ecosystems.
- There was some feedback that BBS, PE, and DIDCommV2 are possible points of convergence.
- Also comments that WACI Bloom may play a part in convergence

DIDComm and the Self-Sovereign Internet

Thursday 21A
Convener: Phil Windley
Notes-taker(s): Phil Windley

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

Link to Phil's Slides:
https://docs.google.com/presentation/d/1h0qi2qyGwM30DHpRAXW_Y0bBneo9xMEFZh1rIAeRa-E/edit?usp=sharing

Summary: DIDComm is the messaging protocol that provides utility for DID-based relationships. DIDComm is more than just a way to exchange credentials, it's a protocol layer capable of supporting specialized application protocols for specific workflows. Because of its general nature and inherent support for self-sovereign relationships, DIDComm provides a basis for a self-sovereign internet much more private, enabling, and flexible than the one we've built using Web 2.0 technologies.

DID-based relationships are the foundation of self-sovereign identity (SSI). The exchange of DIDs to form a connection with another party gives both parties a relationship that is self-certifying and mutually authenticated. Further, the connection forms a secure messaging channel called DID Communication or DIDComm. DIDComm messaging is more important than most understand, providing a secure, interoperable, and flexible general messaging overlay for the entire internet.

Most people familiar with SSI equate DIDComm with verifiable credential exchange, but it's much more than that. Credential exchange is just one of an infinite variety of protocols that can ride on top of the general messaging protocol that DIDComm provides. Comparing DIDComm to the venerable TCP/IP

protocol suite does not go too far. Just as numerous application protocols ride on top of TCP/IP, so too can various application protocols take advantage of DIDComm's secure messaging overlay network. The result is more than a secure messaging overlay for the internet, it is the foundation for a self-sovereign internet with all that that implies.

Because of the self-sovereign nature of agents and the flexibility and interoperable characteristics they gain from DIDComm, they form the basis for new, more empowering internet. While self-sovereign identity is the current focus of DIDComm, its capabilities exceed what many think of as "identity." When you combine the vast landscape of potential verifiable credentials with DIDComm's ability to create custom message-based workflows to support very specific interactions, it's easy to imagine that the DIDComm protocol and the heterarchical network of agents it enables will have an impact as large as the web, perhaps the internet itself.

More here: https://www.windley.com/archives/2020/11/didcomm_and_the_self-sovereign_internet.shtml

(California) Verifiable Credentials Policy Committee - Come Learn About How To Participate in Passing Legislation to Create a California Trust Framework!

Thursday 21B
Convener: Kaliya Young, Ally Medina

Tags for the session - technology discussed/ideas considered:
Policy, Legislation, Verifiable Credentials

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

Link Slides:
https://docs.google.com/presentation/d/1VyxmWan3qbxynxhKvw1CHhWZINiPRF9gjeqSCSDh1MY/edit?usp=sharing

TLDR: We discussed how the Blockchain Advocacy Coalition's sponsorship of AB 2004 pushed verifiable credentials into mainstream political discourse and how companies can help us shape public policy and government pilot programs of Verifiable Credential technology.

We are planning on working with legislators to introduce a bill that creates a California Trust Framework and lays the groundwork for use of the technology in the public and private sector.

Our coalition is funded by the companies who participate in it. If you are interested in being part of shaping legislation in California the will build the market for your tools and services please be in touch. Remember what happens in California shapes what happens nationally and has a global impact.

Ally Medina - head of the Blockchain Advocacy Coalition - ally@blockadvocacy.org
Kaliya Young Chair of the Verifiable Credentials Policy Committee - Kaliya@identitywoman.net

Solving Identity Challenges at the Intersection of Education and Healthcare

Thursday 21C
Convener: Kimberly Linson
Notes-taker(s): Kimberly Linson

Tags for the session - technology discussed/ideas considered:

https://app.slidebean.com/p/6acrochkpj/IIW-April-22-2021

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

Key observations from the powerpoint:

State agency feedback:

- Identity is at the heart
- Disconnect between the data desired and the data entered
- Confusing fields, more confusing mapping
- Mismatched data
- Stick to 99% of a standard

School has changed:

- Used to be:
    - District organized by physical location
    - Revenue systems based on seat time
    - School buildings
    - Classrooms divided into grades
    - Teachers as *sage on the stage*
- COVID:
    - Some kids still out of school
    - Playlists, virtual classrooms, hybrid
    - Access to food. Access to internet. Access to a device.
    - Teachers maxed to the limit
- FUTURE:
    - Learning Loss?!?
    - Social Emotional Learning?!?
    - 1/3 of students expected not to return
    - Virtual models abound
    - Teacher mobility and agency
    - Chaos versus Opportunity?

Questions for discussion:

- Identity technical solutions are easy. The data clean up and alignment is the first problem to solve.
- How can self attestation be trustworthy?
- What are the responsibilities of a proxy issuer?
- How far can we move people's cheese before they rebel?

- Common issues across all industries
- Cognitive dissonance - the people who are trying to solve the problem aren't the boots on the ground.
    - EGO
    - Structural challenges
- Everyone thinks it's a change to technology but it's really a change to PROCESS
- Who is in control of the data?
    - Institution/Agencies - THEY DON"T OWN
    - Once the user has it then they can give consent
    - Old thinking...need to show them how it doesn't work
    - Moving cheese...can't mess with the revenue!
    - Must change the process within the HR department
        - This is the way for adoption.
- Adoption requires an ecosystem
    - Nuclear - is a closed ecosystem with many credentials - this is a perfect use case
    - BUT problem is true SSI is the ability to authenticate a digital presentation out side of the ecosystem
        - This is the verifiable credential
- Must adopt the same protocol!
    - TRUST - 2 separate concepts
        - Attributional - who said it
        - Reputation - Who cares that they said it
    - Cultural data control - not wanting a different problem
- Blockchain isn't the solutions because of ledger lock
    - Doesn't work for Identity
    - Identity is about giving people their stuff!
    - KERI will take over everything
        - READ: keri.one (Sam's Chapter 10 of the Manning SSI book)
    - Blockchain is good for:
        - Double spend proof across the ecosystem
            - Crypto
            - NFTs
- We have to get to protocol/standards like we did with email
    - It will be messy and competitive with new players who emerge and offer more freedom
    - Those who can't adapt will lose ground - need to be willing to let go
    - Messaging apps: Signal/What's APp - PRESSURE...eventually someone will make it so that they work together and scoop up everyone's business
- Application layer must converge before
    - LInkedIn/Twittter doesn't control you with their data...they control your relationships…
    - Peer to peer
- Every topic seems to boil down to adoption!

The World Between Public & Private DIDs - Or How To Make Use of SSI Without the Subjects

Thursday 21D
Convener: Matthias Loepfe, Cardossier CH
Notes-taker(s): -

Tags for the session - technology discussed/ideas considered:

Slides: iiw-between-public-and-private.pdf

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

- It was very hard for me to explain the problem I'm searching a solution for and equally for the proposed solution ideas.
- We discussed a lot of more philosophical questions and if peer-dids are a good thing or not and if it is worth trying to minimize correlation when any involved party anyway stores the personal data of the related persons. I think we should make it as hard as possible to correlate data, even if we can not completely prevent it.
- We also discussed the potential complexity of such a solution and if it is worth it. The conclusion was to minimize the number of personas one should (be forced) to hold, such that it is still easy to maintain.

Verifiable Credentials for Assets <30 min

Thursday 21E
Convener: Mahmoud Alkhraishi
Notes-taker(s): Mahmoud Alkhraishi

Tags for the session - technology discussed/ideas considered: Asset VCs, Supply Chain

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

General Framework on how to think of VCs for Assets including leveraging GS1 and other vocabularies in the traceability vocab.

Requirements and Opportunities that block adoption of VCs in Supply chains

Current Status of work and Steps Forward
https://pmandic-my.sharepoint.com/:p:/g/personal/mahmoud_mavennet_com/EawHRlN0VqpPhiXxZfTnWdMBZxvZuIuA7_kAlEJDWEtthg?e=NVGUnK

Universal NFTs as Authentic Data Without Tokens/Blockchains. How To Eliminate Minting/Mining Fees & Break the NFT Silos.

Thursday 21F
Convener: Dave Huseby
Notes-taker(s): Dave Huseby

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

This session described how we can use the authentic data solution to track provenance and controllership of digital data and effectively create NFTs, now called NFADs, that are completely independent of blockchains and tokens. This eliminates minting and transfer costs common on the NFT silos. I have provided link to the slides.

https://docs.google.com/presentation/d/1VaxwE9d4kEvmsJGUMWcvLf5WOQRcv5o_wTGTsecfseA/edit?usp=sharing

Build an SSI Proof of Concept in <30 min

Thursday 21G
Convener: Riley Hughes
Notes-taker(s):

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

The session began with a short introduction to SSI, an introduction to Trinsic, and an overview of how to get started. Then, everybody present starting building an SSI proof of concept, creating issuers, verifiers, and schemas to learn first-hand how it all works. A step-by-step guide on how to replicate this session can be found at the following link:

https://www.notion.so/trinsic/Build-an-SSI-Proof-of-Concept-dae9d6e565eb4770be41b61d55e090cb

Creating A Positive Vision for the Future - Decentralized Web + SSI

Thursday 21I
Convener: Jemima Gibbons
Notes-taker(s): Jemima Gibbons

Tags for the session - technology discussed/ideas considered:

#future #vision #decentralisedweb #SSI #government #consumers #education

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

Intros + why you're here:

James Ebert engineer - how to we communicate trust to end user?
Definitely heading in a good direction.
We haven't done a good job of communicating the apps and what they do

Robert Brennan, software engineer, Maine - have a belief that everything that can be decentralised will be decentralised? Decentralised finance is more egalitarian. First generation is crypto-currencies. Everything you can do in centralised finance now available on decentralised platforms.

Stephen Yates, product manager. Canadian Digital Service. Looking at setting up SSI type identity verification for the Canadian gov.

Mark Scott, Internet security, long-time IIW fan.

Bruce Conrad, software developer, based in Utah currently. To be fully self-sovereign in this world you need to at least have a website, a blog. WE have the opportunity to decentralise but there are lots of forces centralising this.

Sean Jensen, software developer. Generally interested in what the future holds.

Discussion moved to this Miro board:
https://miro.com/app/board/o9J_lII_R8s=/

Zoom chat:
17:03:33 From Bruce Conrad to Everyone :
https://docs.google.com/document/d/1iELB7PlUp_5ZJa9LGxWXium_-pHcXS35MG4oGgDl98s/edit
17:06:14 From Bruce Conrad to Everyone : The title of your book?
17:06:58 From Bruce Conrad to Everyone : Monkeys with typewriters
17:10:05 From Bruce Conrad to Everyone : Another dystopia prediction from 1909: "The Machine Stops" is a science fiction short story (12,300 words) by E. M. Forster. [quoted from wikipedia]

17:16:07 From Bruce Conrad to Everyone : https://www.amazon.com/Monkeys-Typewriters-Myths-Realities-Social/dp/0956263143
17:18:50 From Jemima Gibbons to Everyone :
https://join.slack.com/t/oneteamgovernment/shared_invite/zt-2tsf24lc-zhqjU6GIjWiDem_APXc0BQ

17:19:35 From James Ebert to Everyone : Can I ask Stephen, what part of Canada you're in?
17:20:06 From Bruce Conrad to Everyone : Jemima, you also mentioned a blog post. Do you have a link?
17:22:31 From Jemima Gibbons to Everyone : https://sfadigital.blog.gov.uk/2017/03/24/dont-bring-policy-and-delivery-closer-together-make-them-the-same-thing/
17:22:48 From Bruce Conrad to Everyone : Id4all.me and .global
17:23:42 From Jemima Gibbons to Everyone : https://www.oneteamgov.uk/
17:23:56 From Bruce Conrad to Everyone : thanks
17:36:19 From Jemima Gibbons to Everyone : Miro board: https://miro.com/welcomeonboard/DRQLs1YeZ9DqbWzmXoBVubmSZ2zgt93AelmqxuZVf9q5zqWLyZI7AFxGePI4biNq
17:52:46 From Orie Steele to Everyone : Shameless plug for our work with GS1 on VCs
17:52:47 From Orie Steele to Everyone : https://www.youtube.com/watch?v=iDkANArgdKI&t=15s
17:52:48 From Bruce Conrad to Everyone : GLIEF ?
17:52:57 From Bruce Conrad to Everyone : GLEIF
17:52:57 From colleen to Everyone : GLEIF
17:57:26 From Bruce Conrad to Everyone : Big players moving SSI forward include: GS1, GLEIF, Credit unions
18:01:21 From Stephen Yates to Everyone : James, to answer your question, I am with the Canadian Digital Service.
18:03:29 From Bruce Conrad to Everyone : A dystopia prediction from 1909: "The Machine Stops" is a science fiction short story (12,300 words) by E. M. Forster. [quoted from wikipedia]
18:06:53 From Bruce Conrad to Everyone : The wallet metaphor would imply a person would likely have one of their own choosing. Mine is made of duct tape, e.x.
18:15:37 From Bruce Conrad to Everyone : Added Verified Organization Name project from British Columbia government, earlier in the timeline
18:17:22 From Bruce Conrad to Everyone : UN model law for digital identity
18:28:41 From Jemima Gibbons to Everyone : To continue discussion around gov SSI solutions join the Slack here: https://join.slack.com/t/oneteamgovernment/shared_invite/zt-2tsf24lc-zhqjU6GIjWiDem_APXc0BQ

UX for AR, Ambient Identity, IoT? Human Disclosure, Consent, Auth With Devices

Thursday 21J
Convener: Phil Wolff
Notes-taker(s):

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

Distrust of devices is rising. https://wider.team/2021/04/21/resistiot/ IoT is being felt as the introduction of surveillance. "**Devices are feared and distrusted as proxies for our distrust of the people and organizations behind them."** From the post:

- Clinical technology as **workplace surveillance**. Hospital providers talk about their frustration with connected technologies because it feels like their every motion is being monitored and tracked, used by bosses to evaluate their speed and cost efficiency.
- Civic technologies as **government surveillance**. From Oakland's corner traffic cameras leading to mass rallies to Boston Police tests and NYPD robot dogs, IoT is deep in the creepy depths of the uncanny valley.
- Consumer technology as **commercial surveillance**. Alexa, Google, and Apple know too much about you and use it to sell adjacent services.

Why these feelings?

- **Devices project power into physical spaces** where people live and work.
- **Devices are opaque**: they hide what happens downstream with device data and upstream with device control.
- **Devices don't put nearby-humans at the center of experience**. "User experience" isn't for them but designed by and for absent institutions. When exactly did Amazon Alexa last ask for your consent when you walked in a room? When did Google Nest ask for permission to send your picture to the cloud? What happened to the gigabytes of data produced during your colonoscopy? Who is looking and listening? What bots are judging your behavior or speech?

How can we approach designing common user experiences that address identity of devices, guardianship, who controls their behavior, owns them, consumes their data, and what jurisdictions govern this?

We talked a lot about consent and some of the challenges with designing user interface and user experience for such a wide variety of connected devices.

The identity conversations might start from the familiar web/mobile human-system consent dialogs, like OAuth and UMA facilitate. But we have some prior art.

- NFC dongles that bring human permission to access a building or a computer
- Car doors that permit entry by authenticating fingerprints

But we kept missing fundamental use cases where I could ask a device:

- Who owns you?
- Who controls you if not the owner?
- Who is your guardian?
- What's your history?
- What are you allowed to do for me?
- What do you think I've consented to?

The media for these conversations could be anything from QR-code linking to a mobile/web dialog to an oral conversation ("Alexa, who owns you?"), to a visual display.

On the consent side we kept running into the sheer depth of complexity of information that might be disciplined might be disclosed and the need to keep that information fresh to renew disclosures as activity in the background, behind the device, changes overtime.

Can Kids use D.I.D.s? What's Your Tech For Kids Online?

Thursday 21K
Convener: Erica Connell
Notes-taker(s): Erica Connell

Tags for the session - technology discussed/ideas considered: DIDs, VCs

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

Brief but rich conversation about what technologies may be available and/or practicable or are developing to use with kids and their online presence.

Use case: Wonderland Stage & Screen, interested in developing a platform to support youth creating media to share, comment, discuss their work that meets COPPA guidelines, allows freedom of participants, and provides a mechanisms for privacy.

- Create an onboarding process that models a physical process
- Collect information
- Issue a credential
- Offer wallet options for use
- What kinds of credentials could we use?
    - View only
    - Interactive
    - Comment enabled

International Semantic Infrastructure: Requirements for a distributed data economy

Thursday 21L
Convener: Paul Knowles
Notes-taker(s): Charles E. Lehner, Neil Thomson

Tags for the session - technology discussed/ideas considered:

Data Management - Data Analytics - Linked Data

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

Presentations:

Decentralized Semantics 101
https://docs.google.com/document/d/1Cn-IiEewkFW9K9pneBWFP6xELzd2frfmIvQAoKH2OcY/edit

Overlays Capture Architecture (OCA)
https://docs.google.com/document/d/1IDXJ8QAq-jO87DQt500Rj2SXL0BMUo1_hEK1VDVZ8Ho/edit

Solutions fit for pandemic? No
MSFT: no problem collecting data from multiple sources, but unable to make sense of the data (semantics)

Inputs and Semantics WG and ToIP
Convened to bring semantics to the Identity Community
OCI
Under this WG, task forces: Storage importability, etc.
Vertical: healthcare task force : underneath it, FHIR focus group

Storage. Rebuild semantics so the data is ready to go.

Linked Data

MIT: David Spivak, Ryan (?)

Collection, storage and exchange.
OCA: Rules. Masking Overlay. Flagged. Some sort of algorithm process of what to do with that flagged data. Rules, algorithms: don't think should be in the storage, but closer to the exchange. Then can simplify OCA - Look at that at exchange side. Character encodings, etc., import. Don't want semantics mixed up, as it complicates the exchange side.
Core overlay need to keep at storage part. Other overlays, more rules-based. Conditional. Rules better off at the exchange side.

Exchange side -> Query languages. Searching data - coming from someone looking for data. Insights-based service provider putting searhc into dynamic data sharing hub, does magic to find data. On exchange side.

Linked Data.

