IIWXXVIII

INTERNET IDENTITY WORKSHOP 28

Book of Proceedings

www.internetidentityworkshop.com

Collected & Compiled by
LISA HORWITCH, HEIDI N SAUL AND JACOB WINDLEY

April 30, May 1 & 2, 2019
Computer History Museum ~ Mountain View, CA

Photo credit Lisa H

Notes in this book can also be found online at
https://iiw.idcommons.net/IIW_28_Session_Notes

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 Horwitch

REGISTER FOR IIWXXIX
October 1 - 3, 2019
HERE: https://iiw28.eventbrite.com


Contents

Photo Credit: @windley These are all the session cards for all the sessions held at #iiw over the last three days. 129 overall.

About IIW

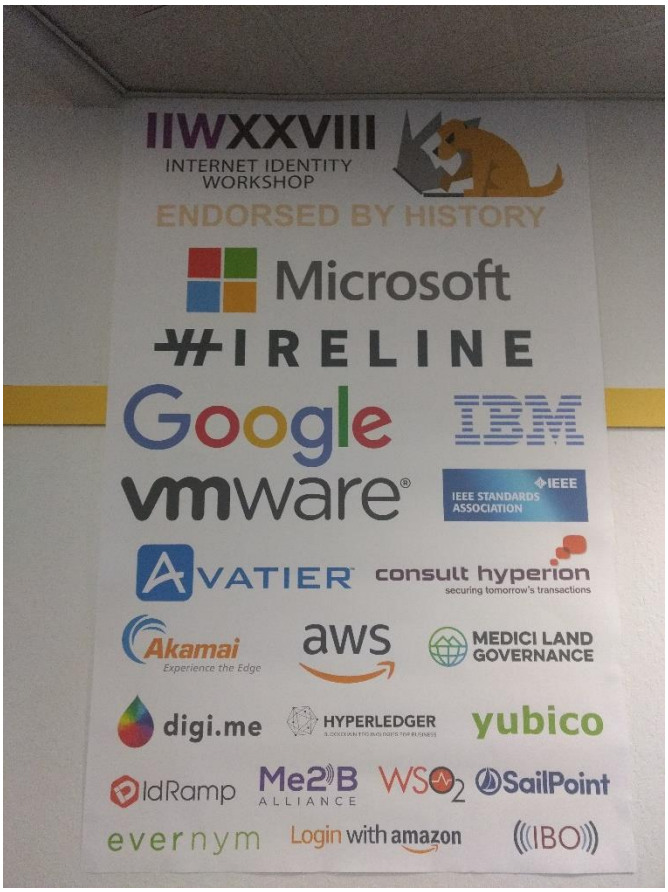
The Internet Identity Workshop (IIW) was founded in the fall of 2005 by Phil Windley, Doc Searls and Kaliya Young. It has been a leading space of innovation and collaboration amongst the diverse community working on user-centric identity.

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 14th year and is Co-produced by Phil Windley, Heidi Nobantu Saul and Kaliya Young. IIWXXIX (#29) will be October 1 – 3, 2019 in Mountain View, California at the Computer History Museum.



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 and Sponsorship information.

Upcoming IIW Events in Mountain View California

IIWXXIX #29
October 1 - 3, 2019
REGISTER HERE

IIWXXVII #30
April 28 - 30, 2020

Thank You! Documentation Center/Book of Proceedings Sponsors – IdRamp ~ Me2B ~ Google

IdRamp

Me2B

Google

IIW 28 Opening Exercise at Tables

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 28 the prompt questions were focused on what has happened or been accomplished over the years that has impacted identity from each persons experience.

Community Created Identity Timeline

Timeline events gathered at IIW #28 in 2019 incorporated with the one created in 2011
https://identitywoman.github.io/identity-commons/ID-History

People can edit/add to it on GitHub if they want here:
https://github.com/Identitywoman/identity-commons/blob/master/ID-History.md

IIW 28 Session Topics / Agenda Creation

PHOTO CREDIT **@MattrGlobal**
Day 1 and we're excited to be at @idworkshop #IIW

129 distinct sessions were called and held over 3 Days.

We received notes, slide decks and/or white board shots for 120 of these sessions.

Tuesday April 30, 2019

Session 1
1A/DID Communication Callbacks, Hubs, and Agents
1B/OAuth 2 An Introduction – 101 Session
1C/WebAuthn (101) An Introduction to the Specification
1F/Your Data Your Currency You Terms & What Do People Need to No Longer Need Facebook?
1M/Decentralized DID's

Session 2
2A/IIW Book! Come get a REAL IIW attendance verification credential and prove it to your IIW friends using your phone!
2B/Introduction to Open ID Connect – 101 Session
2C/Blockchain Social Media & Relationship Sharing
2D/Identity Management in Physical Security World
2F/Sidetree protocol – Massivly Scalable Decentralized Identifiers – DEEP DIVE
2G/A Standardized Information Governance Label for apps and services
2L/Tokenization with DID's?
2M/SSI Startups – Partnerships, Investments, Recruiting/Jobs, Ideas

Lunch Session
(Where R the) KARMIC Identity Endpoints?

Session 3
3A/What Does a Layered Identity Model Look Like? (Like OSI 7-Layer Model for Networking)
3B/Use – Managed Access (UMA) – 101 Session
3C/Relationship Lens
3F/JWT Profile for Access Tokens
3G/Universal Resolver for DID's – What it is and Why it matters
3H/Open Banking – Variable Scopes – Multi-Scope Tokens
3I/Key Management/Usability for Lay People
3J/Personal Information Value Equation
3M/Rubrics for Decentralized Identifiers

Session 4
4A/Git + DID (and fully anonymous open source Projects) –
4B/FIDO – 101 Session
4C/Gov't IS the solution to ID – Change my mind
4D/How can trusted identities be accepted by governments and industries?
4F/Self-Issued OpenID Connect (SIOP) DID Auth Flavor
4H/Identity @ Hyperledger *Indy *Ursa *Aries *Idemix & FabrCA
4I/What is the Problem? – Customer discovery lessons and techniques for building identity products for business
4J/There Is No Scope – Doing Scope, Cliams the OIDC Way – IRL
4L/Is IAL Enough? *Do we need more vectors to communicate both assurance need + "level"? *How are you filling the gap? * Where is it working well?
4M/ WEB AUTHN Together with DID's

Session 5
5A/Meta-Platforms cooperative network of Networks Scaling effects: Decentralized Identity – Transcontexted Value Transfer
5B/Intro to Self Sovereign Identity - 101 Session
5C/5Radical Ways to Keep Vendors Accountable for Your Data!!! Kantara Consent Receipt
5D/Is Practical Sybil-Resistant Self-Sovereign Identity Possible?
5E/MyData HUB (101:The Declaration)
5F/OAuth Clients Create Token
5G/The Case for an OIDC Ephemeral ID
5H/Machine Identity
5I/Deep Dive Demo – Connect Me + Onfido Creden
5J/Digital Natives: How do we get them to care about Digital Identity?
5L/Wyoming Laws & Regs Proposals
5M/Ask Me Anything about Sovrin Foundation

Wednesday May 1, 2109

Session 6
6A/A Process for Discovering Truth? Can credentialed chains, or other ID Tech, help create authentic voices learning from historical research practices of Museums & Archives.
6B/OpenID Connect for Identity Assurance
6C/FastFed Easy Connections IDP – APP + Governance – Who should have permissions in the App
6F/Developing Standards – involving Non-Tech? and Tech? People
6G/Alice to Bob – Self Sovereign Interoperability Without Censorship – U.S. Federal Regulations
6H/DID Communication – What is Message Routing and why you want it in your life
6I/XACML / ABAC / UML 2.0 and SSI Policies
6J/Let's Build A Decentralized Social Network
6M/What's Supposed To Happen When A DID Operator Goes Out Of Business?