Brent Shambaugh. Integrate computing, processing, storage. Virtual machine to integrate databases. Query language, like Linked Data, over a lot of different systems. SeeQL(?) - translate. Categorical databases (Ryan and David's work): to not really rely on a single source ofo truth, but more rely on transformations between things. Use category theory to have an exact/provable way of doing that. Cat theory has to follow certain rules. Cat theory kind of abstract but provides a framework for unrelated disparate things. Ryan could say how to algebraicly describe things, which would branch off into… Josh at Uber: come up with schemas, get down to the data/logical layer. Different places to go. Way to translate in from out. Might have multiple different ones, want to map from each one, but if you have a vague interpediary in centralized model, loosely defined that both map to, then have a mapping between the two things. Linked Data problem

Paul summarizeing. Work at MIT a combo of linked taa and the query language. Veriy sophisticated. Want to pursue integrating with group. But they are missing this restructure.

Labels
Stack structure
Predefined entries

Link data together -> rich semantics lost. Want to say to JSON-LD people, put back together -> need to rebuild semantics on the data, on the human-readable labels If cross border control want credi to be able to resolve into multiple langauges

Burak says, not necessarily true. In layered architecture. If layers considered to add metadata to linkd data nodes, then don't necessarily lose semantics. Ingest data using layered architecture: can incorporate…

Paul says: because pulling data from multipl einputs, the semantics misalign when you pull them together. That's why need to rebuild the semantics. If you miss the semantic rebuild (I know this from clinical trials, they have this for 20 years same problem). Have to rebuild semantics or will be messy at analytics level. Stopped doing analytics because of the data. Went to OCA. Then back to stats.

Neil: God help you try to edit the bits of the code. Need to know much richer stuff to run the code. Get code, first thing to do? Have to build a mental model of what it looks like. If you don't know the semantics, where it came from, it may be absolute nonsense. If want to put Chinese layer on border agents phone, don't need whole layer. Just the executable version. If want to understand labels...
Linking data together is about machine readability. Involved humans… need to understand. Do it through language. Humans like OCA because can understand data in different languages, makes sense for people. Human element. In that capture space. Want to refine OCA, take out some of the rules parts, masking overlay, conditional overlays, and get it away from OCA as architecture - it convolutes things. OCA only meant for making theings human-readable.

Neil: challenge. Presentation … annotates … data exchange, may have to have rules, data type X in one DB, type X-1 over here. If see this value, talking to database cannot support null. What to do with null? Need to specific place for where these rules are placed in the stack. Can still use layer mechanism to identify what the rules are talking to. Alice going to 5 countries, how to find out what VCs need, what questions will be asked? How to do these queries? Suspect things not searchable through SparQL.

Here's how you can walk through the SparQL thing. Need to know what labs ….

Paul: sounds like a governance thing. If built a specification like shown, would expect Chinese government to specify schema database, and their overlays. In Austrait, they specify their overlays on their side.

Data governance authority. Needs to come from proper authorized place. If come to our country, these are the attributes you need.

Neil: giving enough info in the stack so someone searching from country X can say have it or no. International vocabulary. Somewhere so can retrofit on schema. Query vocabulary layer. Can evolve independently of the data.

Paul: data scientist side different. Can use overlay as Burak might want, to do smarter things. Put rules in overlays, use different schema, maintaining context and predefined entries from the issued source. Would like to go there in the Semantics Group. Stripping out things from OCA that don't need to be in Core. Leave stuff for flexibility of data scientist. Collection side: link data in the wild…
High level approach - build something really special.

Neil: Burak and teams looking through, munging data. If model for how code executable chunk… code executable manipulation. Using the metadata in the stack. Operations not just adding attributes: transformations. How to add active actor to do work other than just translation of JSON-LD.

Burak: OCA has special type of overlays, masking or subset, where they should actually not be overlays, should be operations. Layered schema approach is different: treat schema layers as pure metadata coming off well-defined terminology. Build schema to contain linked data containing values, and annotations on values used to ingest the data. Layered schema approach: meaning is evaluated when look at the data, not when you ingest it. Meaning is context-dependend. May have multiple labels, may ingest with one set, but look at with different set of labels, that is when you interpret. That is what linked data gives you.

Paul: that part need to think of a proper use case. Vaccine work.. Governments to dictate objects. Not creating multidimensional code. For this credential, predefined entries. But want to try to make it so that Burak has enough flexibility to do whatever you want outside those core functions the issuers will need to deliver.

Burak: true: layered schema approach purely as metadata. Well-defined functions, projections, Spar(?), transformations on data. Structured OCA limiting it, in my opinion, greatly, because you are too much focused on the capture part.

Paul: it's my life, not going to argue. Know how important it is. Pharmaceutical. Want to introduce to Linked Data community: work done in Pharma stuff hugely valuable: 100 years of structuring data in a beautiful way. Covid stuff: need to be rigid on the layers. But think can drastically reduce them now. Good: sign of good architecture. Reducing functionality right direction. Like DID stuff. Have 96 different DID methods: they probably got it wrong.

Paul Knowles To Everyone Yes please, Brent. That would be awesome.

Burak Serdar To Everyone fyi: Some information about layered schemas is here:
https://layeredschemas.org/

Neil: MSFT. Evolution. Good architecture: Core is immutable but extendable. They put display processing in the core and it blew up. That has to be outside the OS - evolves rapidly over time. Some primitives. What is the core? Can add own layers on top. Analytical layer: what rols is each attribute playing. Attributes can play more than one role. E.g. is this attribute indexable? … things to add on top that don't mess with the core.
"Open/Closed Principle." https://en.wikipedia.org/wiki/Open%E2%80%93closed_principle
Can process any way you want, but what places work.

Paul: can come up with something special. Keep decent structure at storage site, but leave maximum flexibility outside that core. From specs now, I know what I need to do at the capture layer - don't need all the masking. All need ar elabels, predefined entries, diff languages, flag PII. That's pretty much all need.

Burak: believe the separation is artificial. No diff between capture and storage side. Just open-ended layers with defined terminology. Don't agree that should have sensitive overlay or label overlay. Just should have terminology. Layers should not have predefined functions, just be layers.

Paul: not how schema definition works. Need structure at capture side.

Burak: not saying get rid of structure, but restructure so it doesn't have to be separate functional overlays. Still have labels, … enumerations, but they are not separated into different overlays. Just have term in input terminology saying term …, can switch that. As schema-based and overlays.

Paul: defer to Robert

Neil: it's tomatos/tomatoes. We all are agreeing on a layered approach. How you slice it. Problem building an ETL model - going from source A to dest B, is the ETL developer needs to invent each time the internal schema from which you shuffle all the data through. Suck it in through the model and put it back out. Don't have to invent interchange piece: If dealing with vac record, don't need to do that work anymore. … If picking this as core interchange schema, you get all these other things because they have already done that work. … Huge amount of work that just fell off the table.

John Walker: Purpose-built approach. When Gov of China puts out set of code values, there is an intent, the purpose is vaccination receipt/credential. There is a prescriptive set of steps, interpretation of what they publish, that they intend this for its usage. That can be discovered, reassembled, for processing, and in storage. There is a prescription. They are saying there is a context that they are intending the usage for. Reflects back to agriculture which is more prescriptive in pipeline. If know two or three steps or transforms from the source, take advantage of it. Could be discovered, rearranged like Burak saying, yes. But don't want to forget original language. Keep simple

Burak: agree, but then… the work you did with FHIR, OCA: shows that what you just said didnt' really work. OCA/FHIR pipeline outputs OCA schemas/artifacts. Not the right way. Should have had OCA do the transformation. Semantic pipeline in the middle to transform. Produce VC using OCA layers. But that's not how it is working.

John: What we do is start with FHIR bundle, then run a JSON-LD transformation, vs. applying OCA layers, than apply OCA layers after. Think we net to the same place.

For VC/LD Stuff.

Me To Everyone 12:40:15 PM Anything to say about https://github.com/w3c/lds-wg-charter/ ?

Paul: as a semantics team, we should come up with how to go. Naming of stuff not important to me. This whole thing is that my wife doesn't shout at me about that 6G Helsinki app comes up , with everything digitized and out landscape not equipped to deal with that level of automation. If we can all come together to a common place for the benefit of the … solution. Arm wrestle in the core. Outside of that, make sure super-easy to use, people do whatever they want. Data super-structured. If throwing data towards WHO, they can pick it up and do analytics in real time to know how the pandemic is responding. I feel we can get there then I'll be a happy boy.

Neil: … where is the data coming from … Outside VC, data in super-raw form. Same for IOT devices. 5 distinct data organizations to create from the raw stream for different …. Gets bundled into transactions. On top of that, frequently a day to day operational model is created. Keeps going up, more sophistication in each layer, adding additional metadata. Need to apply some categorization, take a range of values, birthdate in ranges. Lifecycle. Right now all hand-coded. Lived through this in BI stack model - Stack of analytic databases. Things in the real-world, when exchanging VCs, the overwhelming assumption is we are exchanging VCs with the same schema and semantics. Only now am I hearing concern on how to deal with mismatching VCs.

And what if a country/jurisdiction wants a health pass that provides a pass/fail on a composite of VCs? Say, a combination of vaccination dates, whether tested recently, or have a test showing recovery from COVID-19. I could easily imagine a country using a specific formula to weigh all these factors in unique ways to decide whether you can come into the country.

This suggests an executable component that works within a wallet or even a VC container to process such a "weighted health status" algorithm provided by a Verifier to the Holder. Current discussions only consider use of a single VC/criteria in credential exchange. Most organizations developing "health passport" type applications appear to be assuming use of the VC of their own design, so there is no evaluation or semantic/structure/value mapping and translation.

Paul: fascination discussion. Have seen a couple interesting things on the data collection side. Linked data stuff, not necessarily what the VC people are using, very sophisticated what the MIT people are doing. Haven't done a layered approach - think they need that. Going from that to the rules part. If we can do a combination of some of that stuff, I think it could work. That's as technical as I go.

Neil: Do we have to buy Brent a beer?
Paul: We do, and I have to send you that stuff so you know what I'm talking about.
Tom you should have it, Neil have it, … Is private?
Brent: it's all publicly available.

Paul: plug: Inputs and Sematics WG. Semantics Domain Group Pushing layered architectures. Layer of data collection could be looking at as well. Think will need to take into semantics to understand it.
Every week on a Tuesday.
Interesting group at ToIP. Like an innovation hub. When came into the space, it was like we wheeled in a trojan horse. ToIP initially built by SSI community. Thinking about authentic data, VCs and stuff. When I came in with my data management hat, saying need a semantics group, fabulous people jumped iout, started building amazing y tealanted group of data magmtnt semantics experts. Got a place at the table. Identity folks recognizing importance of structured data.
…

Neil: plug: watch Buraks breakout video from yesterday.

Neil: Query Intent
Charles: asking about Linked Data Signatures W3C WG?
Neil: Not relevant. Input state. Consumption
John: Interesting work. Best practices encryption. Canonical rep important.
Paul: would want VC to just sign ….

Zoom Chat: Chat messages may be out of order with regards to the other typed notes.

Neil Thomson, 12:04:14 PM Machine readable data is not analytically usable without the metadata

Scott David, 12:04:57 PM Data plus meaning equals information. Is semantics co-extensive with meaning?

Neil Thomson, 12:06:21 PM
> That's the goal...
> Key question - so what metadata is required (and is missing) for data that is useful outside of the original context

Scott David, 12:08:17 PM
> Is semantic layer intended to anticipate all possible future contexts of application? If so, how is this open ended future encoded in the system?

Can the semantic layer be Bayesian, so that modifies anticipated contexts and “learns” as time goes on? Is that them semantic active inference?

Linked data concept

Neil Thomson, 12:10:24 PM Semantics is built from (most cases) several layers.

Brent Shambaugh, 12:15:56 PM
Thanks for summarizing and your work. :)
I believe NULL is a maybe functor?
CQL deals with NULLs . I will need to double check the specifics.
I'd like to participate more if that is useful. I could introduce you to Ryan.

Tom Jones, 12:43:07 PM
I have a different approach to consider

Forget the VC, the user should have their medical records on their phone when they travel anyway. Just go from that HL7 data straight to the VP.

My last meeting was too successful - I’m still trying capture all the data I got from that

Healthcare semantics.

…

Need to know someone they trust authorized a physician
Mixing two problems. Whether data on phone is appropriate. Second question is whether or no have proof presence, of you presenting it. Doesn’t need to be part of the same mechanism.
Paul: have separated those. Separated.

Need to cryptographically link back to the source data.

Tom: health data is health data, it is where it is. Huge money spent to make sure its accurate. DOn’t ned to do that.
Paul: Still need to cryptographically link to the record. To this credential. If lose that, the credential is meaningless.
Tom: I’m not putting my health in your technology.
Paul: Don’t want it, you can keep it.
Tom: Should get data from where it was generated, put in phone and take with you.
Paul?: HL7 is a standard, not *the* standard.
Tom: … Other standards. The data is that way. Where it was captured. Can do that transform. Still will be HL7, but will lose information . No chance to do transform and gain data. Always lose data. Best thing to keep source data, use transformation at end.
Paul: you think hospitals would be happy with that? Real life situation: capture data, goes in their DB, you want to get the same data on your side.
Tom: it’s regularity in force in US today. Must be able to do that.
Paul: layered architetcute. Can have hospital / gov authority to publish overlays… to translate to some sort of VC or proof.

Tom: HL7 is just a structure. It should work everywhere. Just carrying basket. Codes/fields are specific to some regions. Want to keep the data in the format it was generated in, convert it at the last moment. Transformation…
Paul?…
Tom: have to do that contemporaneously.

Paul: have health format, types don't match. Have to match types. One wants certain types of codes.

John: Conversion could go either RDF to JSON-LD.
Papers for round-tripping data.
FHIR standard is JSON. But also graph representation. Issues
Should be able to go bidirectionly RDF JSON-LD
Limited sense: subset of FHIR resources, can take from graph and put into JSON-LD rep. Haven't tried round-tripping it.
FHIR Lab(?)

Burak: Talking about semantic transformations.

John Walker, 1:14:53 PM https://github.com/fhircat/FHIRCat

Tom: … Data collection.

John: work as add-on extension. Talking about step beyond that, (transform to LD).
JSON-LD vocabularies.
Transformation to apply to LD resources.

Tom: part of idea insisteninc. You guys are going to stop after having succeeded. Then a new disease and set of codes will be created. If keep data originally in HL7 format, don't have to recreate it. Have IG do the first transform. In my view, that would be a VP rather than VC.

John: probably requires both. Technique can be generalized to any combination of FHIR resources that make sense. Focus on this use case. Nothing about this technique that is not permutable to any set of valid FHIR resources.

Tom: minor correction: we already have a clinical document for travel. Don't have a public health document. Should be talking about public health document.

John: Event on clinical side.
WHO extending IPS (intl patient summary) - WHOS VC to map/extend from IPS.

Tom: Suggesting have parallel doc for IPS which is already in it for public health. Right start. Take it and modify it. Different set of elements in each one, for privacy reasons and others.

Brent Shambaugh, 1:19:54 PM
> ShEx remind me of Dragon based on C.T. I think Josh mentioned a relation there. Henry Story is also looking at Category Theory. https://web-cats.gitlab.io/

Paul: ^ this is regarding all that categorization/linked-data stuff MIT working on.

Humanizing PoSSI- Human-Centric Structure of the Principles of SSI

Thursday 21M
Convener: Line Kofoed
Notes-taker(s): Sankarshan Mukhopadhyay

Tags for the session - technology discussed/ideas considered:

Principles of SSI
Self-sovereign identity
Governance framework
Ecosystem
Human-centric perspective

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

1. [Line] Welcome and introductions; background information around how this topic is important to discuss.
    1. Principles of SSI - https://sovrin.org/principles-of-ssi/
    2. Sovrin Foundation is working on Sovrin Utility GF and the Sovrin Ecosystem GF
    3. Work on the SEGF led to reviewing how we define an ecosystem (see slide for definition) → identity ecosystem for identity services
    4. The approach to grouping the 12 principles from a human-centric perspective is intended to enable better understanding as digital trust ecosystems grow
        1. Ecosystem of ecosystems will need a foundational set of values and principles and the PoSSI
        2. Considerations:
           The existing 12 principles are left intact and undivided as intended.
           They are all relevant, each is necessary and all should be used together.
           Grouped from a human-centric principle however the list will help understand why "identity for all" is a problem. The risk of lack of human agency (ability to act), control and protection is mitigated with adherence to self-sovereign principles for digital identity.

    e. [Sterre] It is good to have the order of the principles to help better understanding
        1. [Drummond] additional supplementary material to help laypersons understand the PoSSI better
        2. [Alex] is the original sequence/numbering sufficient and complete?
        3. [Line] the sequence might change in some instances for better coherence.
            1. [Chris] the grouping is more important for the SEGF
        4. Please join Sovrin meetings

2. Additional comments to provide context to the approach and topic - The grouping of the Principles of SSI is intended to help digital trust ecosystems adopt the entire set of principles. This approach also enables the Sovrin Foundation to be very transparent about the Principles of SSI and make it easily understood by laypersons. The principles are grouped in a manner that the logical connection between each principle is natural and well understood. The 'humanizing' aspect of this approach is to present the human/individual at the center of all technology conversations related to SSI. This is also seen in the principle of representation.

ZOOM CHAT:

21:25:26 From sankarshan to Everyone : https://docs.google.com/document/d/16RKq9hyN0zvmWEGUDSxX2Zz6OOQWyjqTUXMMlK-ZYEo/

21:34:48 From sankarshan to Everyone : https://sovrin.org/principles-of-ssi/ - Principles of SSI (PoSSI)

21:46:29 From Drummond Reed to Everyone : I definitely like this grouping of the 12 principles into these 3 categories

21:48:07 From sankarshan to Everyone : The Sovrin Ecosystem Governance Framework meets on Mondays - please see https://calendar.google.com/calendar/ical/zoom%40sovrin.org/public/basic.ics we are looking for more input, participation and feedback

21:49:45 From Sterre den Breeijen to Everyone : yes, for example transparency is important in guardianship

21:52:30 From Drummond Reed to Everyone : +1 to a paper in which each principle gets a one pager

22:06:57 From Drummond Reed to Everyone : "A Layperson's Introduction to the Principles of SSI" <== YES!

22:07:21 From Drummond Reed to Everyone : Wow, what a slide!