Session 7
7A/XYZ Transactional Authorization
7B/BC Gov , MATTR, STREETCRED – IIW Book Redux
7C/Healthcare & SSI ??? Use Cases for All
7F/Protocols vs API's – Resolving the programming paradigm difference between DIF and Indy
7G/Approach to Bottom-Up Standardization of Claim Content Structures #interop
7H/Git +DID pt. 2.1

7I/Making a Map of all the Working Groups Working on SSI/Decentralized ID + how it fits together + making a weekly/monthly + yearly calendar
7M/DATA Fiduciaries FTW

Session 8
8A/Git + DID pt 2.2
8B/GC Gov – Indy Catalyst Agent + Agent Framework: What are they?
8C/Product Chain Overview & Update
8D/OAuth 2.0 + on single page Applications
8E/Anonymous Saliva DNA Extraction Kit using Blockchain
8F/Privacy Chain Overview & Update
8H/Where Have All the Trust Frameworks Gone?
8I/Continuous Access Evaluation Protocol (CAEP)
8J/Taxonomy for Digital Credentials – interoperability / multilingual
8K/Verifiable Credentials Q & A?
8L/How Can We Detach Users from CENTRALIZED Social Media?
8M/DID Communication Message (JWE) Encryption

Lunch
Karma DID Method
Domain-Specific: Governance Frameworks – What are they and why might you need one?

Session 9
9A/Linked Secrets and ZKP's
9B/Women In Identity @womeninID *Plans for 2019 * How do we create success? (Allies & Supporters Welcome!)
9C/Vectors of Trust
9D/DID Communication Message Types
9F/Self-Sovereign Commerce (VRM, Me2B) Progress Report & TBD's
9G/Paradox: Recovering from Maximum Personal Data Disaster (when all is lost)
9H/Are Crypto Wars Coming? Issues & Solutions
9I/Workshop on a Layered Model of Identity for Iteroperability
9J/App Level proof of Possession Dpop/Pop A Case Study
9L/Privacy Engineering in Context + Relational Integrity
9M/#Smart Custody

Session 10
10A/Seed Quest 3D Game Mnemonic Easy + Fun Demo Seed
10B/Me2B Alliance Intro
10D/How to Issue That? The DIF Credential Manifest
10E/The Peer DID's Without a Blockchain or any other Central Truth
10F/Managing SSI (A relying party perspective)
10G/How Do We Move From Good Intentions – Gender Parity at Conferences
10H/Creating an Ecosystem of Trusted Applications – Oauth2 Dynamic Client Registration
10I/Overlays (ODCA) What are they and how do they intersect with self sovereign identity?
10J/IEEE in Digital Identity + Inclusion – InDIITA 2019 Bangalore – Standards + Programs – Ethics
10L/Community Claims & Discovery
10M/There Oughtta Be A Law! OCCAM's Regulation, Legal Engineering, & Policy

Thursday May 2, 2019

Session 11
11A/Fraud w/Cred – Attack Vectors and Remediations
11B/Intro to Me2B (1/4)
11E/Why "Specific & Informed Consent" is Nonsense (or Not)
11F/Hub/Agent Cloud Stuff Project/Company Intro's/Explainers
11G/PWN-Back Your ID (from Equifax, Experian, Transunion) Check-it-Protect It
11H/DPoP – Current Draft, Next Steps

Session 12
12A/On No You DIDn't! Your identity is not self-sovereign.
12B/Me2B – Have YOU Changed Activity Because Unethical Data Company? (1/4)
12C/Get Real ONFIDO ID on Your Connect.Me Digital Wallet
12F/Wireline P2P O/S
12G/What Do Activists Need To Know?
12H/Sidetree on Ethereum "Element
12J/Otology + 00 Taxonomy – Crafting Chaordic Organizations in an Ontonomic World

Session 13
13A/Hub/Agent Action Meta Protocol
13B/Social Contract: Universal Guiding Principles – Me2B (3/4)
13C/The Identity.com Validator ToolKit / Demo with OnFido +SoOm Integrator
13D/How SSI Can Disrupt Platforms
13F/OffChain (PKI) Key Management – Revocation Rotation
13G/Latest in Verifiable Credentials Crypto
13H/Workflow/Forms and SSI Credentials

Session 14
14D/PDPR (Personal Data Protection Regime) – A discussion on Digital Street Smarts & IDRC What are the foundational rights of an individual= Independence Respect Dignity Consent
14F/Let's Make a Map! Of OAUTH Specs
14G/What I learned in India about their National ID System
14J/Hyperledger ARIES – Ledger Agnostic Open Source

Session 15
15A/Formal Security Analysis of Web Protocols
15B/Me2B Code of Practice / Harms Workshop (4/4)
15F/Selling the Business of Value of DID's
15G/SSI Agents for the IoT Using Pico's
15I/The 4 Layer Digital Trust Infrastructure Stack

Tuesday April 30

DID Communication, Callbacks, Hubs & Agents

Tuesday 1A
Convener: Sam Curren
Notes-taker(s): Colin Jaccino, Sam Curren & Stephen Curran

Tags for the session - technology discussed/ideas considered:
DID Communication. JWE #did #ssi #hyperledgerindy #interoperability

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

1. **Notes from Colin Jaccino**

Starting with assumptions:

- We have a DID, and a DID Document

DID Document contains:

- Endpoint Information
- Keys

Obvious Pattern:

- User with smart phone
- User communicating through a browser
- Server serves up a web site

QR code scanned by a phone presents a URL that the phone uses to get back to the service. Callback URL.
There is a huge opportunity to standardize how we communicate this callback URL.

You might have a phone-to-phone use case. But supporting this case is hard.
There might be a need to be transport agnostic

DID Communicating - if you're using a DID and it's a key element that you bring to the use case, the other systems and elements will need to be able to communicate with one another as well to serve your use case.

Audience Comment: you might need to support IOT in addition to servers and application.
Audience: How is this different than just providing the DID in a JWT token that can be passed around?
Convener: That sounds like we will , but the devil is in the details
Audience: You need transport agnosticism, integrity, routing, Interoperability.
Audience: Interoperability is the hard part. Standardizing the QR code is important.
Audience: Food for thought requirement - need to support multi-party interactions. If there are many parties, how can they interact together? Two party solutions are not enough.

Audience: Need to break up multi-party into whether its verifiable. Private? Is the communication insular? Group knows who is in the group vs not
Audience: Repudiability? Is everything "on the record"?
Audience: Namespace governance? Conventions that govern identification of elements. DID Doc Conventions?

Convener: We have many communities in the space.
Hyperledger Indy - Modified form of JWE (JSON Web Encryption) to pass messages that are authenticated encryption.
Civic
uPort
DifHub
Transmute
Jolocom
Kilt
LifeID

Ways we communicate DIDs relative to Transport Agnosticism
JWT - Reliant on transport security
JWE - moved some of the identifying portion into the protected block.

INDY is JWE
uPort, Civic, Jolocom, Kilt: Uses JWT solution
DifHub - JWS inside of JWE

Since JWT relies on transport encryption, it's not perfect as transport agnostic
Convener: Would projects that have chosen JWT who then choose to go transport agnostic naturally move toward a solution line JWE?

Audience: Perhaps a project could use a standard signature in HTTP header.
(Diddery)
Audience: Important to be clear to separate signing and encryption.
Convener: When you have JWT and encryption, we enable non-repudiability. It's important that we preserve it. Are there other paths forward?

- Direct support for DID in TLS? Standard supports it, but implementations do not.
    - The assumption that there is a certificate store and traceability up to a root certificate is an implementation assumption, not in the spec. In TLS, it is permissible to trace back to a DID document, instead. To support this, implementers would have to re-understand the architecture of their certificate verification architecture.

Audience: In zero trust networking, you're always encrypting at rest and in transit. You're always encrypting for the recipient. TLS doesn't matter.

Audience: TLS has limited applicability and partial adoption. TLS doesn't work over some transports, such as NFC. Not a safe assumption for protecting the DID.
Audience: TLS is sometimes deliberately man-in-the-middled. It's not guaranteed to encrypt end-to-end. It is not a trustworthy security control.

Audience: You could compromise DIDs the same way we have with TLS.

Convener: Let's move past the JWT vs JWE. There are significant advantages to moving from JWT to JWE.
Audience: If you're trying to leverage existing tooling, We just need enough to protect integrity and non-repudiability.

——
Audience (Tobias): Not all DID communications are going on with a browser. With just a QR code, we may not provide enough context for the services to support the use case. There may be cases where we shouldn't be encrypting or hiding the DID.

Convener/Audience: Would moving to JWE be interesting? Would ubiquitous tooling lead to more adoption of JWE?

Audience: The problem with adoption is that folks aren't adopting support of DID period. You need more reference implementations that can be brought into projects to enable uptake. You want fewer requirements on the underlying infrastructure.

Convener: Where are the opportunities for more work?