22:07:52 From Celia Yeung to Everyone : +1 and I'm happy to work with this group to create the one-pagers :)

22:08:22 From sankarshan to Everyone : @Drummond - the framework which has been helping in placing the bouquet of documents making up the GF

22:11:59 From Sterre den Breeijen to Everyone : Nice work done by this team! I have to drop off now. Good luck with the discussions

sovrin
identity for all

Humanizing (the Principles of) SSI

Human-centric structure of the Principles of SSI

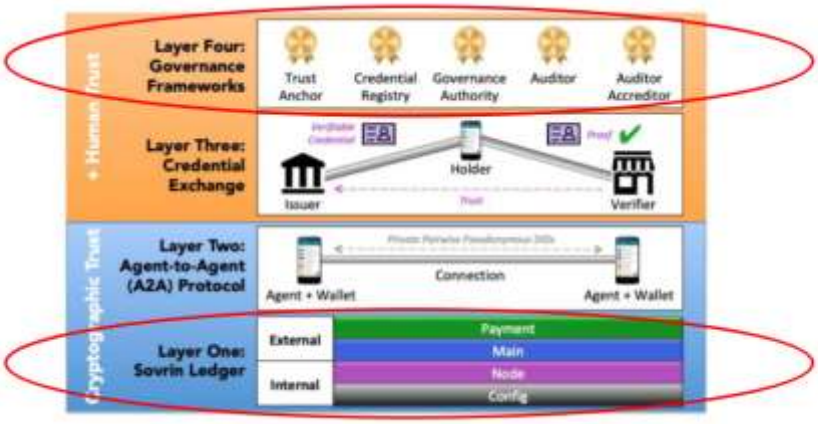
and digital trust ecosystems

IIW#32 | April 2021

SGF V3 History and Status (1 of 2)

sovrin
identity for all

- During 2020 it was determined that it was necessary to split the SGF into Utility (SUGF) and Ecosystem (SEGF) frameworks.



2

SGF V3 History and Status (2 of 2)

- **GOAL:** complete "good" v3.0 GFs (i.e. adequate for the updated division of docs)
- Prepare for development of V3.1 GFs as needed
- The SGFWG has been diligently working on the SGF V3 since Q3 2020:
  - SEGF and SUGF draft Purpose and Scope statements complete during Q3 2020
  - Global community completed the Principles of SSI completed during Q4 2020 (15 languages!)
  - SEGF and SUGF work restarted following PoSSI completion
- SUGF Primary Document is 80% complete
- SEGF Primary Document is 60% complete
  (NOTE: significant work has gone into defining and redefining "ecosystem")

SGF: Key Definitions

Ecosystem
An Ecosystem is a distributed, adaptive, open socio-technical system with properties of **self-organization**, **scalability** and **sustainability** inspired from natural ecosystems. Ecosystem models are informed by knowledge of natural ecosystems, especially for aspects related to **competition** and **collaboration** among diverse entities. (ref. Wikipedia, February 2021)

Sovrin Ecosystem
The Identity Ecosystem that supports availability of identity services for all, following the Principles of SSI. This Ecosystem adopts transparent governance and interoperability at all levels. Any other Identity Ecosystem that follows all of the Principles of SSI is considered to be an Identity Ecosystem compatible with and suitable for inclusion within the Sovrin Ecosystem.

SEGF Purpose

The direct purpose of the SEGF is to enable the global community to participate in the broadest possible digital identity ecosystem that respects the Principles of SSI, thus advancing the Sovrin Foundation's "*Identity for All*" vision.

12 Principles of SSI


1. Representation


2. Interoperability


3. Decentralization


4. Control & Agency


5. Participation


6. Equity & Inclusion


7. Usability, Accessibility & Consistency


8. Portability


9. Security


10. Verifiability & Authenticity


11. Privacy & Minimal Disclosure


12. Transparency


12 Principles of SSI
sovrin
identity for all
Agency
1. Representation
4. Control & Agency
6. Equity & Inclusion
7. Usability, Accessibility & Consistency
Control
5. Participation
3. Decentralization
2. Interoperability
8. Portability
Protection
9. Security
10. Verifiability & Authenticity
11. Privacy & Minimal Disclosure
12. Transparency


12 Principles of SSI
sovrin
identity for all
Agency
Representation
Control & Agency
Equity & Inclusion
Usability, Accessibility & Consistency
Control
Participation
Decentralization
Interoperability
Portability
Protection
Security
Verifiability & Authenticity
Privacy & Minimal Disclosure
Transparency


sovrin
Thank you!

Universal Resolver Driver Policy Discussion

Thursday 21P
Convener: Bernhard Fuchs, Markus Sabadello
Notes-taker(s): Markus Sabadello

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

Currently, instances of the Universal Resolver is hosted by DIF, IBM, and other companies. Danube Tech has been maintaining the project.

The project has some guidelines for contributing new DID method drivers:
https://github.com/decentralized-identity/universal-resolver/blob/master/docs/driver-development.md

We have some ongoing questions on policies for Universal Resolver drivers.

Proposal: We should require contact data for maintainers of drivers (could be email address or any other type of contact data).

Another challenge is that there may be multiple projects claiming the same DID method name. How to decide which DID method driver to include in the Universal Resolver?

Proposal: Driver implementers must get their DID method registered first in the W3C DID method registry, then they can contribute a Universal Resolver driver (this avoids ambiguities)

DID test suite: https://github.com/w3c/did-test-suite

DID test suite is not for runtime, but the Universal Resolver could do a few simple checks on a driver's responses. But there's also a philosophical question: Should the Universal Resolver be "allowed" to check and potentially transform driver responses, or should it just "pass through" everything that comes from a driver?

What should be the Universal Resolver policy once DID Core reaches v1.0? Remove all non-compliant drivers, or automatic translation in a transition period.

Some discussion also about the Universal Registrar, which is a similar project, but designed for DID write operations rather than DID resolve.

App Framework For Mobile Agent Dev - "No More Forking"

Thursday 22A
Convener: Horacio Nunez
Notes-taker(s): Horacio Nunez

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

This session had the objective to present a solution to the problem of forking when developing new mobile agents. With the current starting kits available in the community it is very easy to start a path where it is almost impossible to retrofit updates to the kit back into our custom agent.

The solution consists in using a framework-first approach and ensuring that custom code can reside exclusively outside of the framework, thus ensuring updates can be executed more easily.

The following link can be used as the public url for the project:
https://www.notion.so/App-Framework-for-Mobile-Agent-Development-No-more-forking-52ebe4e5635d400eb225b0ed537404d8

NHS Staff Passport - Based on Evernym Verity built by Sitekit/Condatis - A 12 month experience

Thursday 22C
Convener: Chris Eckl, CTO, Condatis; Richard Astley, Architect, Condatis
Notes-taker(s): Chris Eckl, CTO, Condatis; Richard Astley, Architect, Condatis

Tags for the session - technology discussed/ideas considered:
Staff passporting, Evernym Verity, Condatis Staff passport, Truu

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

The NHS Digital Staff Passport is a collaboration between Evernym, Truu, Condatis, and Sitekit built for the British National Health Service Digital Staff Passport system. The NHS is the largest healthcare organisation globally, and this is a substantial commercial collaboration for the healthcare service, pushing to provide a vendor-agnostic solution. This solution is currently the world's most significant ongoing deployment of Self-Sovereign Identity with 81 different agents within a trusted ecosystem.

The NHS is an incredibly complex multi-organisational system with nearly 400 organisations across the UK. Each NHS Trust is responsible for providing care for different districts across Britain. Each Trust is an independent employer for healthcare professionals, which became a challenge during the current global healthcare crisis as NHS Trusts needed to deploy staff to different locations across the country rapidly.

Part of the NHS's long-term plan is to enable staff to move from one location to another, one employer to another, even temporarily. The solution drastically reduces the time it takes to move staff records from one employer to another.

The Digital Staff Passport (DSP) is based on the foundations and concepts formulated by UK healthcare physician Manny Nijjar, the founder of Truu. Manny had done a lot of work and planning into the project over the past five years to inform the actual requirements, such as:

- Right to work checks
- Barring and disclosure checks which the home office issues
- Moving training records and certification to work with vulnerable groups
- Movement of staff credentials from one employer to another
- Licenses to practice
- Specialisations
- Bank checks
- The clinician's end-user experience.

The DSP was built as a rapid response to the global healthcare crisis and is based on the Evernym stack on Hyperledger Aries with Verity agents. We deployed one issuer and one verifier for every organisation available, run on Microsoft Azure. Each HR team gets onboarded to a directory, and we re-used Staff Identity already in place in the NHS and then issued the DSP to the moving consultants.

The DSP removes the requirement for clinicians to re-prove their credentials that have already been verified by certified trainers, medical schools, the General Medical Council (registry for all medical practitioners. Within the healthcare setting, an education piece still needs to be carried out for end users. While people understand how payment wallets work, there is still a lack of understanding of how a general identity wallet can work. Since the vaccine rollout, we enhanced the solution to include a vaccinator credential which proves a specific staff member can carry out vaccinations for patients.

Core team: Truu, Evernym, Sitekit and Condatis.

- Truu on pre-work in getting us here, collaboration set up initially for the hackathon but then chose to take this live. After the first wave in March, Truu was working on the foundations of the staff passport solution on the Evernym platform already.
- Condatis is a partner of Evernym, and we carried out several PoC's, one was also on the Microsoft SIOP stack as a method of doing this but is not the entire solution. The current live solution is built on Evernym.
- Together, all the companies aligned with the same vision to deliver on the five years of work that Truu has done.

Project key learnings:

- Truu developed a consultant-centric wallet.
- The health engagement for Sitekit.
- For Condatis, the whole concept of abstracting a staff passport to a middleware. We learned a lot about interoperability.
- Condatis proposes a handoff protocol with a standard QR code that allows the user to decide which wallet to use and issue to or present from.
- Condatis is currently developing a similar staff passport for the nuclear sector in the UK.

View Recording

For more information on the Beta Digital Staff Passport, visit https://beta.staffpassports.nhs.uk/.

Slides: Condatis IIW32 NHS Digital Staffpassport Learnings (slideshare.net)

Career Advice for New Professionals in Identity

Thursday 22D
Convener: Megan Olsen
Notes-taker(s): Charles E. Lehner

Tags for the session - technology discussed/ideas considered:

Identity, Career, Internship, Job History

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

Patrick Kenyon, 1:43:06 PM
Waiting on Megan Olsen (host) her computer is updating rn

Charles asked if okay to talk before speaker arrives.

Simon: worked with Megan Olsen for 6(?) months as intern. Do not have job offer yet. Think this is the future. Hard to get from corporations taking advantage, bring freedom back as it was back in the day.
Advise: do some research on your own, educate yourself, do development as much as you can.
Join some communities on the Internet. Be part of an open source and contribute.I will be contributing to open source Indivcio while whiling for job offer.

Simon (Slava) Nazarenko, 1:50:12 PM
please, connect if you want
https://www.linkedin.com/in/slavanaz/

Patrick Kenyon. Indicio. Mobile development layer. 2 months. Mobile development itself. Wanted to learn a bit more about identity aspect that I've been working on. To learn better.

Ian Kulp. Not currently working yet. Finished bachelor's degree same time last year. After 2 year SDE intensive. 2nd years ML. passionate about all things decentralized. See as evolution of internet. Heavily invested in cryptos pace. Mining. 24 GPU miners going. First IIW. Soaking in as much knowledge as I can. By time … graduate from this software engineering intensive. Hope to enter the workforce ideally with a company or org triny got move the decentralized revolution for

Patrick Kenyon To Everyone 1:51:27 PM Megan says she's 45/47 on her update so she should be here soon

Ian: internships at Indicio?

Simon: … Talked to me about internship. Front-end engineering. Talked via LinkedIn. He was looking for projects I was doing in React. That was sufficient.
… Information

Charles E. Lehner, 1:53:57 PM
I am an alum of hackNY fellowship, 2013.
B.Sc. Computer Science University of Rochester, Rochester, NY Class of 2015.

Megan: I work at indicio, intern, new to identity. Hoping people can come together and give tips.

?: We were thinking you would give tips.

Megan: I had some, but they were in a chat box in QigoChat, but they are not there where they were before.

What are you guys all at on your career paths? (Unformed thought)

Ian: repeated intro… Crypto mining… don't necessarily have to work for a paycheck - would like to work on technologies I am passionate about. Will be looking for work when graduate in September.

Megan: biggest advice: go in chat and ask for everyone's LinkedIn. I applied for a lot of jobs and … heard back. Got job through networking. Then got Patrick hired. I don't remember if I filled out application or not.

Charles: pasted session notes link in chat

Megan: learning different things, even though don't sound important to what you are doing, can be helpful.

Phil: looking through this advice, notes. Is any of it Identity-specific? Or just, this is our community? The rest is just IT and cybersecurity-oriented guidance?

Megan: still extremely new. Only 6 months next week. Think the advice is about the same. #1 thing to remember about identity: there is always going to be news stuff coming up that surprises you. Never would have thought of it that way because it's always been the same way for a long time.

PhilWolff: I'm a researcher for digital identity in the Internet of Things.
I've been coming to IIW for about 10(?) years. Everything Megan tells you, do that. But there is a huge leap between world of identity access management - world of well-known well-understood problems, pretty proven toolkit for managing them; and folks like at IIW trying to imagine what's the proven new stuff for 5 years down the road, start designing it now. Bleeding edge of digital identity in some respects. Other pockets of the internet where you can find where the innovators are doing stuff. Most 95% of companies in Identity trying to get some enterprise(s) properly connected, wired up. Industry, IAM. Consider as two separate fields. Identity research, science - vs. Identity Operations. Most work in Identity is Identity Operations and Business practice.

Megan: That was very nice.

Dan: I everyone on call either studying or working in a technical discipline? Or some folks … other?

Megan: I work in a technical discipline, I think i understand what that means.

Dan: Engineering, or architecture….

Megan: Yes. Do you work in technical…?

Dan: In digital product management. It can get technical, but I don't write code professionally.

I think specific to this community, it may be tactical advice, not for an immediate payoff. But being in events like this - will become very valuable, open up a lot of opportunities. How many years is hard to guess. I think we will enter a new … same way as web 2.0 era opened up a lot of business models and opportunities for folks who understood the tech well enough to capitalize and create value, think will eventually land in a similar spot in the SSI. space.

Megan: that's cool.

Ian: according to… blockchain industry to become mature by 2025. Decentralized Identifiers to become a lot more mainstream and mature in the next 3-5 years. Hopefully.

Dan: welcome, Judith. Would you mind… introducing...

Judith: Sorry for late, arrived and nothing happening, went to other cgroups and came back. Judith Fleenor, I've been around the Identity space for a long time, there has been a spinoff of a public/private sector … IESG. Familiar with ... And self-sovereign community

Jumped into this group, advice on how it was spun off as a breakout room.

Megan: no focus, just kindof spewing stuff.

Judith: where are you from?

Megan: Utah.

Judith: Currently in Utah?

Megan: yes.

Judith. My … is from Utah.
...
Working … somewhere outside of Salt Lake City.

Megan: There's basically Salt Lake City, and the place where nothing grows…

Judith: spent a lot of time in Utah. Last job was in a residential sales organization. Partner trainer: went and trained … Resided… Actually didn't sell product in Utah, because of regularity and cost of energy.
Asks about other people to intro.

Dan: either students or young professionals looking for reason about building path. Have any thoughts about career advice or specifically in identity space?

Judith: happy to say. Start of the Internet, would go to dinner parties and people would say it's never going to be anything. Lesson: if coming out of college: if you believe in something, don't listen to the other people, learn as much as you can about it. My day job at the time aas in customer relationship management software at IBM 400s(?). Had day job. But my real work and interest was in all these other things. Built a company. Then when they needed to have a website, needed to put their documents into SGML, stuff like that…. That's my history. Training: I've managed training … in organizations. How I got into Identity: … LDAP… at one of my career times of "what am i going to do now" (I get bored with things, want to find something new and cutting-edge). Identity seemed to be the right place to fit in with the whole knowledge level I had. Just started going to things. Be there, listening and learning is 90% of getting involved, especially around Identity and IIW. other 10% is contributing. Being there is one, have to …. Then find a way to contribute. Example from IESG (doesn't exist any more). Went to this thing, using my own frequent flyer miles. At that time, had to identify sector. Said UX. I'm not a user experience expert, but closest to me. Go to meeting. Chair. While people discussing, I put up flip charts... They said, "Ok, it's been decided". What? He's going to be ther chair, you're going to be the vice-chair. So I became the vice-chair of

a user group, because I was present, I showed up and help, not just stay there and listen, found what I can do with my skills to help contribute with the experience happening here. For career advice: for students, or anyone trying to change industry: to be present, listen and learned, and then contribute. Like the open source model; find a way to contribute. In Identity, even if not a technologist... I'm not a technologist, not writing code. There is equal need, or even more possibilities, taking notes, writing code, as you … learning cycle.

Dan: that perspective is itself helpful, if trying to build systems for others to make sense of. The people most expert are blind to understand. Oftentimes people who are more green may have questions that maybe the top expert would say, "Oh, is that not clear?"

As I dive into identity, the more I know, the more I know I don't know. That's true for all technologies. That's okay. But knowing to look for the things that you don't know, is needed.

Identity Ecosystem Steering Group

Obama administration. National … trusted identity cyberspace. I don't know if it even exists as a body anymore.

Charles asked Judith for clarification about IBM notes.

Patrick: I'm from Utah, Indicio, doing mobile development there.

Megan: may break? Then you can go into another weird session.
I saw in a weird session.... Cookies
Judith: It's okay to be lost. I feel like I don't understand at first. The more I listen… this piece fits with this piece, that pieces fits with that piece. May sit through whole session, don't understand anything, but then the next session, everything fits in.
Megan: I really like that they are doing secondary sessions.
Judith: Sometimes if you jump into the second session, can get confused if weren't in the first session.

Judith asks Geovane to introduce. What intrerings of this title?

Geovane Fedrecheski1: I am a PhD candidate working on IoT and security. Since last year, integrating self-sovereign identity in IoT world. Curious about what was the discussion here, in fact.

Judith: I was a late joiner, but Megan spun up the group … to get involved. Some people here have been in Identity for a while, some people new to Identity.

Thanks Megan for spinning up the session. Going to head out to another session and geek out. Bye.

Megan: I'm not sure if anyone has anything else, or if anyone wants to break.