- There is value in determining the simplest possible way(structure?) to convey the information that must be protected in a message.
    - JSON LD-like type for messages. Without as much of the "baggage"
    - Message types tend to come in families that support domains of functionality
    - Routing: Uses the content of these message types to simply ask an agent to route on the message flow's behalf. "Agent Routing"
        - Audience: please explain more about routing. don't we need address space?
        - Convener: Two problems:
            - How to do the routing "on the way in"
            - Routing based on agents. A node-to-node .
        - Audience: This is a "circuit-switching" pattern.

Closing
Next conversations:

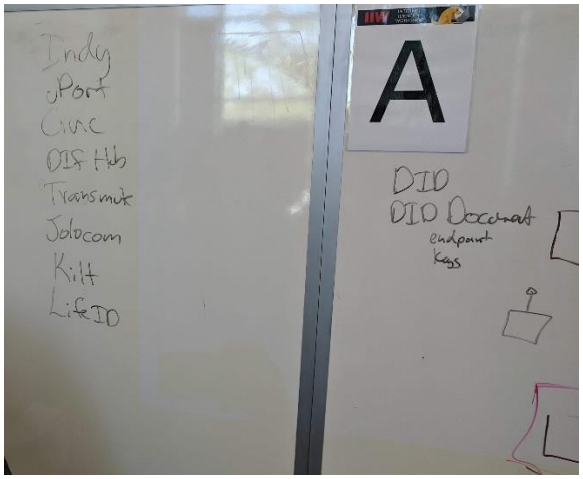
- Agent routing discussion.
- API Mindset vs Protocol Mindset
    - Multi-party

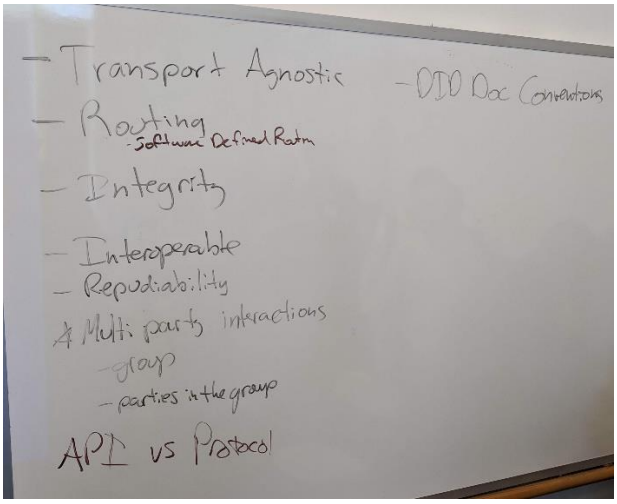
********** ********** ********** **********

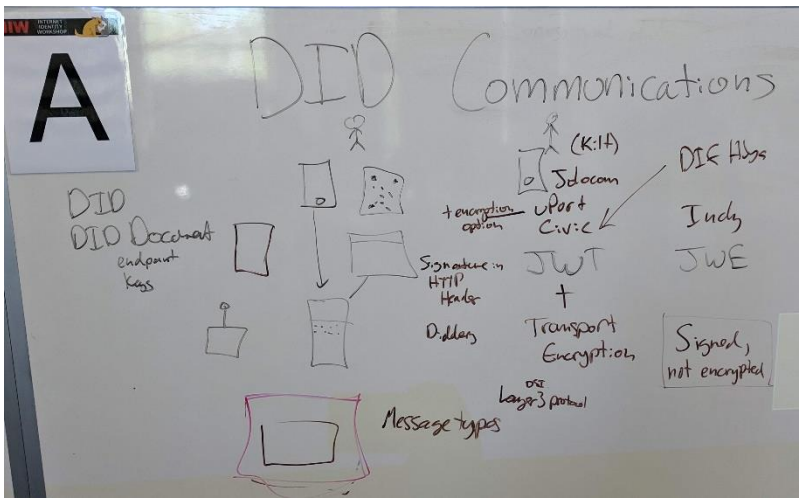
2. <u>Notes from Sam Curren:</u> We covered different aspects of DID based communication.
One aspect is message level packaging. Community members are primarily using JWE-ish message encryption, or relying on JWT for signatures and then transport level encryption.

We will be having further sessions to address specific topics:

- Wire-level wrapping (Kyle Den Hartog)
- Message Routing (Sam Curren)
- API vs Protocol approaches (Daniel Hardman)
- Message Structure (Sam Curren + Daniel Buchner)







********** ********** ********** **********

3. **<u>Notes received from Stephen Curran:</u>**

Scope of Discussion

If you are using DIDs, how are your peers communicating?

Components:

- DID, DIDDoc, Keys, Endpoints

Challenges in DID Communications

- Different transports provide different levels of trust
  - Nice to have - transport agnostic with same level of trust
  - For example - encrypt/base64 the message and deliver it using any transport

- Persistent endpoints are needed for mobile, implying that some amount of routing is necessary
  - Likely, you don't want your presistent endpoints to be able to see the messages intended to be processed on your mobile device.

- Routing / Software Defined Networks

- Interoperability
- DIDDoc Conventions - how are configurations expressed in the DIDDoc (e.g. routing)?
- Repudiability
- Integrity
- Possible issue (not clear yet): Multi-party communications. That further splits into:
    - Groups
    - parties in a group

What communities are present in the discussion

- Hyperledger Indy
- uPort
- Civic
- DIF Hubs
- Jolocom
- Kilt
- Transmute
- LifeID

Two Basic Approaches Used Today:

1. JWTs with the transport layer handling encryption (usually HTTPS)
    - uPort (also has an encryption option), Civic, Jolocom, Kilt, DIF Hub (for some transactions)
2. JWE (mostly)
    - Hyperledger Indy, DIF Hub (for some transactions)

    Side note: Sam Smith

    - DIDery is using a signature in HTTP header
    - Keep in mind that Signing and Encryption are different activities

For the JWT/Transport Encryption Implementations

Question: If you are thinking of going to transport agnostic messaging, what approaches are you thinking of taking?

Why?

- While the JWTs and using HTTPS for encryption works nicely for the User-to-Enterprise use case and is easy to get started with (good tooling), it will be challenging in for peer-to-peer messaging.

- It will be challenging to be in alignment with Zero-Trust computing initiatives. In such environments (which will be everywhere), encryption is required for DID Communications (e.g. messages) in transit and at rest. It makes sense to encrypt messages for saving and sending, regardless of the transport.

Proposal: When moving to transport-agnostic encryption, go with JWEs using the DID Doc keys for encryption. Put another way, go with the approach used by Hyperledger Indy and DIF Hub.

Response: If not accepted as a good approach, there was little dissent expressed in the follow on discussion.

Aside: One participant mentioned that they are experimenting with altering the OSI Layer 3 (below Transport) to handle encryption.

Aside: TLS 1.3

- The TLS 1.3 protocol supports the use of DID-type keys, but none of the implementations support it, and adding the support is a requires a non-trivial rewrite that is unlikely to happen any time soon. Further, adoption of TLS 1.3 is still happening relatively slowly.

- Solving the issue with TLS 1.3 would not make the communications transport agnostic, which is at minimum a nice to have, and perhaps required.

Routing

In Hyperledger Indy, routing is done using "forward" messages (aka envelopes). Forward messages are sent to intermediaries as envelopes with a "To" address for the next recipient and the payload (itself a message) encrypted for the ultimate recipient. This enables an onion-type of routing (envelopes in envelopes...) with intermediaries able to see only enough information to do their job - pass the message along. They cannot see the payload within the envelope they are handling.

The appropriate routing is communicated by the receiver to the sender by a path to each destination agent into the DIDDoc. The sender wraps the message into as many forward envelopes as specified to get the message to it's intended recipient.

Aside

- This routing appoach reminded some in the session about the early days of sendmail and circuit switching networks.

- Note that since this routing is being done at a higher level of the networking stack, this would seem to be more akin to a Software Defined Network (SDN) approach than those no longer used approaches.

Conclusions

While the JWT+HTTPS approach is the right starting point (good tooling, understood model), the reliance of transports for encryption is probably not the best idea in the long term. As other approaches are evaluated, consider the JWE path as it seems to be the best approach.

Additional IIW sessions to be held:

- Kyle Den Hartog on JWEs, making Indy's "almost" JWEs into JWEs and migrating from JWTs+transport encryption to JWEs.

OAuth2: An Introduction (101 Session)

Tuesday 1B
Convener: Justin Richer
Notes-taker(s): Allyn Chen

Tags for the session - technology discussed/ideas considered: #OAuth2.0 #Authorizationprotocol

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

* What is OAuth 2.0
Delegation protocol that lets people allow applications to access things.
Client in OAuth is the software that tries to access the protected resources.

* Old way
**Copy the resource owner's credentials and replay them to the protected resources.
Problem: need give the key, no management on the access.
** Universal key
** Service-specific credentials

* Authorization server
the Authorization server gives us a mechanism to bring the gap between clients and protected resource
** Generates token for the clients
** Authenticates resources owner
** Authenticates clients
** Manages Authorizations

* OAuth token is opaque

* OAuth 2.0
** Modularized concepts
** Separate previously conflated components

OAuth 2.0 defines common concepts and components and different ways to mix them together.
Therefore OAuth is not just a protocol, it is an ecosystem today.

OAuth Is not:
Not defined outside of HTTP.
No User to User Delegation. (OAuth is targeting to allow the user to software delegation)
No Authorization processing.
No Token format
No encryption method.
Not an Authentication protocol.

* Step by step
1. Client redirects the customer to OAuth Authorization server.
2. Resources owner Authenticates with the Authorization server
3. Resources owner authorize the client.

4. The authorization server redirects resource owner back to the clients with an authorization code.
5. Clients send the Authorization code to the Authentication server's token endpoint. (Clients Authenticates using their own credentials.)
6. The authorization server issues an OAuth access token to the clients.
7. Clients access protected resources using the access token.

Refresh token:
* Issued alongside the access token.
* Used for getting a new access token.
* Not good for calling protected resources directly.

Scope:
Type of action.
Type of resources.
Limits of access time.

OAuth protocol is flex. Drives to a lot of different protocol.
1. Implicit flow.
2. clients credential flow.
3. The resources owner password flow
4. The device code flow.

WebAuthn: An Introduction to the Specification

Tuesday 1C
Convener: Nick Steele
Notes-taker(s): Jordan Wright

Tags for the session - technology discussed/ideas considered:

#authentication #passwordless

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

We covered the core principles of the protocol, how requests and responses are handled, and how WebAuthn authenticators can be different types of devices, FIDO-specific or otherwise.

We also talked about how FIDO2 is not only WebAuthn, but includes CTAP2, the Client to Authenticator Protocol, which is not necessary to accomplish Web Authentication, and how WebAuthn prevents phishability by scoping credentials to a Relying Party.

Additionally, we discussed how WebAuthn can be used in Federal agencies, how we can attach additional identifying information, and what resources can help with implementation of the standard.

Helpful sites included: webauthn.io webauthn.guide webauthn.org webauthn.me webauthn.bin.coffee

Your Data, Your Currency + What Do People Need to No Longer Need Facebook?

Tuesday 1F
Convener: Lubna Dajani & Ricardo Mendez
Notes-taker(s): Scott Mace

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

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

Lubna – Your data, your currency, your terms

Other leader: Merged with how to leave Facebook

The privacy paradox – short term convenience trumps long-term gains

Lubna: FB is convenient. First ubiquitous platform where people discovered childhood friends. People don't understand the depth and magnitude of what's being done with their data.

At least 3 privacy paradoxes academics are talking about. People will share things more intimately with strangers (Brookings Institute). Behavioral economics. Third, difference between what's claimed and what's delivered. Search "privacy paradox"

Doc: I'm here for the terms. If we're not talking about terms, I'm going to bail.

Lubna: How do we transition to the next world. I want terms I define for how you engage with me. This is my data. If data is the new money, and we are the generators of data, how do we take control of our own currency?

Doc: If you start with what people care about, you'll never invent anything. Data is a head trip. We're dealing with considerations. They may or may not involve data. We're in control of what we reveal to other people. We don't have that online.

Does it matter what motivates people?

Almost irrelevant. The lawyers look for harms. There aren't a lot of harms. We haven't built the thing we need yet, the thing we need for ourselves yet. We're all wearing privacy technologies right now (clothing). They're norms. We're naked still online. What can be done with tech will be done until we find out what's wrong. FB is a learning experience that is a model for itself. Whole other things we could do. Such as what do I want here? We've already written no stalking. This saves publishing today if we do it.

Jeff O: Demo table tomorrow. GDPR, my bit is PDPR, personal data protection regimen. Understanding ourselves, that free is appealing. There's an association with dollars and cents. Really we're talking about cost. More exploitable is the data. The word free should not be involved. The cost is your data. Free is a dark pattern. The human element.

Joyce: SB 1084, a dark patterns legislative bill, the Detour act, deceptive experiences to online users reduction act. Become aware of private social networks, such as the one in Sweden.

Doc: We learned about it from Chris Savage.

Silicon Valley funded think tanks are going to D.C.

Scott Mace: Another group active in D.C. is the Center for Humane Technology, Tristan Harris' group, mentioned prominently in Roger McNamee's book about Facebook, Zucked.

In Japan, students are getting free coffee in exchange for their data, matched with employers. Functioning business model for your data, your currency. Clearly not the students' terms. FCC lawyers say if you don't agree with the terms, don't sign up. Doesn't work well with LinkedIn where you have to sign up to be employable.

What are we really afraid of? (Many think targeted ads are great). How far do the terms go? Could be much larger than an EULA.

Objecting to surprising uses of data.

Joyce: Trust is actually a commons asset. When trust breaks down as a commons, now nobody believes anything. We need to insure that we share trust. Chris Savage's academic paper is posted on the Project VRM list. People think it's just ads, but your information can be used in ways you never thought. Do you know how your car insurance rates are set? Consumer Reports 2-3 years ago, the #1 factor should be what kind of driver you are. Actually it's your credit profile. Plus zip code, other things. American Express will turn you down on a credit card if people who go to a bar you go to with bad credit. A bunch of examples like this. People have learned to trust companies and institutions. If FB was bad, my friends wouldn't use it. I can hardly open an email, is this spam? We've lowered the trust so much. Can't get it back up that quickly, unless we have some agency to see who that person is. Tools are the way.

OnStar comes with the vehicle. Built in. GPS, cellular tech whether you enable it or not. Insurance company could easily find out the driving history from GM. Would an insurance company care about that? This came with the package.

Another example, your credit rating was determined partially by shared addresses with people with bad credit.

Lubna: We are living in two eras at the same time. Kids now can swipe before they can stand. We do need an interim for this time. What does my data mean?

Come to the MyData session.

Privacy: Control what you share and with whom. This is my car I paid for, I should be able to control what my car shares with.

MyData guy: There's a rights issue. Every right is bounded by other people's rights. If I choose to share my information with a trusted party, I cede some control to them.

Jeff: Say you have a Nest thermostat, 20 years of data, using this energy, you had it well, we'll be parsing the space down. Others were more frugal. A creepy potential. Happening right now in China.

Joyce: Chris's paper is: Managing the ambient trust commons, the economics of online consumer information privacy. We take the commons model, has much more value. Commercial model is doing the destruction of what we call trust. Many examples, hundreds of footnotes.

20 people here, 10,000 at F8 trying to do the exact opposite.

What about a law like DMCA that allows takedown notices so my data can be removed.

But beware of unintended consequences, like corrupt politicians using GPDR to get sources revealed, or stories taken down.

Decentralized DIDs

Tuesday 1M
Convener: Joe Andreu
Notes-taker(s): Heather Vescent, Nathan Martin, Kurt Milne, Ellie Stephens

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

1. **Notes from Heather Vescent:**

DID Background

Explain what a DID method is.

- DID
- Method
- String

Informal registry on CCG list: 22 methods registered

Lightweight requirements to list your method

- 3 for bitcoin
- 5 for Ethereum
- Various systems

History

Markus Sabadello + Oliver (uport) brought up issue
Oliver+Dmitri proposed DID:web(method):(methodspecificidentifier)

Dan Burnett: To be an easy on-ramp for people who were scared by the notion of distributed ledgers

Idea of bridging current technology and new technology

How can we connect existing technology/systems to new technology?

Fear of co-opting the technology by a large organization. (E.g. Facebook)

Questions

- What's wrong with the URL method/path?
- Supposing I want a centralized ID?
- Can you have Sovrin method in a vertical/federated (e.g. financial industry/mobile network operator) – it is decentralized but also centralized. Could they implement Sovrin in those configurations? Would you consider that to be more centralized or decentralized?

Logistics (how Joe is running this meeting)

Will list **decentralized points** vs **antipatterns**.