Auto-Generating Language-Specific Wrappers for Rust Libraries

Thursday 22E
Convener: Steve McCown
Notes-taker(s): Tomislav Markovski

Tags for the session - technology discussed/ideas considered:

Rust, FFI, Code generation, language bindings, UDL

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

- Implementation of FFI that makes it easy to call Rust code
- Define API contracts using UDL
- Generates language specific code that's idiomatic to the language used
- Tutorial documentation and source code: https://github.com/sudoplatform-labs/ffi-tutorials

Slides: https://docs.google.com/presentation/d/183cn6NyrMUJLdid8-IoKmPZjVslmp4X0UvYIQvyeSBU/edit#slide=id.p1

OPN-R (Open Public Notice - Rights): Starting Notice & Control Language For People to Use Rights & Govern Identity (govinterop) with @Kantra, ToiP and W3C Data Privacy Vocabulary Using International Vocab - From ISO/IEC 29100 Legal Framework Vocabulary

Thursday 22F
Convener: Mark Lizar
Notes-taker(s): Mark Lizar

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

The language consists of

- International standard vocabulary for security and privacy frameworks provides roles and actors to govern the transfer of personal data.
- The active state notice and consent receipt - is a format for generating consent records from notice/policy - which provides people with information to use rights. .
- W3C Data Privacy Control Vocabulary and ISO/IEC 29100, Legal Framework Vocabulary

This language can be used to auto generate receipts to process rights and negotiate terms .. At Kantara we are working to use the standards to auto read the notices/polices to provide a conformance / trust assessment for people so they can see risk independently of the service provider

We discussed these projects and have some links

For more info
Goto Kantara ANCR WG
https://kantarainitiative.org/confluence/pages/viewpage.action?pageId=140804260

W3C DPV CG - https://dpvcg.github.io/dpv/

ToiP - ISWG - Notice & Consent Task force for a Privacy Controller Credential
https://wiki.trustoverip.org/pages/resumedraft.action?draftId=72226&draftShareId=8b665919-3b23-4a4d-be90-26947c7ae82c&

ToiP Privacy Risk -

Data Privacy Impact Assessments

- Breaking down -
-

Kantara - ANCR -
Showing off the work and topics

- Privacy as Expected - a gateway to online consent
- 2 Factor Consent (2FC)

https://kantarainitiative.org/confluence/collector/pages.action?key=WA&src=sidebar-pages

W3C Data Privacy Vocabulary Control
https://dpvcg.github.io/dpv/#Representative

Figuring out Verifiable Credentials Exchange - Combining Bloom, Aires Protocols, Presentation Exchange into a Unified - Killer Whale Jello Salad

Thursday 22H
Convener: Kaliya Young
Notes-taker(s): Kaliya Young

Tags for the session - technology discussed/ideas considered:

DIDComm, Verifiable Credential Exchange, Aries Protocol, Bloom Protocol, Presentation Exchange,

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

Slides to complement this document -
https://docs.google.com/presentation/d/1t4o6AXclqR7SqhGCbIJKVtYxh4fm_5mGT11MBx9K95c/edit#slide=id.p

This session was the 2nd in a series - the first one was Day 2.

“Credentials Exchange - Figuring It Out - (Jello Bowl Death Match?) [please link to these sessions in the wiki version]

The third one was in the last session.
“More Killer Whale Jello Salad...figuring out how credential exchange can harmonize. ← this one has the outcomes of the work and next steps artilcuated. [please link to these sessions in the wiki version]

State a vision or goal - dream scenario.

Presentation exchange across trust zones (relative to the VC-HTTP-API) - new way of doing it? How much influence to ma
Opportunity to make next version support - Aries Ecosystem and BBS+
Future
Vision - everyone has one way that is documented to move BBS+
Demonstrating interoperability over HTTP

Do it right - interoperability - would have vendors from Aries in there passing the tests.
Lets make interoperability set go up - make API evolve to make it work.

Orie is working on a code example here:

- https://github.com/OR13/waci-didcomm/blob/main/test.js
- Related to: https://github.com/hyperledger/aries-rfcs/blob/master/features/0510-dif-pres-exch-attach/README.md#request-presentation-attachment-format

Plz help.

Orie’s summary of where DHardman/DIDComm-community is alignment-friendly

- Transport = URI-friendly (over HTTP for now/this version of CCG-SVIP interop tests)
    - Sam C: transport over websockets as an example of how to narrow scope further to what’s easiest to align
- Envelope = didcomm [v2] compatible (JWE)
- Payload = json
- Easiest way to align interop testing FOR NOW

No Negotiation for V1

Presentation
Two message?
It is Is a two message flow if you constrain it.
(to be clear) it is not request/response - it is two message.
Reasons for complexity - get down to two if you want to start there.
Cryptography may pass - but business case won’t.

VC-HTTP-API (VHA) - has no holder interaction.
Discussion of expanding to VHA - do this instead of that (expanding)

Look at DidComm messaging

What parts of the presentation exchange can we cut.

“Presentation-Exchange has a large surface area - we should agree on the subset we want to support for AIP 2.0.”

What key parts do we need to drive attention to for a simple 2 message spec.

VP request spec - assumes JSON-LD - includes payload
Initially proposed - through over HTTP and get it done.
Do it better and have it be better.

Seen another way of doing things.

Functionally - similar to GNAP
What comes back from here is a presentation - ??

Magic - request multiple credentials at the same time - allows sending multiple at the same time.

David - asked a question about Schema URI. - pointer to a policy? What I get what I want. URI is intended to - what is the primary resource indicator - winno down the list.

Fetches policy - policy registry -

DIDComm HTTP transport
JWT
LDP

Posted in previous session, but again, here is some discussion: https://github.com/w3c-ccg/universal-wallet-interop-spec/issues/84

Do you have right format right keys.

DIDComm HTTP - what is there what do need to build.
https://identity.foundation/didcomm-messaging/spec/#https

Things i don’t see here that I expect to see.
HTTP end point - opinion of router itself.

Doesn’t look like Rest - Message oriented HTTP.
Fits in a swagger.
Messages that are getting created.
Possible open API specification 3.

DIDDoc Service end-point doesn’t have an option about scope.
Routing key seems something cut for first version - web accessible end point can get wavy without messaging key - apps on mobile devices will need it.

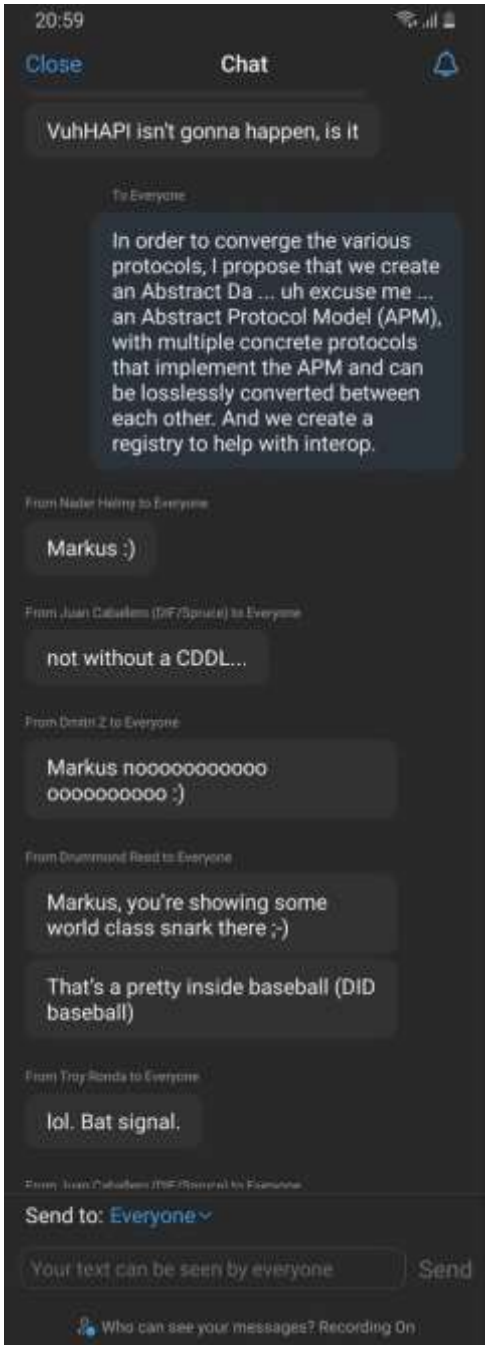
In case where mobile is wallet do I need a mediator.
Mobile agent or web wallet not have an end-point - yes need mediator.
If present to wallet that is a mobile application - mediator pass to mobile application.

Markus - structure of service end points.

Rest patterns.
Paths/routes of URL
DIDComm message type map to REST-like HTTP URL paths (e.g.for issue, present, verify, etc.)

Chat: Define automatic mapping between OpenAPI specs and DIDComm message types

Joke: Define an Abstract Protocol Model (APM):



2 ways around - place constraints on the protocol that is allowed.
Declare a new protocol?
VHA - VCI- HTTP-API

Is there a “setup phase” that we can skip?
InteropAPI
How does Bloom feel?
Cool to see it be used - excited to be a part of this effort here.

Does Authorization have anything to do with it?

What are the animals we can see from our boat deck. OpenIDConnect - and SIOP

DIDComm + Aries FRCs together + Bloom proposal

VC-HTTP-API and Aries Alignment.

Coupling certain credential formats and exchange.
Yes: We talked about DIDComm v1 only really supporting ZKP CLI
And OIDC only really support JWT

DID privacy -
One service end point +/- mediators.
If there is going to be only one? To a messaging protocol or an authorization protocol?
Answer: Let GNAP, HUBs, and Agents fight that out in their own session
Answer: Sake of narrowing things down - DIDComm (has a service endpoint definition - but could
Orie I think service endpoints are not needed

Anil Question:
What are the things that are defined and articulated in the envelope format?
Answer:

- JWE - structure inside
- Each message has a message type - attributes you can expect to look for
- Message ID
- Threading mechanism
- Timestames that can be included.
- Message - content is subject to the message type as defined.
- Payload is JSON - can be JSON-LD? - Yes JSON-LD non-conflicting.

  Request body in VHA - is just JSON but can be JSON-LD - request response format is VHA - does not assume JSON-LD.

We have put a stake in ground with JSON-LD - make sure we are not losing anything or compromising anything - we are not.

Anil Question: Hard requirement - around selective disclosure - pairing based cryptography BBS+ - does anything you are proposing prevent that - within movement between?

Answer by Orie: Issue-movement- holder whole point is to enable this - for both sides of the community - Aries - able to support both of them in both communities - and prove interoperability -
Seconding what Orie said: Intentionally defined to be agnostic - to payload - new definitions might be needed.

Anil Question: Perspective from organizational perspective - diversity of types of wallets - web based ones, agent based wallets. Does this help - providing a common pathway used by both.
Orie: this supports that vision in particular if adopted will allow interoperability testing - web wallets, backend services and native wallets (apps).

Anil Question: we know how to manage REST based APIs - if we go down this path - do we need to make this special - can the current generation of capabilities in an API gateway support something like this.
Sam: you can use an API gateway - each of the Rest calls to a different URI - know the URI to make things happen in - didcomm recipient has an encrypted - so it knows the type of message. Not make internal semantics visible - some of the features - won't work the same way.

Stephen says: - it is fully aligned with an API gateway - you can't see the inside the message. Lots of routing you can do with it - we have found in enterprise environments we are very aligned with it. Backend side of controlling is aligned.

Anil Question: How do people define API - HTTP proxy headers - also point of security enforcement. Does it take away with existing API authentication mechanisms like OAuth - mutual TLS - impact to current API security model.
Orie: - transport level security concerns and message level security concern - can still apply transport level security that you can - do now.

Adrian: Anil's last question - can we factor out by design the encryption part form the payload part - between UMA1 and UMA2 - mutual TLS connection.
Jacob: seconds. Hold message level encryption and hold line on this - big issue is key distribution. What ends up happening keys need to scale horizontally. Or you decrypt at boundary - message level format anyways.
Is there a way to separate payload contents.
Cost to have interop with message level security folks - worth hightented friction - to have common interoperability - arguing level to turn of message level encryption is arguing to not use DIDComm
Cost of processing spam - becomes and issue if we do this wrong. IT is not just Jacob seconding. Not just question about factoring it out

Cost hast be on sender.
Lots of ways to deal with it.

Anil - I sympathize with question Jacob asked and answer that Orire gave.
The flexibility of making choice should be given to enterprise - so they choose
Surviving multiple hops.

https://github.com/hyperledger/aries-rfcs/blob/master/features/0510-dif-pres-exch-attach/README.md#request-presentation-attachment-format

https://specs.bloom.co/wallet-and-credential-interactions/

Skip over bloom spec.

- RFC-454 parties present a proof
- Agnostic about actual format.

Important parts of the protocol - what format you want is in an attachment.
You can provide multiple attachments - request things in multiple formats
You have the option of responding in different formats.
Messages - that go back and forth and messages that respond with different formats.

DIDComm v2

Work Item within DIF right now - envelope format with some other opinions we may or may want. Daniel Hardman gave vision - of parts that are done - leaving behind parts not done.

- DIDCom V2 Envelops JWEs (a standard that exists)
- Aries RFCs for payloads that go in JWE envelopes.
- Send envelopes over HTTP as a starting point

Implementing Interop with Technology Across Ecosystems (did:ion, did:key, did:ethr and JWT, LD+ DIDComm v1 and Chapi)

Thursday 22K
Convener: Martin Riedel, Oliver Terbu, Rouven Heck
Notes-taker(s): Martin Riedel

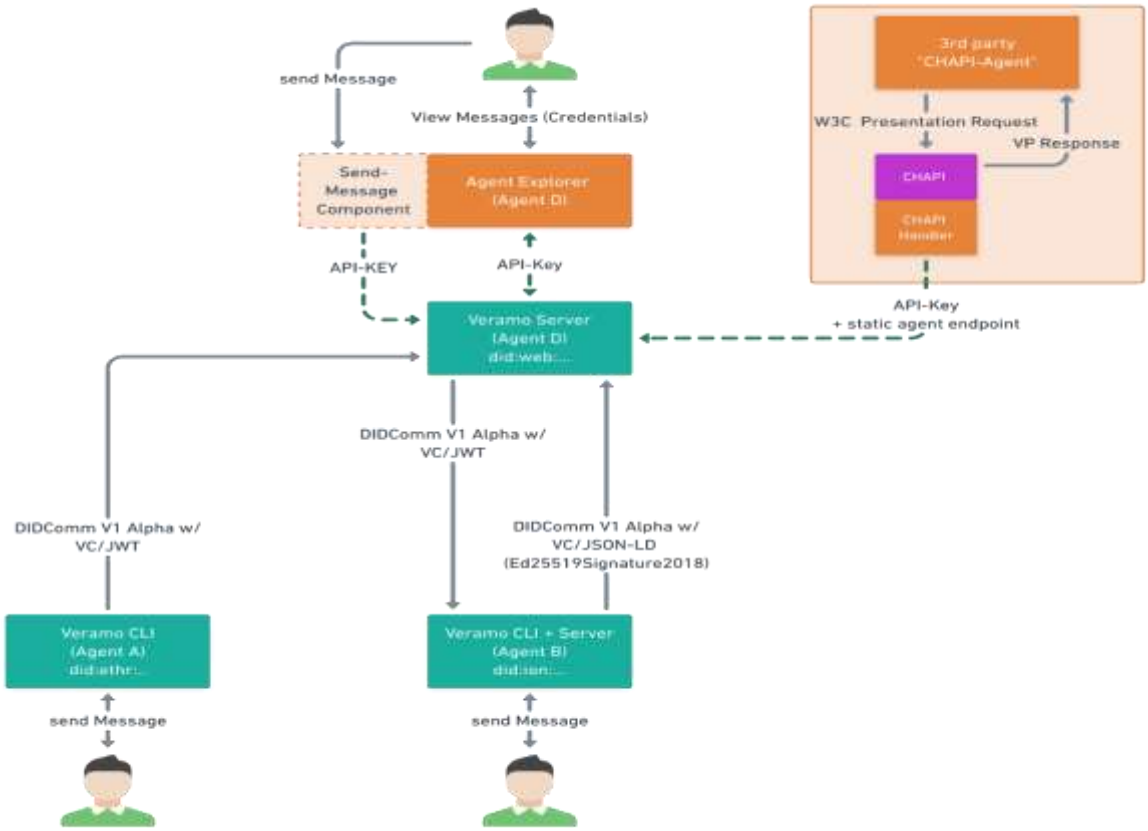
Tags for the session - technology discussed/ideas considered:

Demo, Veramo, JWT, LD Proofs, did:ethr, did:key, did:ion, CHAPI

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

In this session we demonstrated Veramo in an interoperable demo setup using different DID methods, Signature Schemes, Credential Formats and Communication Formats. We postulate that interoperable solutions would develop faster if agent implementations would support technologies and protocols that also live outside their primary development focus.

Martin presented the following demo setup.



Demo Flow Description:

- Multi-Agent Setup with Veramo (local (Agent A/B) and remote (Agent D))
- Hosted CHAPI-Verifier

1. DID Manager Presentation for DID Methods (did:ethr, did:ion, did:key), specifically to create and resolve DIDs at these methods
2. Issuing credentials via DIDComm v1 in different Proof Formats from local Agent A/B to Agent D. These are:
    1. Issuing a JWT credential from did:ethr and Secp256k1 key(s)
    2. Issuing a JWT credential from did:key and Ed25519 key
    3. Issuing a LD credential from did:ethr (Secp256k1) and EcdsaSecp256k1RecoverySignature2020
    4. Issuing a LD credential from did:ion (Secp256k1) and EcdsaSecp256k1RecoverySignature2020
    5. Issuing a LD credential from did:key (Ed25519) and Ed25519Signature2018
3. Presenting previously issued credentials from Agent K to Verifier via CHAPI

KERI Security Considerations #3 (Detailed Walkthrough of How KERI Achieves Secure Portability)

Thursday 22L
Convener: Samuel Smith
Notes-taker(s): Samuel Smith

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

The Three KERI Security Sessions at IIW32 have the same set of Slides it just takes 3 hours to get through them.

They are slides #161 through #189 of the following Document
https://github.com/SmithSamuelM/Papers/blob/master/presentations/KERI_Overview.web.pdf

Mapping FHIR JSON-LD to OCA

Thursday 22N
Convener: John Walker, Mukundan Parthasarathy, Paul Knowles
Notes-taker(s): John Walker

Tags for the session - technology discussed/ideas considered:
FHIR Mapping JSON-LD to OCA - OCA

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

Presenters: John Walker, Mukundan Parthasarathy Paul Knowles

Project Goals:

- Project began with the FHIR Focus Group at ToIP Inputs and Semantics Working Group
- OCA creation and definition began as a work effort in The Human Colossus
- Map FHIR JSON formatted resources to OCA and persist in an OCS supported repository
- Leverage existing and relevant FHIR Consent, Security,Compliance, Purpose of Use tagging
- Demonstrate the transform of the FHIR bundle and creation of the core OCA overlay artifacts

Link to Presentation: https://github.com/SemanticClarity/oca-fhir-cli/blob/master/presentations/Comprehensive%20approach%20to%20address%20post-COVID19%20scenarios.pdf

What's an Aries Interop Profile (AIP) and Status of AIP 2.0?