Characteristics of decentralized and !decentralized.

Decentralized	**!Decentralized (antipatterns)**
Any root of trust Provably under • Controller of DID • Controller Anti-censorship (censorship resistant)	Single root of trust Required use

- Chris A: Architectural, political, social categories of categorizing decentralization
- Joe A: Avoiding political, focusing on the functional aspect of identity. What is the criterial for a good DID method? This isn't about controlling what people might do. We are creating a working group to create the standard/debate that define what DIDs are.
- Drummond: A DID is a URI. The 4 things brought up on the list
    - 1 Persistent: signed once & available forever
    - 2 Resolvable (to the DID document)
    - 3 Cryptographically verifiable
    - 4 Not under control of centralized authority
        - What is the definition of a single authority? Is a government? Nato?
        - A university? It really means, you want a good guy?
    - 3 is more important than 4.
    - This is cryptographic control (Drummond holds us phone). Look at it from the keys back, that is what we've designed. The DID is an identifier, for a public key that goes with a private key I control. Not always an individual, can be for a corporation. What system do you trust for the corresponding private key?

- Q: how do you classify an identity that is assigned by a government, or university – centralized?
    - They are centralized.
- Not talking about distributed identifier. The methods are each a root of trust (in their domain).

- The platform level – can choose any root of trust.
- DIDs and DID Documents should
- DIDs feed into VCs
    - Should be able to move to DID Sovrin and DID Veres1
    - It's gonna be a nascar sticker problem for OpenID all over again.
- MS: Trying to get to clicks – who do you trust to get these.
    - Less Nascar, stickers, vs accept all these things
    - Move to claims vs identifiers.
- Separate the identifiers from the credentials.
- Drummond: 2 levels of roots of trust
    - Lower: DID level, root of trust is the decentralized network the DID method uses.
        - Issuer of the credential. University, register a DID on a certain method. Have that DID and use Private key to sign documents.
    - Other level: Verifier: the verifier has to decide 2 things – trust the university & secondary, trust the public key (the method).
        - If you don't trust the method, you can't trust anything from/using that method.
- Question: Why not URLs (format)?
    - It is a URL…
    - But you said URI
    - It's really more like a URN
- I don't see what is decentralized about DIDs at all. the claims might be decentralized.
- In the way that HTTP is centralized, so is this.
- This is a scheme for capture by a big player. Each method is an authority. We have watched repeatedly this get captured by an authority.
    - Is there something we can do to minimize/reduce this? Political, social, cultural?
    - Drive the preferential attachment to a big player
    - **What would drive the preferential attachment to a big player?**
    - What would make it popular?
- The question of DIDs are centralized
    - The answer is yes, all of the above.
    - The standard can say many different subpockets of control
    - Centralized issuance control vs operation/usage of it. Dependent on peers. It seems like it's a federation vs…
- Governance (rules) vs operations
    - But it comes down to policy
- There's no one to sue for bitcoin?

- Have you thought about the vacuum you create?
    - Where do you draw the line between anarchy and centralization?
    - FB is the largest IDP in the world, but they don't follow
    - They aren't good guys, they are vested interested in making this work
    - The standards are great, but how do we stop a crackpot.
- One of the killer apps – offshoring username/pws
- **One of these did methods should be able to fail/be compromised/corruption, the system continues.**

    - Andrew – this is the killer feature
    - What have we designed into a system, a user to location and reassign DIDs from a broken/failed/compromised system.
    - Dave: a mathematical truth, operational falsehood. Popular method, has access to docu…
        - This is a recovery feature
    - How are we building into the architecture for this?
        - Joe: this is a different layer
- Identifier can't be stolen, but it can be maliciously taken from you. But if you lose your keys, no one can give you new keys or reset.
- Markus: what's to prevent did:facebook
- It has to do with community and building a tribe/individuals that know you. It's about social recovery

********** ********** ********** **********

2. **Notes from Nathan Martin:**

***Glossary*:**

DID: Decentralized Identifiers (https://w3c-ccg.github.io/did-spec/)

KYC: Know Your Customer

AML: Anti-Money Laundering

IPFS: Inter-planetary file system

Intro

How many people know what DIDs are?

Half of room raises hand

We live in a world where we can now reliably transfer $100M without KYC + AML, a requirement traditionally held by banks. These IDs are not tied to a "traditional ID", e.g. driver's license.

DIDs record an identifier, and a means to control that identifier. There is no single root of trust. For instance, the blockchain-based IPFS with no centralized control or point of failure. Compare that with the https protocol, which ultimately resolve to a root of trust.

Problem Statement

What does the /decentralized/ in Decentralized ID mean? Is Bitcoin decentralized? Sovereign DID method is on a permission blockchain…is that decentralized?

What is decentralized? What do we want it to mean? Decentralization implies a requirement.

The challenge we're facing is that some argue…you start with a DID, you get a DID document…that's not decentralized at all! This could all become DID Facebook, Twitter…with no real difference from today. How can we have a good set of criteria? What is a good DID method?

Specifically, we're working to develop a specification that's evolving, and we're trying to make a community final version, to become an official standard. We didn't expect to get to the point of a

working group, but the W3C said it was important enough that we do it now. So we're finishing a charter, and will be going in to vote. We need to come up with a common language for…what is decentralized? This is not about control, it's that we're trying to create a standard. A good set of written English statements.

Discussion

DID is a URI. URI has been established for nearly 20 years. How to classify whether under control of a central authority?

Want to be able to easily move from DID provider A to provider B, similar to how today we might login with our Github, Facebook.

The standard seems to be moving towards claims instead of an identifier, trying to work with claims.

It's important to distinguish between claims vs credentials. There is a paper about verifiable claims, originally in early verifiable claims — Oasis group our research on how might replace XDI https://w3c.github.io/webpayments-ig/VCTF/charter/VCTF-final-report.html (unconfirmed report link by Verifiable Claims Task Force) .

When looking at a proof of a credential, e.g. student getting a discount at a university, there are two questions regarding trust:

1) Do I trust the university?

2) Do I trust the (DID) method?

Who determines trust? That yes, that DID belongs to the university?

DID can be politically centralized, it's just a protocol.

Useful to distinguish between various terms when referring to something being decentralized or not. Vitalik Buterin considers the following properties:

* architectural
* political
* logical (structural)

There is nothing that can meet all the rubrics! There is no perfect decentralization. When you have a single standard, you have a logical centralization, e.g. Bitcoin.

DID format does limit design space, but these are features.

Is http centralized? If accessible via the public web, it is centralized (under the root servers of DNS) because there is a single root of trust. The scheme isn't centralized, but each method is under an authority. An authority oversees creation of domain names, root servers can do whatever they want, but they happen to do the nice thing.

DIDs are centralized and they are not. You may have one taken by Microsoft, and one by Sovrin. Bridges the gap between centralized and not—a confederation of centralized environments. Issuing and complying with the protocol, the protocol is centralized, they manage but in compliance with overall standards. Yet it is not centralized, that is taxonomy. Let's not confuse following structure. Language is necessary for a level playing field.

Factors to consider about a name are registering, representing, using and assessing (trust for ownership). Right now, with the exception of P2P (as decentralized as it gets), all fall under decentralized network. There is no centralized registry. Are you inviting collisions? What enforces INFS servers? Convention.

What's the syntax: did:method_name:method-specific ID

E.g. `did:ex:abcd….`

Right now there are lightweight requirements to get into the registry, you let us know and make sure you've published it and followed all the rules. The current registry has roughly 22 entries: 3 are Bitcoin-related, 5 are Ethereum-related, and the rest seem to be application-specific. New ones are being proposed, e.g. `did:web:...` to make it easy for those scared of distributed ledgers. We're looking to make this bridge current + future technology, and address fears of the technology being co-opted.

What is the definition of a single authority? Really means, I want a "good guy". Distinction between governance, ultimately relies on institutions and others agreeing upon rules. Comes down to policy more than the rules.

Facebook DID can change at any time, versus Sovrin ensure operationally decentralized. With Bitcoin governance is chaotic (politicized). Is it technology or policy that makes it centralized?

Where to draw the line between centralization and anarchy? There is a vacuum. Facebook has a vested interest in getting it to work. Where is the practical application?

Killer apps:

* off-shoring password management

* government grant gatekeeper

* Getting a government grant requires going through some private company…it's like that company is baked in the government process.

What about resilience? If one fails, we want the whole system to be OK. If a method fails…it results in operational failure. In reality, you would lose all access to your documents. If a big system fails, you lose your documents. How to build into the architecture a way to stay operational? Let's clarify something here, think about the IP datagram. This discussion is not about reliability. This is regarding W3C, a syntax specification.

What if this committee fails due to being overly politicized? Can it be forked?

What is the relationship between cryptographic verifiability and "not under the control of a single authority"? Cryptographic verifiability trumps the other. All devices and sites store your private keys. What if I lose it? The point is…DIDs outward vs keys inward; a private key that I control. Ok then, what system do you trust for the address of that public key?

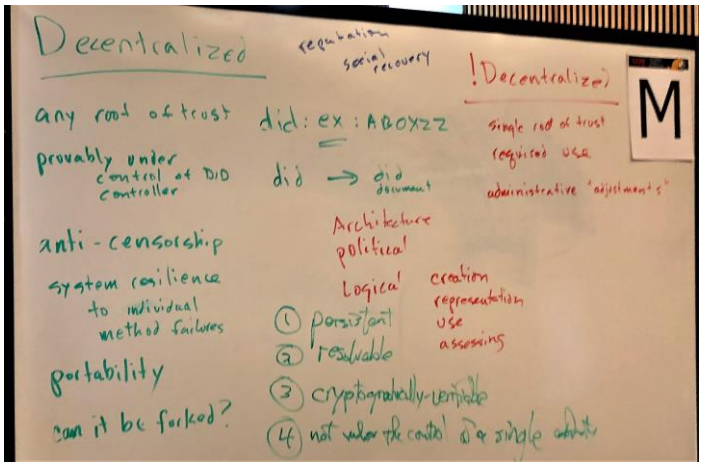
What if I lose my key?

Reputation management should exist. Community building tribe, in a group of 8 people, perhaps 4 needed for recovery of a lost key.

What's to prevent `did:facebook: ` where the method-specific ID is empty? Killer feature: the system should be resilient. What have we designed such that a user can generate another method at their own DID.

That DIDs are not under the control of a single authority seems to be an important point of failure. If that fails, all others fail quickly.

One of the DID requirements, that of persistence, is not feasible nor wanted! Tattoo it [DID] on my ass? It is morally abhorrent. And it can't be implemented.



********** ********** ********** **********

3. **Notes from Kurt Milne:**

Summary

Problem:

- What is decentralized mean in terms of decentralized identifiers?
- As DID implementer, what is a good set of criteria - what is or is not? Not about controlling outcome.

Intention:

- Bridge current and future technologies
- Fear of being co opted

Summary list generated by end of meeting:

Decentralized:

- Use Any root of trust
- Probably under control of DID controller (user?)
- Anti censorship - no one to subpoena
- Resilience - to individual method catastrophic failure
- Portability
- Able to be forked

!Decentralized

- Single root of trust

- Required use
- Administrative layer - (please reset my key)

Notes in order of discussion

Drummond: DID spec editor. Verifiable claims task force. Creating guidance for working group. Working towards community final version.

Discussed methods:

Start with DID, get document with keys etc.

IPFS methods

DID methods –
- Sovereign DID method - decentralized?
- ? Others

did:method_name:method_specific_identifier

Registry group - 20 current methods registered: 3 bitcoin, 5 Etherium
Methods for bitcoin: Create, update, deactivate etc.

Q: What about URL method? with method:path

Paper - who wrote initial paper ?
Term - originally in doc Manu early verifiable claim -
Oasis group presented at IIW - replace decentralized xDI
Rebooting web of trust

Meeting notes - add document links or reference to links

Sovereign method in vertical - federated financial industry multi-network operators

Self sovereign -

Side bar - Aspects/categories of decentralization - Source Vitalic Buterin (sp?)
- Architectural
- Political
- Logical

Drumond presented original spec - least to most controversial
DID - is a URI - standard has been around 20 years
Standard identifier on the web

1 - Persistent - sign 1 and forever URN
2 - Unlike URN - all DIDs are resolvable

- submit and get back DID document

3 - Cryptographically verifiable
- DID identified DID subject
- Whoever controls the DID - can prove the controller

4 - Not under control of centralized authority

Nothing against identified controlled by central authority

Methods are each a root of trust - within a domain -

DIDs and DID documents - should have credentials tied to decentralized identifier.

NASCAR problem - lots of logos

Industry moving towards claims versus identifiers

Use DMV to issue drivers license, would like them to use DIDs

2 levels Roots of trust

Example: Student goes to bookstore, wants student discount. Verifier (book seller) decides 2 things
- 1 - Do they trust issuer (University issues student ID)
- 2 - Do they trust method used (ID real or fake)

DID root of trust is centralized method used
- Register ID under some method, register, have DID, will have issuer credentials.

DID phishing?

Q: Back to question Why not URL?
A: Discussion

Bitcoin is rigid centrally. DID format limits design space.

Registry is not exhaustive or definitive

Scheme is decentralized to an authority
That approach gets captured historically

Real decentralization - no opportunity for that

Q: Does kill switch or other governance - reduce attractiveness?
A: Marketplace is highly decentralized - but prone to capture

Each method owned by entity - if it becomes popular

Opportunities of control

- Create/register the name
- Represent the name
- Using the name
- Reputation/trust of the name

Example decentralized name creation - odds of naming collision diminishingly small. This is not that.

Publicly available identifier - cryptographically verifiable

22 example methods registered.

Decentralized identifiers - not rely on single root of trust - for use with decentralized networks

If not centralized registry - invite name collision
What enforces use of INF(?) convention

Creation of domain names -

Q: re ask - Why not URL? More like URN?

Centralized issuance controls
Use of DIDs - between peers

If use environment
Confederation of centrally controlled

Issuance, protocol definition - centralized
Use of protocol in various environments (MS Google etc) - decentralized

Diffusing of centralization

- To enable decentralized nature - must agree on protocols
- Centralized - language needed to operate
- Decentralized - DID method, who can, who can't

Q: what does it mean to have a central authority.

Distinction - Governance (relies on humans) and operationally decentralized.
Comes down to policy more than rules.

Q: where does idealistic vision define practical application?

- People build and sovereign state caring about it e.g. offshoring password management

Phone - cryptographic control
What if loose it - what happens if loose phone
Design from user key back. Not DID out.

Q: what system do you trust - public key assigned?

Resilliance - Killer feature - if DID fails - system stays functional
Individual - relocate and regenerate DID on another method
If move off bad actor - still work

Q: What happens if catastrophic failure?

Operationally failure - popular Documents
Killer feature -
Moving a document is equivalent of regenerating
Recovery feature

Social recovery - Multiple people vouch for DID
Community - build tribe people that know you

IP datagram - not describe how to maintain

********** ********** ********** **********

4. **Notes from Ellie Stephens**

Blog discussed: https://stories.jolocom.com/prioritizing-individual-sovereignty-over-interoperability-95ec17a36c9b

What the blog calls for:

At the DID level the root of trust is
The university will register the DID at some method - bitcoin method. They're gonna use that public key associated that private key. They will be the issuer of credentials. Uni — > student. Student gives ID to prove their ID - does the bookstore trust the issuer who issued it, does it trust the bitcoin method. The vast majority of the trust is the university, but if you can't trust the trust that underlies it (bitcoin method did.bitcoin.university e.g.) then you can't trust any credential it issues.

I don't necessarily know that this would be captured by a large player

All that has to happen is for one method to become highly popular

If they're all largely the same

The web is largely decentralized for users but we gather around the facebook fire

Opportunities for control: creation/registering the name, representing the name (common syntax), using the name, — the reputation and trust and trust for the ownership for the name. An example for decentralized name creation is with algorithms large enough
20 methods registered with the ccgs. All of them are using some form of decentralized network. You can take that whole set put them against centralized registeries like we use today in DNS. Decentralized identifiers were designed for decentralized networks.

When you're using a method you don't have to register it?

No.

You're inviting collision?

This right here is the dialogue that has happened. If we are going to take a world of decentralized identity and put it on one central register, wPhil would say what actually ienforces the use of INS root servers? convention.

Uniform Resource Locator
Uniform Resource
Uniform Resource Name

Seems to me that the standards allow for many pockets of sub control and that it would establish communication between established issuance control and the operation and use of the dids is between all spheres I can't as a single individual depart from how I operate in the sovran environment.