Thursday 23A
Convener: Stephen Curran
Notes-taker(s):

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

- Link to Presentation slides
- To get involved:
    - Aries RFCs repo
    - Aries RFC 0302-aries-interop-profile
    - AIP 2.0 PR
    - Aries WG Wiki Page
    - Hyperledger Rocketchat Channel: #aries

TMI-BFF - OAuth Token Mediating and Session Information Backend For Frontend

Thursday 23B
Convener: Vittorio Bertocci
Notes-taker(s): David Waite

Tags for the session - technology discussed/ideas considered:
OAuth, Javascript, Backend Infrastructure

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

When there is an alternative, it is more secure to keep tokens out of the browser.

Specifically talking about clients which are divided between a front end or javascript app, and backend supporting systems specifically for that/those apps

Questions on whether this would also apply equivalently to native apps, which may have different capabilities and infrastructure requirements. It likely does work, but

OAuth in the browser can be complicated and ASs don't necessarily provide sufficient security features, support web interaction

Bespoke workarounds acquiring tokens on the backend and passing to the frontend. Implementers may have security issues and not understand how to map best current practices

TMI BFF

1. Backend gets and stores tokens, javascript frontend gets a cookie
2. Request to backend for access (scopes, potentially resource)
3. Backend returns the token, requests new token with appropriate scope, etc.

Discussions on:
Prescriptive for RP/client, which is somewhat unique in terms of standards and pushing for infrastructure/security/complexity in the hands of the OP.

Does this become a best practice - starts out with a documented process

What is the scope - acquiring a token for direct API access, not necessarily prescriptive for BFF architectures which put all API interactions through BFF. (DW) raised issue that simply converting OAuth calls in a remote party to local API calls protected by a cookie disables some security protections provided by OAuth tokens (XSRF), so some sort of BFF best practices may be needed to prevent footguns.

Discussions on how prescriptive the specification should be about what to do when there are no valid tokens on the backend - e.g. provide authentica

An Identity Through Time

Thursday 23D
Convener: David Schmudde
Notes-taker(s): David Schmudde

Tags for the session - technology discussed/ideas considered:

The history of identity online. Finger, CompuServe, DNS/WWW, Facebook

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

The slides are based on this blog post: https://schmud.de/posts/2021-04-22-id-through-time.html

---

Nothing to prevent players to take advantage of SSI. They may add something small and useful aspects to the protocols.
The hope is that our stuff is super interoperable. So you can actually really leave.
Facebook is interesting because it was based on the .edu domain. Small network. Solving for the endstate that we see now is different than starting back then.
Zero-knowledge proofs and trustless networks may require high-trust environments for adoptions.
ZOOM CHAT:
1:06:29 From Cam Geer1 To Everyone : outlander!
21:06:45 From Jemima Gibbons To Everyone : David's company: https://yorba.co/
21:06:57 From Jeff O To Everyone : CServe
21:08:09 From Bruce Conrad To Everyone : And no one was worried about identity because they knew each other
21:09:31 From Marc Davis To Everyone : +1 Bruce
21:23:05 From Cam Geer1 To Everyone : wow! I filled out a few dozen of those!
21:35:33 From Neil Thomson To Everyone : The problem with privacy online is there is sufficient numbers of people who don't know or don't care or know but don't see the downside of using services that capture their PII and behavior, that those services thrive (and profit from that data), creating a significant "barrier to entry" to privacy respecting alternatives.
21:37:44 From Frederico Schardong To Everyone : +1 portability is key
21:38:12 From Frederico Schardong To Everyone : About that:
https://womeninidentity.org/2020/03/31/data-portability/
21:39:02 From zceline To Everyone : +1 @marc -- FB never set out to be an ad network...
21:40:23 From Cam Geer1 To Everyone : not at all. we need to know our history to know how to navigate through what we do next
21:41:09 From Cam Geer1 To Everyone : @marc +1 about boot strapping ZKPs in a high trust environment
21:41:31 From zceline To Everyone : +1 @cam - so important to have context. thanks @schmudde
21:44:12 From Marc Davis To Everyone : "Adoption requires (or at least greatly benefits from) high trust."
21:45:50 From Marc Davis To Everyone : So paradoxically, technologies that deal with derisking low trust interactions, may require a high trust environment in which to first gain adoption.
21:48:36 From Cam Geer1 To Everyone : that's why I see a paradox in Joe A's functional identity vs my own reflection of myself as a whole combined with my life online.
21:50:12 From Cam Geer1 To Everyone : I see myself as far more than just my function in the abstract ("In the abyss" as Hal Holbrook said in Wall Street -1986) where you see yourself staring back at you
21:51:06 From Niels van Dijk To Everyone : There is a Black Mirror episode on that...

21:52:18 From Brent Shambaugh To Everyone : ha
21:56:28 From Brent Shambaugh To Everyone : Do you want everyone to be able to correlate?
21:57:58 From Frederico Schardong To Everyone : @Cam, I agree. I see functional identity as an engineer approach to model identity so to put it into a system of some sort. The folks from the philosophy side of the force have very different views on identity (both personal identity and other forms).
21:58:04 From Cam Geer1 To Everyone : that's why this session is so critical to use schmudde's investigation as a proxy for how to think through this
21:58:19 From Marc Davis To Everyone : @Brent, no I just want that I can correlate myself for myself.
21:59:11 From Cam Geer1 To Everyone : +1 Marc
22:02:00 From Brent Zundel To Everyone : That Brent seems to have left
22:04:30 From schmudde To Everyone : d@schmud.de
22:04:38 From Cam Geer1 To Everyone : At PayPal, I got the EU payments regulator (CSSF) to talk to the GDPR regulator to see what takes precedence: The law to document the identity of a party to a transaction for antimony laundering purposes vs the GDPR right to be forgotten. AML won!
22:06:14 From Kaliya Identity Woman To Everyone : software is more like growing lettuce then making bricks
22:06:32 From Erica Connell To Everyone : identity remnants; online we live forever?
22:07:03 From zceline To Everyone : Willow Brugh and Megan Yip have done a ton of amazing work on what happens to your digital self after you die
22:07:12 From Niels van Dijk To Everyone : "Let me download the internet"
22:07:29 From Marc Davis To Everyone : Thx zceline!
22:08:01 From Erica Connell To Everyone : It brings to mind a notion of "how do we clean up after ourselves" online? Do we just *not*? Or can we "leave no trace"?
22:09:07 From Kaliya Identity Woman To Everyone : https://vimeo.com/42481807 <- my talk on digital death from privacy identity and innovation
22:09:35 From zceline To Everyone : Ooh thank @Kaliya, will add that to my collection
22:10:01 From Erica Connell To Everyone : thx, Kaliya!
22:10:20 From Cam Geer1 To Everyone : thanks! gotta run to school pick up!
22:10:41 From zceline To Everyone : great session!
22:10:58 From Erica Connell To Everyone : fantastic
22:11:01 From Marc Davis To Everyone : From Popular Mechanics 2011: https://www.popularmechanics.com/culture/web/how-to/a6527/what-happens-to-your-online-data-when-you-die/
22:11:33 From Jeff O To Everyone : https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/storage-limitation/
22:11:42 From Jeff O To Everyone : watch the cookie settings for above!

WHiSSPRr - Human Transparency Over Identity & Surveillance Risk

Thursday 23E
Convener: Sal D'Agostino
Notes-taker(s): Sal D'Agostino

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

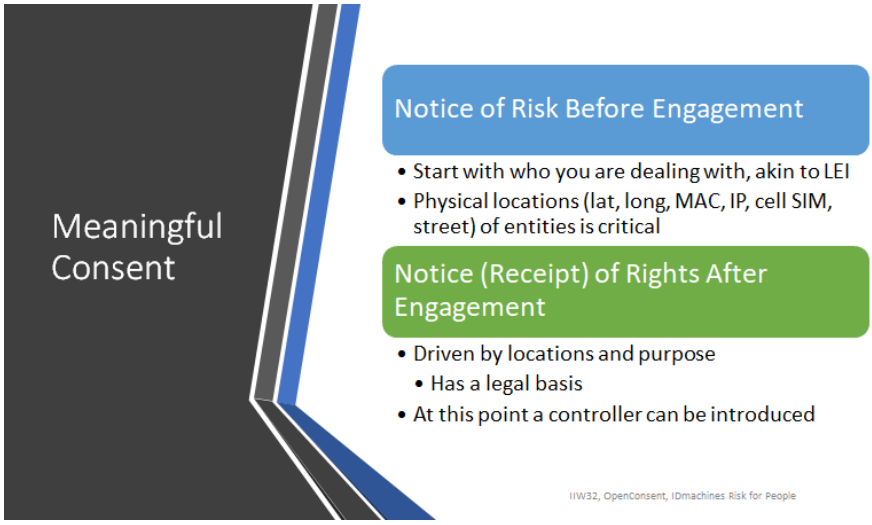
There needs to be an understanding of the different types of risk and order in which to assess them. Only then can it be made clear (to people) and be able to best manage personal (physical and digital) risk. This tends to minimize the risk profile and the operational requirements for (enables) decentralized governance, independently of any identity framework.

- White Hat
- Identity
- Surveillance
- Security
- Privacy
- Risk
- Rating

IIW32, OpenConsent, IDmachines Risk for People

- Fine grain identity management is an alpha surveillance technology
- There is an explosion of information
  - Cloud, IoT, Moore's Law (include pixels)
- The security is focused on information ***in*** the identity management system (enterprise information, including cloud).
- It is easily exploited.

IIW32, OpenConsent, IDmachines Risk for People



Good Health Pass Ecosystem Trust Architecture: DIDs and X.509 Trust Registries with Ecosystem Governance Frameworks

Thursday 23F
Convener: Drummond Reed, Darrell O-Donnell and Scott Perry
Notes-taker(s): Scott Perry

Tags for the session - technology discussed/ideas considered:

Governance, Trust Registry, Ecosystem, Transitive Trust, Architecture

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

Presentation Deck: GHP Ecosystem Trust Architecture PDF

- Proposed Trust Interoperability (Global) for the Good Health Pass (GHP) Ecosystem
- Kaliya Young & Rebecca Distler - Working Group Co-Leads
- Trust in the system - focus for today's discussion.
- Principles - https://www.goodhealthpass.org/wp-content/uploads/2021/02/Good-Health-Pass-Collaborative-Principles-Paper.pdf
- Blueprint Outline - https://www.goodhealthpass.org/wp-content/uploads/2021/03/GHPC-Interoperability-Blueprint-Outline-v2.pdf
- Global Problems inhibiting world travel. Many emerging instances of GHP related ecosystems. GHP establishing an umbrella for all GHP-compliant ecosystems.
- Relying on the ToIP Trust stack as an architectural blueprint
- Ecosystem Governance Framework is at the top of a governance and technical stack.
- Some specific Ecosystems need to accommodate x.509 certificate and VC constructs.
- ToIP Stack diagram is undergoing new changes - some new terminology being discussed at IIW.

- Governance and Trust Framework terms are being used as synonyms but we conveyed that Governance Frameworks are over arching of subject Trust Frameworks.
- GHP wll be a General Ecosystem Governance Framework. Overseeing Specific EGFs..

- It is likely to have a GHP compliance but only on the lightweight tenets of interoperability.
- We are introducing a trust registry infrastructure that works with all GHP-compliant ecosystems.
- Issuers within an ecosystem will be included in a trust registry.
- Each Ecosystem must publish its governance framework and make its trust registry available
- All issuers need to be recognized by a governance framework and included in a trust registry
- The second principle is that each specific EGF will identify its trust registry with a DID and specify its trust registry service endpoint(s) in its associated DID document
- The third principle is that each VC issued under a specific EGF will identify its issuer with either:
    - a DID
    - a URI (for X.509 certificates)
- The final principle is that each VC issued under a specific EGF will identify its type with a type URI. That field will be using common semantics.
- With this architecture, all we need is a simple trust registry protocol to answer the question:
    - Is this issuer
    - authorized to issue this VC type
    - under this specific EGF?
- GOOD - is a pass
- BETTER - may be purpose-limited (“trivial” example -

Chat Notes:

- Bart Suichies to Everyone : It's slightly different, no? It's modeling governance frameworks rather than adding hierarchy? specific EGF (typeOf) general EGF
- Darrell O'Donnell to Everyone : @Bart - correct. Not hierarchical - additive.
- Dan Bachenheimer to Everyone : I think the GHPC EGF is a template - Guidance only
- Darrell O'Donnell to Everyone : @Dan - but can a Specific EGF be a “Good Health Pass” if it violates fundamental tenets of the GHPC EGF?
- Darrell O'Donnell to Everyone : it’s inheritance
- Bart Suichies to Everyone : maybe add a little text to the lines
- Tom Jones to Everyone : Taxonomies are hierarchical - can we talk about something else?
- Jacob Dilles to Everyone : It took ICAO 10 years to get 2/3 of countries to talk to each other. Most are still not strongly verifying signatures.
- Kaliya Identity Woman to Everyone : what the hell is a “trust level”?
- Bart Suichies to Everyone : Sovereigns are funny beasts ;)
- Bart Suichies to Everyone : I think US is one of the countries still not strongly verifying?

- Dan Bachenheimer to Everyone : @Darrel - interesting question; GHPC is offering guidance (e.g., what does good look like) - I don't think there will be any certifications (e.g., pass / fail, compliant / non-compliant)
- Jacob Dilles to Everyone : @Bart (correct)
- Bart Suichies to Everyone : What would even be certified? the country implementing a hp? the provider of such a hp?
- Bart Suichies to Everyone : +1 to show what good looks like
- Bart Suichies to Everyone : I think certification would be overreach given the time and market-dynamics
- Todd Gehrke1 to Everyone : @Bart that is exactly the discussion that is being had
- Darrell O'Donnell to Everyone : @bart - 100% in the short/medium term, but may be required longer-term
- Bart Suichies to Everyone : true - but by then most governments will be locked in
- Darrell O'Donnell to Everyone : they can license the “(not so)Good Health Pass” mark then! (totally kidding)
- Bart Suichies to Everyone : We have to be honest as well - GHP is also one of more initiatives trying to do this
- Darrell O'Donnell to Everyone : agreed Bart
- Drummond Reed to Everyone : This is true - and we know that GHP needs to interop with WHO, EU Green Certificate, and VCI
- From Bart Suichies to Everyone : do verifiers need to be in a trust-registry as well?
- Darrell O'Donnell to Everyone : @Bart - depends on the governance framework - in some places I suppose so
- Bart Suichies to Everyone : @darrel - is that explicitly optional in the trust framework? I think it would be good practice to limit verification of medical data
- Bart Suichies to Everyone : countries allowing it for anyone should be the exception rather than the best practice
- Bart Suichies to Everyone : @drummond - so this would be the PKI from WHO for instance?
- Darrell O'Donnell to Everyone : @bart - agreed that health records need limits. but if you’re travelling with data-minimized pass already (i.e. no direct medical/health data beyond “ok to travel by rules 1,27, and 43”), perhaps not.
- Darrell O'Donnell to Everyone : @bart - totally - WHO SVC is one registry - and countries may continue that - or do their own thing.
- Bart Suichies to Everyone : strongly disagree on that one: what if employers start asking for it. Purpose limitation is something that needs to be promoted
- Bart Suichies to Everyone : purpose binding is something that should be in there by design
- Bart Suichies to Everyone : it's a nuance - which is why I'd be in favor of adding a trust-registry for verifiers (it could contain a GRANT ALL statement)
- Darrell O'Donnell to Everyone : privacy-centric areas (let’s use EU/Switzerland as example) may consider that forbidden. More market-driven/less-privacy (US for example) may totally allow it. The in-betweeners (Canada for example) may allow wide use in some cases, very tight in others. Nuance.
- Bart Suichies to Everyone : we're implementing it in our interoperable aries bridge, in combination with a link to eidas
- Bart Suichies to Everyone : the eidas demo is here: https://essif.adaptivespace.io/
- Darrell O'Donnell to Everyone : @Bart or @David Chadwick - YAML would be massively appreciated.
- Bart Suichies to Everyone : https://gitlab.grnet.gr/essif-lab/infrastructure/fraunhofer/deliverables not sure if this an open repo
- Bart Suichies to Everyone : https://gitlab.grnet.gr/essif-lab/infrastructure/fraunhofer/deliverables/-/blob/master/api_documentation/train-atv-1.0.0-swagger.yaml

- Darrell O'Donnell to Everyone : closed repos - I have reached out to Victor though
- Bart Suichies to Everyone : perfect! we've been thinking about doing a nice cross-border test-case with some of our Canadian friends...
- Bart Suichies to Everyone : eIDAS to PCTF
- Bart Suichies to Everyone : Observation: in GHP the aspect of human readability is quite underappreciated
- Kyle Den Hartog to Everyone : Sorry just joined, what's an EGF? Is that an electronic governance framework?
- Darrell O'Donnell to Everyone : Ecosystem Governace Framework @kyle
- Dominic Wörner to Everyone : I'm quite late to this session. A bit of a technical question How do you encode the x.509 as the issuer? Just a HTTPS website oder a URI that's pointing the x.509 in some format? Is there a link I can read up on that?
- Jacob Dilles to Everyone : @Dominic there isn't a standard way, HTTPS is one way, .well-known/jwks.json is commonly used in OAUTH/OIDC; technically there is an LDAP URI format but I haven't seen that in use
- Bart Suichies to Everyone : Isn't that what ACDC is working on?
- Bart Suichies to Everyone : @drummond - returning to my earlier question - shouldn't #1 also contain the verifier. If we're talking about a 'trust registry protocol'
- Kyle Den Hartog to Everyone : Does anyone have a link to the TRAIN work?
- Bart Suichies to Everyone : @kyle: https://gitlab.grnet.gr/essif-lab/infrastructure/fraunhofer/train_project_summary
- Todd Gehrke1 to Everyone : @Kyle the TRAIN documentation is part of the eSSIF lab project. Bart and David Chadwick are going to help us get the info.
- Drummond Reed to Everyone : I think this is critical for anti-coercion
- Drummond Reed to Everyone : See the anti-coercion section of the original ToIP RFC: https://github.com/hyperledger/aries-rfcs/blob/master/concepts/0289-toip-stack/README.md
- Dan Bachenheimer to Everyone : it sounds like we need rules to respond to a Proof Request
- Sterre den Breeijen to Everyone : https://blockchain.tno.nl/blog/verify-the-verifier-anti-coercion-by-design/ Blog on anti-coercion by my colleague Oskar van Deventer
- Dan Bachenheimer to Everyone : if the request is OK / NOK versus raw health data
- Mahesh Balan - pocketcred.com to Everyone : There is the "Terms of Use" in the VC per the data model
- Riley Hughes to Everyone : This trust registry for verifiers is already party of the Trinsic Ecosystems product we announced Monday - happy to talk more about that
- Mahesh Balan - pocketcred.com to Everyone : As well as in the Verifiable Presentation
- Drummond Reed to Everyone : This is an our opportunity for Privacy by Design at scale
- Drummond Reed to Everyone : +1 for verifiers to publish their policies. The cool thing is that we can make it MUCH simpler for them by having them join a digital trust ecosystem!
- Bart Suichies to Everyone : there needs to be more attention to HUMAN READABILITY on GHPs on all levels.. #changeMyMind
- Judith Fleenor to Everyone : What is the TRAIN project?
- Bart Suichies to Everyone : @judith: https://gitlab.grnet.gr/essif-lab/infrastructure/fraunhofer/train_project_summary
- Darrell O'Donnell to Everyone : TRAIN - https://essif-lab.eu/essif-train-by-fraunhofer-gesellschaft/
- Kyle Den Hartog to Everyone : What considerations have you put on limitations to what verifiers need to publish so that to balance their privacy with their necessity to request information?
- Drummond Reed to Everyone : Bart, I am totally on board with the human-readable element for GHP. Happy to chat more with you about that. There is a lot of focus on that in the Consistent User Experience drafting group