Why do you want to work in their environment if you want to be decentralized

If you take something like the protocol definition which is very centralized if you allow that protocol to be used in various environments like Microsoft, they do so in compliance with the overall standard. It's

It's a taxonomy that people agree on not centralization. To enable the decentralized nature of it you have to speak the same language. Anyone can create a did method. It has to have did:method:XXX to me what you're calling centralized is the language that's necessary to interoperate at the base level and compete on the product level

What is the definition of a single authority? Is a foundation a single authority? It really means, you want a good guy, but how do you know who's the good guy? I think it comes down to policy.

The did:facebook doesn't exist. That means that I go to a facebook server to fetch my did and facebook can change it at any time. Operationally the DIF wants this to be decentralized.

Is it a technology that makes that single authority? Or is it about a policy that the company or organization does to make it

Anti censorship. Sovrin can be sued. Bitcoin can't. That's one notion of decentralized. If someone comes after the platform can it be sued?

Is there a thought in all this to the vacuum we might create - who's gonna fill that vacuum? Facebook is the largest id provider on the planet, but they don't follow any of our criteria. By crying to get to this idealistic point of view, do we not set ourselves up for failure or create a vacuum? Can this not be filled by the bad guy

The federal gov needed an identification system to send grants, so they give DUNs numbers, this is coming to an end,

One of the dids can fail and all of the others will still be fine

I think #3 is more important than 4. Real decentralization is that all of the devices have the keys. My phone is cryptographic control. What if you lose it? We have to solve it. If you look at this whole thing not from the point of the dids outward but the keys back. That did goes with the public key that goes

with the private key that I control. What system do you trust for the address of that private key

If a did method fails, then the system should still be resilient. If you can move away from your did then doesn't that solve the capture problem??

I own the did, what's the guarantee that I'm a good actor? There should be a score that's associated with my did that validates me as a good actor

I think this has to do with community. Individuals that know you. 4/8 people should be able to verify you. Social key recovery.

Mathematical truth. Highly popular. Lose acces. That's a failure operationally. You lost all those documents. Real decentralization would minimize that damage. If a big system fails. Moving a document is not a reliability feature, it is a recovery feature.

If the community builds it and it fails, can it be forked?

I give you a did and now and forever that did corresponds to you. I don't want that. And I have always had issues with persistence. Morally abhorrent.

What is decentralized	What is not decentralized
Any root of trust	Single root of trust
Provably under control of did	Required use
Any censorship	Administrative adjustments
Portability	
Can it be forked?	
System resilience	

IIW Book

Tuesday 2A
Convener: John Jordon
Notes-taker(s): Jim Wowchuk & John Jordon

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

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

1. **Notes provided by Jim Wowchuck:**

Key understanding: a demonstration of an identity authentication, issuing, relying party connection and document/chat exchange using authenticated identities.

Steps were described and followed as per slide 1 (photo attached).

Most of the session was walking through participants through the process and providing ids for delegates.

Discussion followed on about the increasing integration between different agent providers using a set of criteria as discussed on slide 2 (photo attached).

There was continued discussion about a Connectathon last February where 6 different systems were verified as connecting. Evernym was not a system that passed, but this was not held as a lack of ability as much as direction of activities – they had more important features they were working on.

Acceptance that even with non-connecting apps, all family protocols have many of the features but with slightly different protocols.

John Jordon speaking:

2. **Link to presentation provided by John Jordon:** Http://IIW.vonx.io

Introduction to Open ID Connect (101 Session)

Tuesday 2B
Convener: Mike Jones
Notes-taker(s): Mike Jones

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

See the PowerPoint and PDF versions references in the last line of the following link: http://self-issued.info/?p=1971.

Blockchain Social Media and Relationships

Tuesday 2C
Convener: Matt Vogel
Notes-taker(s): Selina Herrera

Tags for the session - technology discussed/ideas considered:

Needing to define what social media is. Why Yadacoin is the answer to social media monopolies. Giving demo and requesting feedback on the current state of the product.

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

A quick demo was given and discussion about blockchain social media started:

- YadaCoin aims to remove unique identifiers.
- Yadacoin blockchain is written in python 3.
- The blockchain is trying to give a backbone for relationships on the internet.
- Friends need to easily be found on the blockchain and YadaCoin is a central store of relationships, not users.
- Users generate transactions that represent relationships. Only relationships are visible on the blockchain.
- One person added the possibility of data analytics from facebook being given in exchange for some kind of incentive on the Yadacoin blockchain.
- Marketing advice included Tweets on Twitter in exchange for coins. Another marketing concept was that an invite could point to an already created wallet with coins.
- Social media is a “space” where thoughts can be collaborated and people can feel safe. - A person asked why would the younger generation be interested in using the yada blockchain? Response was that yadacoin could capture young crypto enthusiasts who will use the wallet and its features, but also noted that service providers could abstract the experience to be virtually identical to a classic client/server application.

- Another person inquired about a use case pertaining to government use where a user’s identity can be consistent across different systems without the need for a central server for authentication. The response was that this is certainly possible and could be done because the blockchain retains relationship data that can be used to authenticate at later times.

Identity Management in Physical Security World

Tuesday 2D
Convener: Rajesh Arukala
Notes-taker(s): Rajesh Arukala

Tags for the session - technology discussed/ideas considered:
Mobile Credential, Security Convergence, WebAuthn

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

1. Discussion was focused primarily on how the User Identity physical security and access control systems world is different from IT and online Authentication and current state of Identity management in Access control systems.
2. Discussion on how centralized identity providers should also focus on physical security and access control systems as well.
3. While Authentication in IT world is moving towards using devices (smart phones) and keys (U2F Keys) as a second factor, Physical security teams are considering replacing the physical badges with mobile credentials that can be stored in devices such as smart phones and can be used to authenticate with bluetooth/NFC enabled readers to gain access to facilities.
4. Mobile Credential and WebAuthn share some similarities in-terms of How they work on exchange of pair of keys.
5. Critical Infrastructure facilities such as Utilities, Nuclear Facilities, Date Centers, Banks require verifying the Access (Authenticating and Authorizing) in incremental and layered approach: All the way from Access to physical perimeter to a configuration changes to a control systems within the facility.
6. Discussed on various methods (User behavior analytics) and technologies (Density Sensors, Micro location targeting) that can be used to verify the identity where physical presence is mandatory to gain access to perform specific critical function.
7. Discussed on various critical infrastructure breaches that resulted in loss of human lives.
8. Expressed interest on forming a interest group to discuss on these topics further.

Sidetree Protocol: Scalable DIDs

Tuesday 2F
Convener: Daniel Buchner
Notes-taker(s): Karyl Fowler

Tags for the session - technology discussed/ideas considered:
DID, scalability solution, blockchain-agnostic, Bitcoin, Ethereum

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

- Raiden on ETH & Lightening Network on Bitcoin are the only [channel-based] scalability solutions for transactions on blockchain protocols to date; this is not sufficient for most applications.
- Scalability Trilemma: decentralization, scalability & security
- "Scale of identity" - humans are just tip of the iceberg (7.5 Billion but devices are far more and rapidly growing)
- We need protocols that are *generic.*
- Requirements for DPKI: 1) global, immutable, append only logs, 2) no central providers or authorities and 3) censor/tamper resistant
- Key realization is that identity doesn't have the same double spend issue as money.
    - Although this opened a larger discussion around the nuanced challenges specific to ID.
- Sidetree technical assumptions: 1) no secondary consensus required 2) no conflicting states are allowed and [to achieve this, we anchor to layer 1] 3)ID states are siloed and do not affect each other
- "Sidetree uses blockchains as an oracle of time." – Daniel
- Like timestamping, in that any writing node can collect operations, Sidetree protocol lets you send your operations off to another node (that say, Microsoft or another service provider is running) to avoid you paying those costs.
- Optional: Holding batch files *and* anchor files [vs only holding one] = enormous difference in node size for holding both vs holding only anchors
    - Why would a company retain your batch data? to retrieve/parse *fast* for their customers.
    - But, you don't need to rely on this; you can persist this data yourself on your own node.
- Sidetree has differential capabilities, so you can have a node that only replicates your own operations or specified types of operations (e.g. financial transactions, DID attestations/authorizations, etc.)
- Sidetree relies on the layer 1 consensus model to verify DIDs
    - Sidetree is 95% of a DID method; it becomes whole when applied to a chain and configured to support a chain-specific method
- Audience Question: How do you know how to resolve certain payloads on certain chains if you're not running a node specific to a chain? **Ask Orie re: what is url for DID methods we use/why we consider Sidetree a DID method [for sales]**
- If I am not running a node myself, I only need **one of the nodes in the network to be honest** [because I will always be able to deterministically compare/check their work]; very strong property of Sidetree Protocol