- Kyle Den Hartog to Everyone : Also, looking at these things I'd highly suggest looking to the VC Data model and triangle to see if you can build upon it to enable these capabilities at the machine readable layer
- Kyle Den Hartog to Everyone : I can see ways to leverage VCs that are public to enable these in an open world model
- Darrell O'Donnell to Everyone : @kyle a "you have a GHP-I-Can-Request-A-Pass credential?" process may help.
- Bart Suichies to Everyone : @drummond - make sure the consistent UX WG links towards the paperbased WG
- Kyle Den Hartog to Everyone : The two actually can play together well
- Bart Suichies to Everyone : Have to drop to watch the magic of ledger agnostic AcaPY - thx for the great discussion all!
- David Chadwick to Everyone : The policy registry publishes its requirements for VCs. It is similar to a shop putting visa and mastercard stickers on its window
- Kyle Den Hartog to Everyone : Doing a demo we've worked on for paper based credentials if anyone's interested in attending next session

Self Attested vs Chain of Custody - Assurance Levels in Data Provenance in VCs

Thursday 23G
Convener: Stew Whitman & Alka Lachhwani
Notes-taker(s): Stew Whitman

Tags for the session - technology discussed/ideas considered:

Identity Binding, Credential Binding, when they go high, we go low?

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

What levels of identity enrolment and binding of credential to identity are required for "good" SSI

Is (Using US centric NIST 800.63) IAL 1 sufficient, can self-attestation of identity and of a claim (e.g I am vaccinated) work.

There are two important factors in establishing "truth" or the trustworthiness of the information. Attributional and Reputational. You need to have both to have trust.

Digital needs higher level of attestation because it is easier to forge and easier to propagate that forgery.

If the risk level is low lower levels of reputation may be acceptable.

Definition of Trust - Sufficient information to leap into the unknown

A certificate must meet 4-criteria of definition
Who issued it/ Who was it issued to/Has it been changed / Has it been revoked
So long as these attributes are clear the verifier can interrogate and make a decision based on the Attribution and Reputation of the issuer.

Concept of what is preferred by the verifier.

For the verifier it is based on risk, it is never going to be based on perfect information.
But it is most important to make sure that you are binding the credential to the correct identity

So what is the requirement for onboarding or enrolling an identity?

In a COVID cred use case, the individual getting the test or shot is there in front of the HCP, so the identity and credential binding can happen in that moment

But the current world is imperfect, example of Express + system in Australia, basic user/pass login and a download of a PDF. This is the best case scenario.

So without a HCP to bind the identity, how do we anchor a blank identity? What about the cases of minors under guardianship, undocumented immagrants, refugees?

Birth certificate is the kernel of identity, then other evidence is mounded or compiled over a lifetime. It takes many prior proofs of identity to qualify for a driver license or a passport.

There is also the concept of differing levels of verification needs, example of the rental application between a landlord and tennant.

Initial application for property viewing can all be self attested.
Application for rental acceptance will require a information at a higher level of trust/assurance
Contract will require almost entirely attested high trust assurance.

So long as the information is recognized and encoded as self-attested it can be up to the verifier to choose.

There is also the value of Ceremony is users (holder) getting used to the concept of holding a digital credential, so if lowering the standard of assurance helps establish the market and creates a means for establish the habit or the ceremony of presenting a digital certificate, then it is good for the overall identity tech market.

NFTs are another great example of how users are now getting used to carrying permanent digital assets in a digital wallet.

Talking on Aries Bifold, Building A Community Effort Around An Open Source Mobile Wallet in React Native

Thursday 23I
Convener: James Ebert
Notes-taker(s): James Ebert

Tags for the session - technology discussed/ideas considered:

Hyperledger Aries
Aries Bifold
Aries-Framework-Javascript
React Native

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

Slides: https://docs.google.com/presentation/d/1XKrgnUUF7nZI-bOqWMKijKZHWThsIjFkVkfPIVy3gkY/edit?usp=sharing

Discussion on the following topics:

- Face recognition capabilities and discussion
- Discussion of project goals
- Brief demo of current state
- Questions on Ionic vs React Native
    - React Native is more broadly adopted
    - Need to start somewhere
- Does Aries Bifold plan to support BBS+? Yes, planning on utilizing Aries Askar and surrounding components to enable these capabilities.
- What is the MVP of Aries Bifold?
    - Connections
    - Coordinate-mediation protocol support
    - Credential Exchange
    - Revocation
- Aries Bifold interoperability
    - AIP 1.0 and AIP 2.0 support
    - Aries Agent Test Harness capabilities
- Componentization of Aries Bifold
    - Allows the inclusion of the project in existing apps.
    - Helps with separation of concerns.
    - Use of React Redux
    - Packaging and monorepos.

ZOOM CHAT:
TimoGlastra: It would be nice to eventually split into building blocks + app
doncwaugh: Have to go. Thank you for this presentation.
Karim Stekelenburg: https://github.com/microsoft/react-native-tscodegen
TimoGlastra: I was pretty amazed by that

TimoGlastra: because the app is not slow
James Ebert: Agreed
TimoGlastra: agree wit ken
Horacio Nunez2: Agreed
TimoGlastra: monorepo could work
TimoGlastra: core / data / data components / ui components
TimoGlastra: All could have subpackages
TimoGlastra: mvp = credential exchange + acapy mediator support at minimal
TimoGlastra: hopefully revocation
TimoGlastra: Then we're interoperable with the other apps
Horacio Nunez2: That's no true. We just work together
Horacio Nunez2: Nate++
TimoGlastra: I actually meant mediator coordination protocol
TimoGlastra: It's up to dotnet to support the RFCs
TimoGlastra: I'm more interested to split RN atm

Self-Sovereign E-Commerce

Thursday 23J
Convener: Doc Searls
Notes-taker(s): Doc Searls

Tags for the session - technology discussed/ideas considered:

#vrm #intentioneconomy #byway #intention #customercommons #cuco #ssi #SSEC

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

There is momentum here, and a need to start building out much of what was discussed.

Doc introduced the session with the slide deck here, wearing his hat as a founding member of Customer Commons, the .org working on the *Intention Byway* discussed at earlier IIW sessions and described in this blog, posed later.

His case is that the incumbent e-commece system hasn't progressed past its dependence on the cookie, and perhaps never will; and that there is a need to stand up an alternate model, built on asynchronous pub-sub messaging and compute nodes that run apps that don't have to come from the stores of Apple and Google.

First examples of target areas (where communities are already active) are food distribution in Michigan and real estate in Boston. Hadrian Zbarcea led the discussion of both, using slides from the deck above.

KERI Composable Event Streaming Representation

Thursday 23K
Convener: Samuel Smith
Notes-taker(s): Samuel Smith

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

The Three KERI Security Sessions presented at IIW32 have the same set of Slides, it takes 3 hours to get through them.

This session is slides #190 through #208 of the following document:
https://github.com/SmithSamuelM/Papers/blob/master/presentations/KERI_Overview.web.pdf

AMA: Sovrin + ToIP Core Purposes & Cooperation

Thursday 23M
Convener: John Jordan, Drummond Reed, Chris Raczkowski
Notes-taker(s):

Tags for the session - technology discussed/ideas considered:

Trust over IP Foundation - Sovrin Foundation - Collaboration

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

Chris Raczkowski introduced this topic with the aim of familiarizing participants with the Letter of Agreement signed between the Sovrin Foundation and the Trust over IP Foundation.

In part, this letter responds to confusion that has existed in the market over the past year in terms of the respective roles each organization plays in verifiable credentials and decentralized digital identity.

Moreover, it also establishes clear parameters by which the two organizations aim to foster collaboration between their communities and members in areas of shared interest/concern.

The Letter of Agreement puts forward three main items:

1. Mutual recognition and support for the distinct, but interrelated, mandate of each organization.
2. Commitment to name a member from each organization as a liaison to act as a point of contact and maintain lines of open communication.
3. Proactively seek opportunities to collaborate in areas of shared interest, including communications products.

This Letter of Agreement has been approved and signed by Sovrin and Trust over IP.

It will be the basis for ongoing activity that aims to build on the strengths of both communities and advance their shared interest in the emergence of secure, privacy enhancing credential and identity ecosystems.

David Luchuk, Program Manager for Trust over IP, addressed the importance of ensuring that Sovrin and Trust over IP's mutual support for one another is clearly presented to the market to the broader community represented here at IIW.

Chris Raczkowskiindicated that a joint announcement would be developed in the very near term.

BC Gov Collaboration on the Business Partner Agent, Sharing Our Roadmap (Create Creds, Issue Them, Verify Them, Hold Them, Publish Them, ZKPs, Selective Disclosure)

Thursday 24A
Convener: Matthew Hall
Notes-taker(s): same

Tags for the session - technology discussed/ideas considered:

Business partner agent, credential management, issuers, verifiers, holders, digital wallet

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

Practical session, what we are actually building today using the hyper ledger Aries tools

Some interesting points
- Viewing organizations as Issuers, Verifiers and Holders
- Talked about the complexity of defining a verifiable credential, I.e. what are you attesting to?
- Went over the need to make it easier for users to be able to create credential schemas and credential definitions without having to gain understanding about the tech.
- Question was asked about where do we start, do we have to bootstrap the first credential? And we went over being able to start with existing governance structures, and the trust that is already accepted there to issue the first credentials.
- I gave a demo of our prototype that shows three actors (Mine, Bank, Verifier) doing a credential exchange flow between them

Chat:
13:47:59 From John Phillips to Everyone : Matt made me muse..... While many us (myself included) may recognise the phenomena that our families and partners don't really understand what we do (and why we may get paid for it) - perhaps we should be more concerned/interested in finding ways to explain it in ways that they can understand since what we do is, actually, important to them as well as us.

There's also the work of GLEIF with the vLEI and the ISO standards around official and engagement roles

DEMO: https://www.youtube.com/watch?v=09-LOHPTHWs

Connect with Us: https://chat.hyperledger.org/channel/business-partner-agent

Repo: https://github.com/hyperledger-labs/business-partner-agent/projects/1

More Killer Whale Jello Salad...Figuring Out How Credential Exchange Can Harmonize.

Thursday 24B
Convener: Kaliya Young, et al
Notes-taker(s): Kaliya Young

Tags for the session - technology discussed/ideas considered:

DIDComm, Verifiable Credential Exchange, Aries Protocol, Bloom Protocol, Presentation Exchange,

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

ReCap & Summary

- Because what we need is interoperable - issuance - issue-> holder || holder -> verifier some conversation about SIOP - has not been the focus of the discussion.
- Goal to create a bridge between
    - the W3C CCG / DHS SVIP - VCI-HTTP-API (VHA) in combination with CHAPI protocol and the (VC Request) for issuing credentials.
    - Aries protocols run on top of DIDComm

- If we agree on a credential format we can exchange across those universes - JSON-LD ZKP BBS+ then we need a protocol to do it - can go between.
- Orie proposed - that we rather then extend VHA - that the we take a streamlined path with DIDComm as envelop layer - present proof - presentation exchange as a payload including the DIF work presentation, Aries and hopefully alternative to expanding VHA - for holder interactions - since it doesn't have a holder interactions leverage existing
- So can be tested with next SVIP - testing.
- Presentation Exchange and use of DIDComm and for sake of interop testing pave a narrow path - and expand in future interoperability efforts.
- Summary: DIDComm, Presentation request, presentation exchange, present proof format using JSON-LD ZKP with BBS+
- Potentially quickly spinning up a working group at DIF - Decision was to nest within the Credentials and Claims group at DIF

Agenda Creation

Things on the Path:

- Scope/Goals:
    - Specification good and complete
        -
    - BBS+ enabled attestation that transit across issuer, holder, verifier using the rails (paved path) that are envisioned here.
    - Maximal adoption as soon as possible,
    - Proceed forward in a way - that doesn't require us to abandon some aspect of what we are doing - start with simpler form to get to bigger. Path can be made wider in future.
    - System architecture diagram that articulates how it all fits together - next step.
    - Do not re-invent things that already exist.
    - Test Suite - Test conformance vs. a Specification <- end goal interoperable implementation
    - A matrix Testing N-N testing - plugfest.
        - Be nice pick fast resolving DID methods for testing
    - Implementation Guide - *maybe by: Documentation Corps in DIF*
    - Test are about SHOWING the protocols work - not that the DID resolution works

- Define the Rails:
    - Government issues the credential using software of their choice - did anchored in some did utility - citizen able to use a wallet of their choice - that they hold it in - business using a different software (and different ledger for their public did) all able to do this making their own choices. The reason they can is because of those rails - claim we can do this to a great extent - what we can not do right now across the linked-data signature Aries Ecosystem. Show how we can do what you just described across ecosystems. (Mediation is important - how do we do mediation on these rails).
    - System creating presentation is - web wallet, backend system or mobile app.
    - We need to handle working with registered web wallets - and also be able to formulate a payload for mobile (QR code) both of these paths need to be speced out to cover both communities.
    - We need as many Verifiers as possible (to devalue information on the dark web - with

- Only HTTP Transport
- Verifier - Holder - Issuer

Verifier - is a web accessible verifier.
Holder - app/mobile wallet, Browser wallet , backend service wallet (supply chain)
Issuer - is a web accessible verifier.

Things to Paint out of Interoperability Picture / Path Narrowing:

- Non-HTTP Transports (however, let's leave room for non-HTTP transports for future iterations)
- Don't do negotiation in presentation exchange
    - Request -> Presentation -> Fail -> Error
- Lots of way to specify requirements inside presentation exchange - features we decide we are not going to use.
- Credential formats will comply with the W3C VC Data Model
    - Support for VC-JWT and LD Proof with example of BBS+ (BLS12381 G2) and ES256

- No revocation (not ready enough yet) [revocation list 2020 does exist]
- Holder refresh is out of scope [there is some work going on on this]
- Issuer/verifier mobile app

Targets for path widening later

- Revocation
- Holder Refresh
- Credential Issuance

What work will go where?

- Work within DIF
    - Credentials and Claims working group (explicitly mentions something like "unifying existing formats and protocols" in its charter) <- fast time
    - Or new WG, draft charter by Balazs: https://docs.google.com/document/d/18L2-t4_2yrO_xZkwPjMCRcKIDiRGCziNs2X4k093pvo/
    - DIF - presentation exchange?

Timeline:

- When is the next Claims and Credentials Group? (who are the chairs? - Martin, Wayne, Daniel McGrogan) Bi-Weekly -
- Work Items within DIF WG can have their own dedicated Calls.
- Join DIF: https://identity.foundation/join/
- Stewardship - , Orie, Brent, Snorre, Stephen? Troy
    - DIDComm Expert - Sam, Stephen
    - Presentation Exchange Expert -

- Register for the first meeting:(26th April, Monday 1pm ET) https://forms.gle/SqkymupnYc9tDARm9

When do we want it done?

Good Health Pass has tremendous pressure!
When do we need what by?
Feedback into this group from Good Health Pass.

May 1: GHP Drafting Groups First Drafts Due -

June 1 GHP Interoperability Blueprint Recommendations Spec complete

- 30 day vision
- 90 day vision <- would be ideal to have something that can be tested against for this timeframe.
- 180 day vision

July 1 Test Complete

August 1 - 10+ Implementations / Vendors passing VP Exchange Interop Tests.

October 1 - Cross Wallet Interop Exchange Tests.

Share with DIF Interoperability Working Group

Success Criteria:

- Interop Testing Outcome
- Artifacts Produced
- Test Artifacts to TEST <- effort time and energy

Milestones:

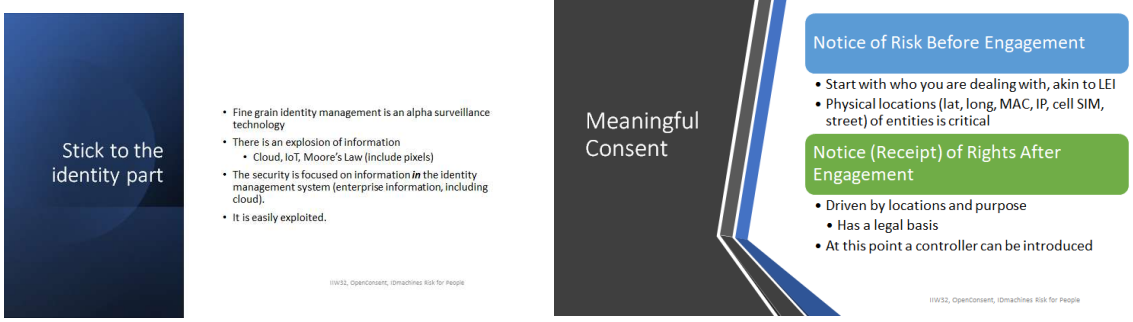
Daniel Hardman wrote this before IIW in the DIF slack and many people +1 it.
this was ideated by Daniel before the last meeting, Balazs just copied it here for safekeeping.
Daniel Hardman 18 hours ago
I see this as being a layered spec:
Layer 1 = plaintext JSON payloads, presented in sequence, with possible error conditions. Understanding the spec at this level requires nothing except knowledge of JSON and the general problem domain of VCs. No DIDComm, no HL anything, no dependencies anywhere.
Layer 2 = Security. How to wrap layer 1 such that two parties can exchange the payloads and achieve the trust they need in the process. Here, I see a forked path: use TLS (in which case security is really simple, but is transport dependent), or use DIDComm (in which case you use the JWE wrapper that DIDComm is standardizing, based on keys in a DID doc -- more complex but more flexible). The key thing about Layer 2 is that once it's stripped away (e.g., by an adapter), the payloads exchanged at layer 1 are identical and interoperable.
Layer 3: routing. This is for delivering payloads via intermediaries. It is not needed by HTTP that's direct point-to-point. If you add this layer, you introduce more DIDComm-isms but gain extra flexibility as well.
If you like this framing, then I see a spec where layer 1 is presented very quickly and easily; it should be ultra simple and easy to understand by anyone who knows JSON. No mention of any dependencies anywhere.
This would be followed by an explanation of why additional layers could be added, and then a presentation of a 2-forked road, where one is pure HTTP (TLS for security, no routing), and one is DIDComm (DID docs for security, transport-independent routing). Both use the same layer 1.
Having presented the two forks at a high level, I would then imagine a page of text describing how the HTTP fork would work (HTTP status codes, adaptation for web sockets vs. web hooks, etc).
Then I would imagine a page describing how the DIDComm fork would work -- but instead of hyperlinking to DIDComm auxiliary material, it would be a page or two of copy-pasted material that would allow DIDComm compatibility without consuming any other docs.
The upshot would be a single doc that:
A) describes a simple exchange of messages that lets credential-based proof be requested and presented
B) Structures the messages in a way that's compatible with DIDComm, without requiring anybody outside the DIDComm circle to know that.
C) Explains how the protocol could run over a web service.
D) Explains how the protocol could run over DIDComm -- but in a simplified, self-contained doc rather than with dependencies.
E) Explains the tradeoffs of the pure HTTP vs. DIDComm approaches.

WHiSSPRr Risk for People

Thursday 24C
Convener: Sal D'Agostino
Notes-taker(s): Sal D'Agostino

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

*Note – The same slides are shown below as in other WHiSSPRr



IDunion Introduction and AMA (same as on Day 2!)

Thursday 24D
Convener: Andre Kudra + available IDunion Crew: Sebastian Schmittner, Christopher Hempel
Notes-taker(s): Andre Kudra

Tags for the session - technology discussed/ideas considered:

IDunion | SSI | Identity | Consortium | Cooperative | Germany | Europe | BWMi

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

IDunion enables self-determined identities based on Self-Sovereign Identity (SSI) technologies Hyperledger Indy and Hyperledger Aries. The aim of the IDunion organisation is to create an open ecosystem for decentralised identity management, which can be used worldwide and is based on European values and regulations. IDunion is also a project co-funded by the German Federal Ministry of Economic Affairs (BMWi) as part of the Showcases Secure Digital Identities program. We gave an introduction covering

- The IDunion consortium consists of 37 partners - other major partners have already signaled interest in participating
- Our solution is enabled by the distributed ledger technology (DLT) and the concept of self-sovereign identities (SSI)
- Instead of a central authority, trust is organized via a DLT network, which works as a decentralized PKI system
- In recent months, in addition to intensive research, we have developed a DLT test network including governance structure, 35+ use cases and numerous software components for the allocation, verification and management of digital identity data developed
- In the future, the identity network will be managed by a European cooperative in which every institution in the EU can participate
- In total, we are working on 35 use cases in the areas of eGovernment, education, finance, industry/IOT, eCommerce/mobility, IAM, and eHealth
- Focus points within the project are interoperability, involvement of municipal bodies and citizens, generation of everyday relevance, cooperations
- Implementation schedule: 2021 - Incorporation European Cooperative | 2022 - Productive Network | 2023 - Building Trust

and answered questions.

LinkedIn @idunion | Twitter @IDunion_SCE | Mail contact@idunion.org

Making ACA-Py (Almost) Ledger Agnostic: DID resolution over DIDComm (instead of HTTP) to a Universal Resolver.

Thursday 24F
Convener: Victor Martinez Jurado, Markus Sabadello, Daniel Bluhm
Notes-taker(s): N/A

Tags for the session - technology discussed/ideas considered:

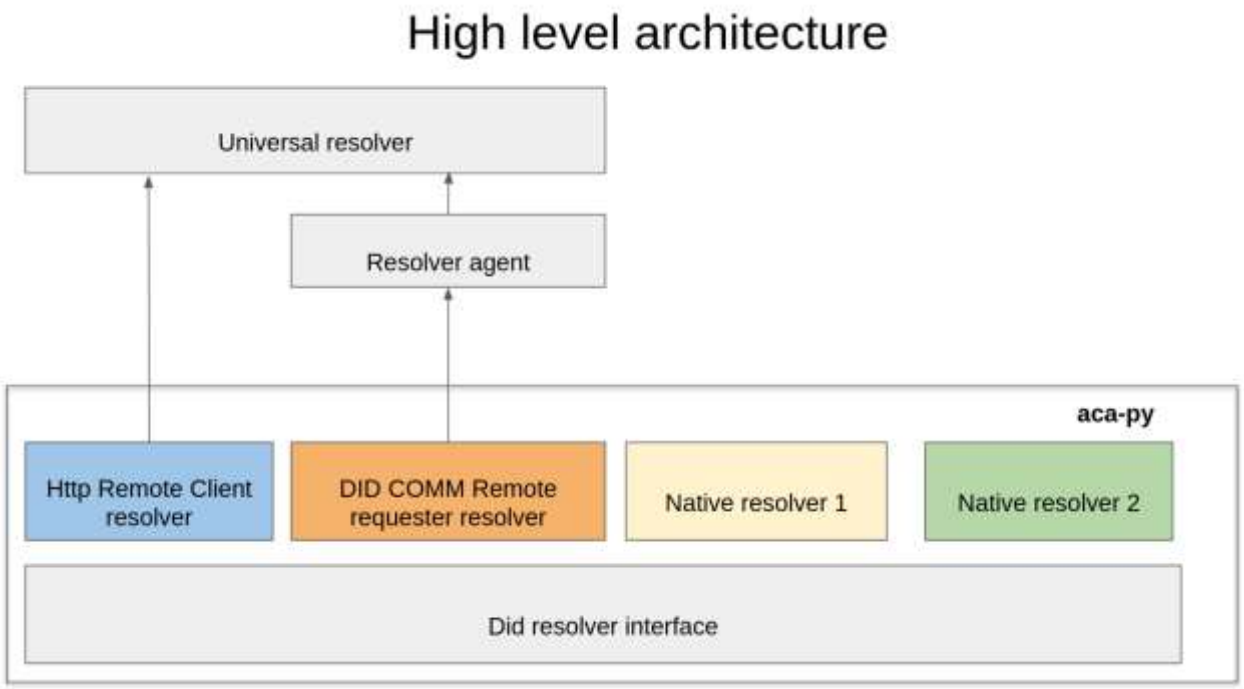
ACA-Py, Agents, DIDs, DIDComm, Universal Resolver

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

Link to slides:
https://docs.google.com/presentation/d/1oHOr5dZV5fUg3Prbx9VNDHuIM_IcDbgGablvYvTN6Ps/edit?usp=sharing

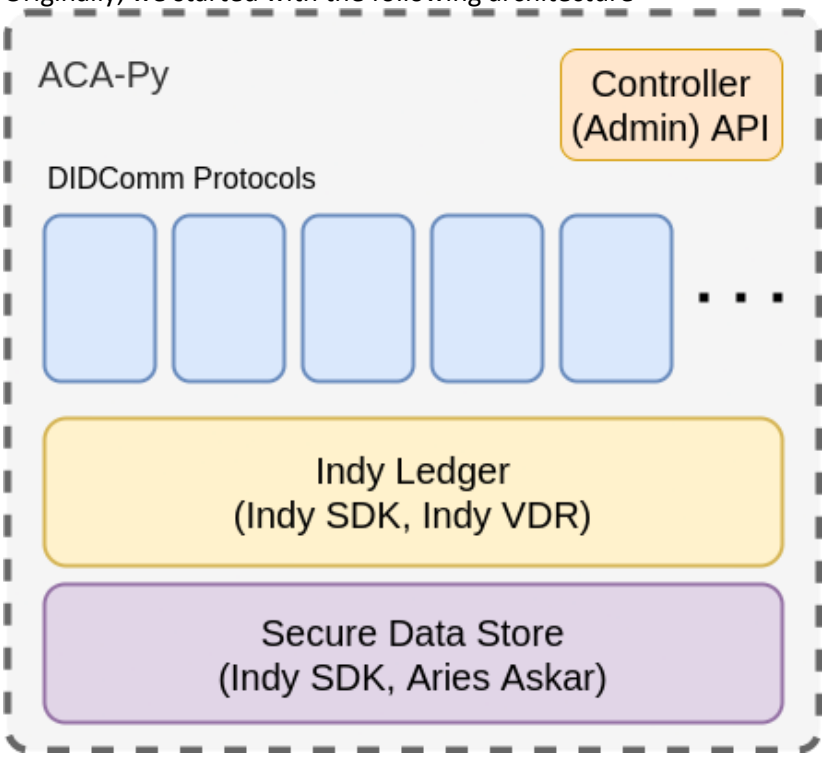
The Vision: Resolve as many did methods as possible during verification

- DIDs are everywhere: the number of DID methods is constantly growing, also we don't want be locked-in to any single DID method.
- We want to leverage in ACA-Py the addition of JSON-LD credentials (plain and BBS+)

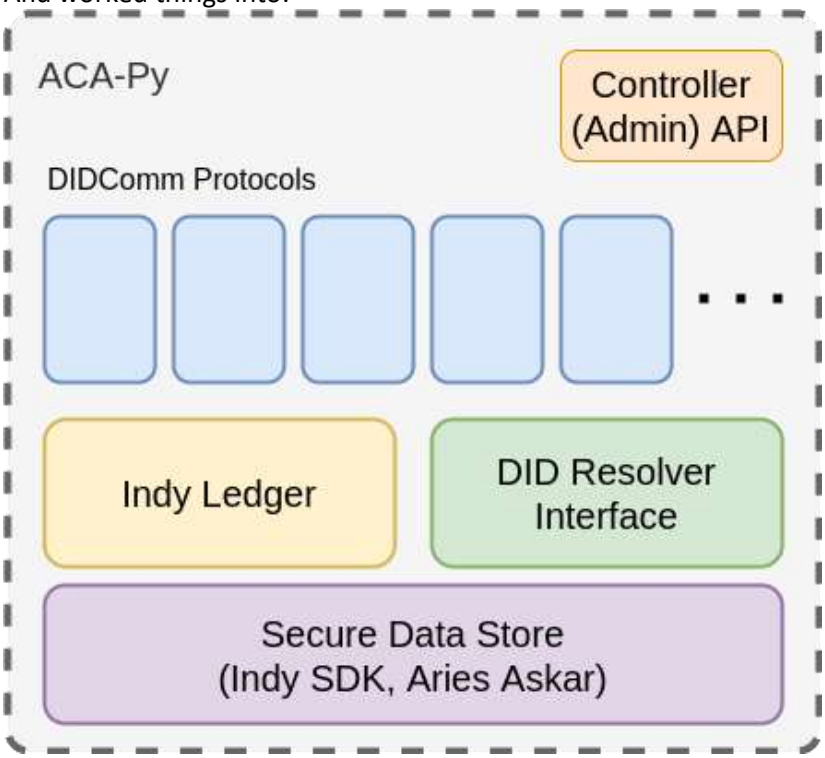


Changes made in Aries Cloud Agent - Python

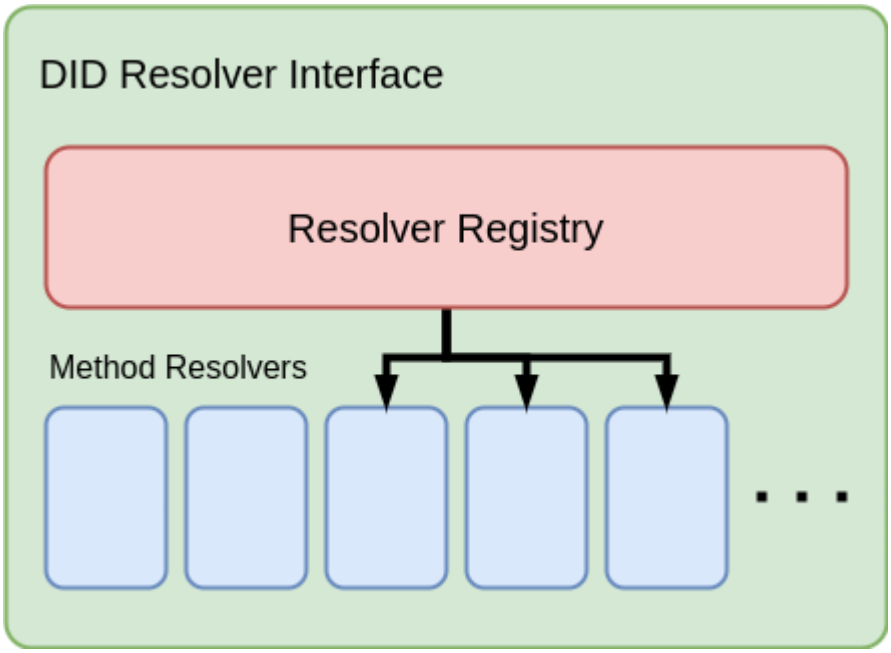
Originally, we started with the following architecture



And worked things into:



Creating an interface for pluggable DID resolvers in ACA-Py. Resolvers are matched to DIDs through use of a Resolver Registry, giving priority to natively implemented resolvers over remote resolvers.



You can run the demo yourself by following the instructions at:
https://github.com/sicpa-dlab/aries-acapy-plugin-didcomm-resolver/tree/demo/iiw/demo

Next Steps:

- Technical Items
  - Tighter integration with ACA-Py?
  - DID to Resolver matching via Regex (PR pending)
  - Resolution metadata included in result (resolved via native vs. non-native resolver, etc.)
  - Publish resolver plugins
  - DID Document parsing (PyDID)
- DID Resolution Protocol Improvements (reporting failures and errors)
- DID Registration?

Resources:

- https://hackmd.io/@dbluhm/uniresolver-acapy
- https://github.com/hyperledger/aries-rfcs/blob/master/features/0124-did-resolution-protocol/README.md
- https://github.com/sicpa-dlab/aries-acapy-plugin-didcomm-resolver

- https://github.com/sicpa-dlab/aries-acapy-plugin-http-uniresolver

KERI & ADS Key State Provenance Logs Kumbaya (KEL & ADPL)

Thursday 24H
Convener: Sam Smith & Dave Huseby
Notes-taker(s): Dave Huseby

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

This was a meeting of the minds between myself and Sam Smith and Adrian Gropper that was hugely successful. We all decided to use the term "endorser" for what we all called "registrar"/"witness"/"notary". We also realized that the KERI proposal for encoding is good enough for authentic data provenance logs and we will be using the KERI encoding. Sam has modified the spec for KERI key event logs to include scripting capabilities needed in the authentic data economy for doing things like cross-chain atomic swaps for selling non-fungible authentic data (NFADs).

The result is that there is grand convergence on the encoding and file format for key event provenance logs that will be supported by both KERI networks and the broader authentic data economy.

Dissertation Study on Adoption of SSI Digital Wallet

Thursday 24K
Convener: Kerri Lemoie
Notes-taker: Bruce Conrad

Tags for the session - technology discussed/ideas considered: #ssiadoption

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

Link to Kerri Lemoie Slide Presentation:
https://docs.google.com/presentation/d/1BxFtjqypzPfeSe5Bbatl4NAPXn3lixWfWicdMNPOqQY/edit#slide=id.gcd69ee338d_0_288

Perceived benefit + Perceived ease of use => Behavioral intention

Her hypotheses: (slide 13)

H1: Perceived usefulness will have a positive effect on behavioral intention to use a self-sovereign identity digital wallet.

H2: Perceived ease of use will have a positive effect on behavioral intention to use a self-sovereign identity digital wallet.

H3: Trustworthiness will have a positive effect on behavioral intention to use a self-sovereign identity digital wallet.

H3a: Trustworthiness will have a positive effect on perceived usefulness.

Methodology: anonymous online survey using design fiction (think “Star Trek”)
(slide 14)

Web page proclaim.io/study/ used in survey
Story told, set in the year 2031, followed by questions

Survey ran for one week.

See results (slide 15) H1+, H2-, H3+, H3a+
And slide 16.
Biggest factors leading to trustworthiness were “access” and “protect.”

Freeform comments (slide 21)
Respondents got the advantages
Lots of worry about lost/hacked phone, distrust of company, identity theft, and harmful AI

Question: were respondents knowledgeable about SSI? Were they reflecting about their presence online.
Answer: most were somewhat proficient. SSI, block chain, etc. were terms not mentioned at all. Faked SSI verified stamp/seal was there to set some expectations.

Takeaways (from slide 22):

- Usefulness & convenient
- Emphasize protection of data & access to data
- Comparison of SSI to older mental models
- Educate about SSI and why it is different

Older mental models might not transfer well.

Works now an a badging program, where holder can click on “see the data” to see what is behind the badge earned.

Limitations (slide 23)

Future work (slide 24): we need an Internet self-efficacy scale; real demos; in-person focus groups; more diverse participants

Marc: Helpful to see perceived benefits. Useability, suggest A/B testing would be better. Answer: Probably shouldn’t have tested ease of use in this study.

Riley: Maybe people perceive ease of use is less important than benefits of use.

Discussion of ways of testing useability in user experience. Low vs. high fidelity prototypes.

Perceived ease of use is part of the UTAUT framework used. The embedded webpage was presented in Qualtrics so that it looked mobile.

Leah: sample size? 382 of which 319 after data cleanup. Method partial least squares. PLS-SEM (Structural Equation Modeling (Marc put a link in chat)). Eliminated participants who didn't answer all the questions.

Phil: anything different you would have done to speed things up? Was done in about a month.

Kristina: very hard to do a study like this without an actual demo. Are the use cases presented in the study web page real? Has been working with open badges, and worked with Manu on verifiable claims. Millions have been issued, but there has been no place where they could be used. Adoption won't be increased until the systems actually exist and can be used. What would an SSI wallet allow us to do that we can't do now with other technologies. Hype and excitement vs. actual use.

Simon: Have you considered features from implemented wallets? Did a little bit of this while planning the proposal, but didn't work closely with any vendors. Limited by funding.

Marc: Would like to be better able to explain how SSI works. But how is understanding how it works more important than what can it do for me? Is how it works important for understanding the benefits? Is SSI different than other products in that way. A: It would be helpful to understand how it is different, at least at some level of detail. How it prevents hacking, etc. Q: engineers consider trustworthiness based on how.

Phil: would you be more likely to try this out if someone trusted recommended it? (doctor, insurer, government, etc.) Is there a particular anchor tenant that would be important, knowing that it is trusted by them and easier to get data from it? Bringing up "safety" is a negative that you then have to quell. A. My argument has been that having a lack of digital literacy leaves you more vulnerable. SSI is different enough that it is even more important here.

Riley: Thanks a lot. A passion area of mine over the last few years. My research gave these comments: as a founder of Trinsic, we have a bunch of data on this. Vast majority (90+%) of those 100,000+ are using a wallet that is part of a domain-specific wallet. Is having all your stuff in one place the best value proposition? The network effect. Did you touch on this in your research? The usefulness of a particular VC is a function of the number of places where I can use them. Chicken and egg problem. No question of the value of VC once it is widely available, but how do we get there? A: This didn't touch on that, being limited to intention to use, rather than actual usage. No testing of use behavior as such. For some time we won't see one wallet with everything in it, but will use what we can get.

Vittorio: Tolkein spent a lot of time to flesh out the details of his fictional work. People should care about controlling their identity and identifiers. [hopefully, Vittorio will add his insightful comment here]. What is the task that people cannot do today, but will be able to do with SSI. How do we interest the issuers of VC so that they will give them away? What is it that interests the verifiers to do the work on their side (presumably for free)? Where are the financial incentives? A. in education we issue lots of credentials but no one is using them.

Leah: Why are people not using the educational claims? A: business model disruption. E.x. registrars charge for transcripts. Or maybe they weren't verificable enough; but no. Probably a lack of understanding and revenue model. In education, entrenchment of how things are done.

Link to Session Zoom Chat Provided by Kerri Lemoie:
https://drive.google.com/file/d/1akxpWkRO7637bRP1W7iDeNKHtHamrr1_/view?usp=sharing

Decentralized Publication, Micro-Publication & Moderation - What The Real Pitfalls Would Be

Thursday 24L
Convener: Juan Caballero and Kim Duffy
Notes-taker(s):

Tags for the session - technology discussed/ideas considered:

Decentralization, social

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

Link to Session Slides:
https://docs.google.com/presentation/d/1RMozl86wihBw8_rJvC97tUUjYVpTHk6aF8QOs_ng6l0/edit?usp=sharing

Set-up Presentation:

- Silos and echo chambers?
    - Countermeasures?
- Pink Checkmark system? Verify all accounts or continue 2-class system
- Can we still make money?
- Moderation
- Clients and API openness - on what axes will they compete? Can they compete on algos? Community curation?
- How important is authenticity? Each tweet signed?
    - Editable cheeps?
    - Delete cheeps?

- Mike Jones: Listening to Daniel's ION presentation, I asked from the POV of a naïve person, what are these ION DIDs good for in the first place; his answer was
    - Daniel wants identities that Twitter can't take away from Donald Trump
    - Child pornographers would also then be sovereign over their identifiers
    - Kim: People select their own echo chambers
- Juan: Echo chamber / child porn dynamics have a lot in common (HBO Documentary "into the storm")
- Erica: Social media as a way to advertise, finding markets. Want to market to people who are interested
    - Small business, organic marketing, micro-commerce
    - Bullying, social problems, child protection
- In chat: distinguishing identifier control/sovereignty from data flows and recommendation
    - Silencing the horrible
- Mike: Govts and major players/communities have their own prerogatives and priorities
    - Rebecca McKinnon (former Chief CNN correspondent in China) - "If we want to know that a conversation is actually private, we're going to have to do it the old fashioned way and meet in the middle of a rice field in our skivvies."

- Brent: Algorithmic tyranny -
- Erica: What communities and platforms you opt in to/out of IRL
    - Contextual expectations and social contracts
- Juan: basic expectations that we've tasked centralized platforms with; how will this adapt in world where shutting down accounts isn't primary recourse
- Brent: AI approaches, will it get good enough?
- Juan: can never count on that
- Dan Robertson: layers on top of base protocols so I'm not flooded; it's been filtered by party/parties I trust (spam detection library, child protection, etc)
    - Email spam filtering; child protection in search results
    - Where is the line between safety filtering and filter bubbling/echo chambering
- Juan: e.g. certificate transparency and allow lists and role
- Kim: Seeing this as a data problem: streams and filters/policies
- Dan R: Getting out of "winner take all" paradigm: competing on feature
    - Hotmail never went away because of interop

Secure Scuttlebutt Outro

Thursday 24P
Convener: Charles E. Lehner
Notes-taker(s): Charles E. Lehner

Tags for the session - technology discussed/ideas considered:

Secure Scuttlebutt, Decentralized Identifiers, Key Management

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

Dmitri expressed interest in SSB and reported using but then having lost their key (when switching/resetting devices?). Expressed Frustration (with the key recovery process). Have question, how could SSB use DIDs?

Charles responded that there is a draft PR on DID Spec Registries adding a SSB DID method a few days ago.
https://github.com/w3c/did-spec-registries/pull/291

Dmitri Z. asked about other ways other than as a DID method.

Charles said SSB could be extended to support DIDs, but this would be a breaking change, which the community doesn't seem to want, considering SSB's message signing format as "set in stone".
There could be other ways, such as making a new system that uses DIDs but inherits some of SSB's design.

Notes in this book can also be found online at
https://iiw.idcommons.net/IIW_32_Session_Notes

Demo Hour / Day 1 & Day 2

Thanks to our Demo Hour Sponsors!

DANUBE TECH GMBH

coinbase

Demo Hour Day 1: Tuesday April 20, 2:30 - 4:30
Demo Hour Day 2: Wednesday April 21, 1:30 - 2:30

DEMO Table/SPACE #

1. **Blockster Labs: National id as a VC and verify with IoT:** Ravikant Agrawal, Kalyan Kulkarni, Amit Padmani
   URL: http://blockster.global/
   An innovative interim solution to convert existing credentials like national id (taking Aadhaar example), COVID vaccination into a VC, and granting touch-less access using an IoT device post verifying access credentials like employment id card, boarding pass, etc

2. **UBOSbox:** Johannes Ernst, Indie Computing Corp
   URL: https://indiecomputing.com/products/
   UBOSbox is a pre-configured server appliance that enables consumers and small businesses to take their data home from internet platforms such as Google Docs or Dropbox onto a server they control. No spying or tracking by third parties; no lock-in and no subscription fees. Now ships with Nextcloud Hub, the leading open-source document collaboration solution that includes Google-Docs-style collaborative editing in the browser, calendaring, chat and much more.

3. **Coinbase: Mike Lodder**
   URL: http://coinbase.com/
   As Coinbase becomes more involved with decentralized finance and exchange, the need for facilitating decentralized identity has recently come more into focus. Come learn how Coinbase plans to adopt decentralized identity and how we can work together.

4. **SeLF & esatus Wallet by esatus AG:** André Kudra, Christopher Hempel & Jonas Schneider
   URL: https://self-ssi.com/en/
   Latest updates on esatus SeLF and wallet app! Fully leveraging Hyperledger Indy and Hyperledger Aries technologies, all employed in Sovrin and IDunion. Integrates SSI into existing IT-infrastructures. Credential-based access rules transform SSI to classic authentication and authorization. Bridges SSI to conventional technologies like SAML, OIDC, SCIM, JDBC, LDAP.

5. **Pravici PocketCred:** Mahesh Balan
   URL:www.pocketcred.com
   Product allows for issuance and verification of VC's. We will demo how our product can be integrated into any EHR, with examples of integration with Salesforce Vaccine Cloud as well as Epic to demonstrate how it can be used to issue and verify vaccine or test credentials.

6. **Center Identity - Location-based private key recovery method:** Matthew Vogel
   URL: https://centeridentity.com
   This presentation will demonstrate using either a Center Identity device or a web browser to securely recover a private key, register, and/or sign-in to a service/web site using our patent pending location-based recovery method.

7. **IOP Global - The IOP Console's SSI-flow:** David De Troch
   URL: https://iop.global/
   Steve wants to open a bank account without showing his ID Card. He won't reveal more than the required personal information. We will cover the flow and the W3C-compliant entities involved in this process. Our tools are built on production-ready open-source technology.

8. **IDENTOS: An Ontario trusted account, a digital identity service for putting patients at the center of care:** Alec Laws
   URL: myTrustedAccount.ca.
   The new digital identity service available for use in four hospitals provides patients with a convenient, repeatable, and secure method to control access to health services and information. Learn more in this press release.

9. **Trinsic - Next-gen SSI Platform Launch Applications:** Riley Hughes
   URL:https://trinsic.id
   Decentralized identity and SSI adoption has been slow-going because the software only solved half the problem. Trinsic's v2 platform provides a complete solution for scalable technology, ecosystem governance, and adoption tools. Come see what the future of decentralized identity looks like.

10. **RANDA Solutions/The Lifelong Learner Project:** Kimberly Linson
    URL: www.lifelonglearnerproject.org
    The Lifelong Learner Project envisions a world of data agency for professional educators. By breaking apart the teacher license into individual credentials the teacher workforce has both portability and mobility beyond the four walls of the classroom.

11. **Pico Labs - Manifold -- Manage All Your Things:** Bruce Conrad
    URL: manifold.picolabs.io
    A demo of the "Safe and Mine" application in Manifold to help when you lose one of your things. How to create tags that you can physically attach to your things.

12. **Universal DID Operations:** Markus Sabadello - Danube Tech
    URLs: https://uniresolver.io/, https://uniregistrar.io/
    Demonstration of DID operations such as resolving, creating, updating, deactivating, and more, in a DID-method independent way.

13. **The Intention Byway :** Hadrian Zbarcea
    URL: https://customercommons.org
    We all read Doc's book The Intention Economy (http://j.mp/ntnecn). The CustomerCommons foundation is implementing the infrastructure to support the intention economy. The two major components are the Intentron, a compute node that gives the customer agency, and the Byway, a federated messaging service, that supports Intentcasting. This session will demystify how the byway and addressing on the byway works.

14. **HearRo Identity Based Communication (IDC):** Vic Cooper - CEO HearRo, Inc.
    URL: www.hearro.com
    The need for organizations to easily connect with their customers/citizens in highly personalized yet secure and efficient ways has never been greater or more urgent. See how HearRo uses SSI and DID Comm to enable secure "1-click" communications between People, Organizations and Things.

15. **Unum ID**: Liam McCarty
    URL: www.unum.id
    Unum ID is backed by Draper and Samsung, building the world's first Sharified -- shared, verified -- identity network. See how they're leveraging DIDs and VCs to create seamless and secure user experiences alongside Fortune 500 companies like Franklin Templeton and RBC.

16. **Credential Master:** Alan Davies & Timothy Ruff
    URL: https://CredentialMaster.com
    Credential Master turns the world's largest CRM (Salesforce) into its first dedicated VCM (Verifiable Credentials Manager). Credential Master enables VC Issuers and Verifiers to manage up to millions of VCs with enterprise-class features, flexibility, and performance.

17. **Spruce Systems, Inc. - DIDKit:** Wayne Chang, Charles Lehner
    URL: https://github.com/spruceid/didkit
    DIDKit is a cross-platform toolkit for building decentralized identity applications, written in Rust at the core. It's open source, built for enterprises, and easy to get started within 10 minutes. DIDKit already works with Java, Python, Node.js, WASM, Android/iOS, and more!

18. **IDRamp Next Generation Utilities -** Mike Vesey, IdRamp CEO - Karl Kneis, IdRamp COO
    URL: https://www.youtube.com/watch?v=eKcpDzXA5uk
    See how American Electric Power (AEP) adapts verifiable credentials to address strategic business challengesWill demonstrate how AEP envision the use of verifiable credentials to reduce third party fraud, increase privacy preservation, and optimize customer satisfaction. The session will cover integration with legacy systems, private ID network interoperability. and auditability with big tech blockchain services.

19. **Affinidi Unifier:** Stepan Gershuni
    URL: https://safetravel.affinidi.com/
    Unifier enables airlines and immigration authorities to verify digital medical credentials. Unlike some of the end-to-end solutions, it solves interoperability of multiple standards (13 so far) and issuers / issuer registries (28+).

20. **Northern Block -NB Orbit SSI Platform with Mobile Wallet and Enterprise Web App.**
    Subhasis Ojha, Head of Delivery at Northern Block
    URL: https://northernblock.io/products/ssi-digital-wallet/, https://northernblock.io/products/ssi-enterprise-cloud/
    We will be demoing our NB Orbit SSI Platform, which consists of a Mobile Wallet and Enterprise Web App. We will look at how NB Orbit can be used by relying parties with compliance needs, and then how NB Orbit can help these relying parties add additional value through verifiable credentials

21. **Bloom - WACI Demo:** Jace Hensley
    URL: https://specs.bloom.co/wallet-and-credential-interactions/
    I'm going to be demoing our proposed WACI spec to show how you can use a VC for passwordless authentication

22. **The Blinky Project (I.o.T) Update :** Brent Shambaugh
    URL: https://theholo.space/
    "Explorations with LoRa wireless modulation technology, cryptographic coprocessors, and the Ceramic Protocol"

23. **MATTR - Demonstrating multi-vendor interoperability via web infrastructure (DHS SVIP):**
    Nader Helmy, Preet Patel
    URL: https://mattr.global/
    In March 2021, MATTR participated in the DHS SVIP Interop Plugfest -- a showcase of cross-vendor interoperability. We built a number of capabilities for our live demo including a web wallet that's compatible with web issuance & verification infrastructure built by other vendors.

24. **Condatus SSI-OIDC Bridge:** Chris Eckl and Richard Astley
    URL:
    Offering a simple out of the box SSI extension to existing federated systems. Can make an enterprise SSI agent available for any digital service that already used federated identity. Allows abstraction to one SSI technology stack and will offer interop between SIOP and Hyperledger Aries.

25. **Domi Labs - "Credentialising electronic contracts":** Pavel Metelitsyn, CTO Domi Labs
    URL: www.domilabs.io
    SCEP is a component that enables two or more Self Sovereign Identities to draft and execute an electronic contract and build contractual records. It represents an executed contract as a verifiable credential that contains the contract's terms and the verifiable data of the signatories. Therefore we extend the trust chain beyond the simple credential exchange to also build verifiable records of contractual transactions.

Closing Circle Group Shot - Hollywood Squares Version

Photograph by David Huseby / Closing Circle Group Shot!

Closing Circle - As a result of attending IIWXXXII

***** Please complete the sentence: As a result of attending IIWXXXI …. *******

… I have hope for converging credential protocol standards.

… I missed an hour of sleep each day. :)

… I have accelerated my understanding by 12 months

….I realized standards are less important than working interoperability with friends

… I have a new family

… my eyes are burning, my head hurts and i'm bleeding from my ears. A good three days.

...I know I'm a part of a great team, doing the right thing, for the right reason... with lots to do!

.. satisfied a recent "To Do" of learning up on Cryptographic Accumulators!

…I may have to change my first name (also learn more about KERI)

… I'm an entrepreneur!

… I made a lot of new friends

… I have became a permanent addict for IIW

… I am interested in learning a ton and figuring out how to stay involved until IIW33.

… I learned a lot more than I could have done myself in a long time

… I'm feeling hopeful about the identity space and the progress that is being made.

… I got help with my project, learned more things that were helpful, and .... was really surprised by the outcome...lots of things I didn't expect. Cheeper Creepers.

… I see that the non-SSI attendees have faded out.

… I have a better understanding of the current state of SSI technology, and thankfully, many new questions.

… I believe we need to find even MORE ways of collaborating effectively to produce real, effective interoperability

… I ❤ IIW

… I remembered how smart and good-willed this community is!

… I made friends, learned new things, am looking forward to future events and participating in new/different ways and raise my glass to the Snarkies!

… I miss surfing the tables in the center of the room talking to people in person

… I had a taste of really good Killer Whale Jello Salad.

... I am more and more convinced that collaboration is the way to go

…I have become a permanent addict for IIW" being a First Timer " !!

… I was able to reconnect, and I invited a 1st timer ❤

… As a result of attending IIW XXXII in Hawaii, I want to come back to both.

… As a first timer here, the ending of this event creates a void. It's an amazing event! I'm think I'm speaking for all of my colleagues when I say we've found our tribe :)

… I'll report out next IIW about my kids' experience with (their) DIDs. They'll be about it by then

…I got so many pointers to be followed as a first timer through these great three days (three midnights for me). thanks

… there needs to be more discussion on the opportunity and economics in the IIW community

… I've never seen a conference where people gift each other with compliments. Very nice!

… Chop Wood. Carry Water. That's IIW!

17:38:27 From windley to Everyone:
That's a wrap. Thanks VERY much for coming and participating everyone!

Stay Connected with the Community Over Time – Blog Posts from Community Members

New Community Resource
Each week Kaliya, Identity Woman and Informiner publish a round of the week's news from the industry. It is called **Identosphere - Sovereign Identity Updates (weekly newsletter)**
You can find it here: https://newsletter.identosphere.net/

As a follow up to the session 'Let's Bring Blogging Back' an IIW Blog aggregator has been created here: https://identosphere.net
If you want your blog to be included please email Kaliya: kaliya@identitywoman.net

A BlogPod was created at IIW - Link to IIW Slack –
https://iiw.slack.com/archives/C013KKU7ZA4
If you have trouble getting in, email Kaliya@identitywoman.net with BlogPod in the Subject.

Planet Identity Revived ~ @identitywoman & @#InfoMiner cleared out & updated Planet Identity (see links below) you can support the work here:
https://www.patreon.com/user?u=35769676

IIW Community Personal Blog's shared via: https://identosphere.net/blogcatcher/
IIW Community dot.org's in the IIW Space: https://identosphere.net/blogcatcher/orgsfeed/

See you October 12, 13 and 14, 2021

for

IIWXXXIII

The 33nd Internet Identity Workshop

REGISTRATION OPEN in Late JUNE

www.InternetIdentityWorkshop.com