    - Follow On Question: Is it possible to collapse Sidetree such that all layer 1 protocols can be supported under it. Answer: Longterm, we will have libraries to reference. Other responses included:
    - Perhaps “time” is confusing as a term for a premise; let’s call it “order”[of events]
    - if there is no consensus on layer 2, then first hash always wins.
    - The protocol is based on “first seen,” so for cross chain/interchain applications, you will need to find a way to determine first seen across chains.
- Transmute’s Element Implementation (Sidetree on Ethereum):
    - Demo video: https://www.youtube.com/watch?v=KY_dt2tKQxw
    - Get started: https://github.com/decentralized-identity/sidetree-ethereum
- Audience debate: some IoT devices cannot support/handle certain hashing functions, so what about the case where a device generates the DID and key?
    - Further context: DID documents decouple the hashing function from the identity; some are concerned that Sidetree recouple these things in a limiting way.
    - Some Answers included: The IoT device doesn’t necessarily have to know its DID in the Sidetree context
    - or a Sidetree compatible DID can be generated by the protocol on behalf of the IoT
    - OR you can just change the hashing method Sidetree uses when you implement it

A Standardized Information, Governance, Label for Apps & Services

Tuesday 2G
Convener: Adrian Gropper
Notes-taker(s): Thomas Berry

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

Link to PPR Information Governance Label Doc: **https://bit.ly/PPR-IGL**

Formed from work on Patient Privacy Rights (PPR)

- Shift risk to consumer or service provider (supplier)
    - Facebook/Cambridge analytics
    - Nutrition information on food

- Variation on Privacy by Default (e.g., HIPAA)

Service App ranks 0-5 √

- 1. No sharing: The data is never shared with any external entities. It is not even shared in de-identified form.
- 2. No aggregation: The data is never aggregated with other types of input or data from external sources. This includes mixing the data gathered via The Device with other data, such as patient-reported outcomes.
- 3. Always voluntary self-identification: The user of The Service is able to choose their own identity, the user does not need to have their identity verified unless required by law.
- 4. Digital Agent Support: The user is able to specify a digital agent, trustee, or equivalent information manager, and this specified agent will not be subject to certification or censorship.
- 5. No vendor lock-in: This service is easily and conveniently substitutable, so the user can easily move their data to another vendor providing a similar services. This prevents vendor lock-in and is often accomplished using Open Standards.
- [6. Differential Privacy] removed because it could be gamed.

Indications for Use: The five separately self-asserted statements on the PPR information Governance Label are subject to legal enforcement as would the privacy policy associated with The Service

Objections:
A. Could decrease sharing which could be damaging to community benefit (e.g., science)
B. Aggregation may restrict functionality
++C. Does not state how data will be used (stated positive purpose of use)
D. Not useful if no choice
E. Too “strong” or “rigid”
F. Privacy by default is [could be] antisocial
G. Needs ordinal checkboxes (red-yellow-green)
H. 5. No vendor lock-in is too loose to be useful
H2. Bundling of service is discouraged
Vendor lock-in has to be “loose”
I. Too philosophical

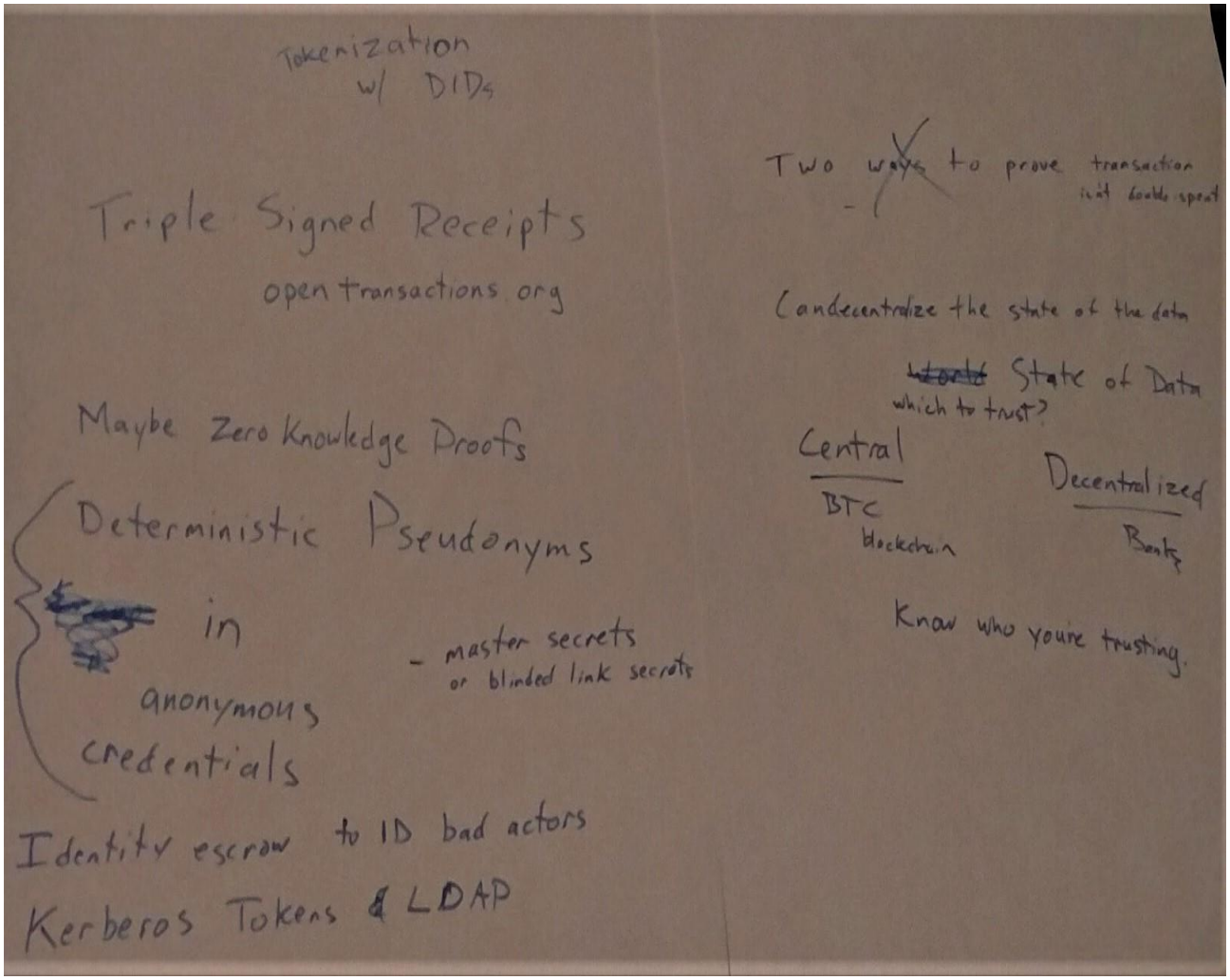
Tokenization With DIDs?

Tuesday 2L
Convener: Trent Larson
Notes-taker(s): Trent Larson

Tags for the session - technology discussed/ideas considered: #Blockchain # DIDs #property

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

Photo received from Trent Larson



SSI Startups

Tuesday 2M
Convener: Timothy Ruff
Notes-taker(s): Heather Vescent & Ellie Stephens

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

1. **Notes from Heather Vescent**

SSI Startups
Credit Unions (call in, walk in, log in) **Credit Reporting Agencies - CRAs** "ultrafico" Thin files → (Finisity, Experian Boost) A new way of creditworthiness, by looking at how you manage money. A new model, regardless of income and payments on time, they can analyze how you manage your transactions, they can determine whether you are responsible with your money. Booster 17% of the Thin files, can be borrowed. He can take banking files via open banking, asks permissions to see your transactions, algo calculates your score, and you can buy it / sell it to others. **Credit industry** – fraud is a major issue. In a few years, 50% of the calls will be fraud. The security measures to prove you are who you are when you call in. (CU Ledger project??) To authenticate their own customers online. Pet identity Medical Data

Centralized Identity example: Passport failed because they tried to own it.
We're going to solve the identity problem, but through us, they create the same identity problem over and over.

Sovrin – use DLT and get the right people to invite the right way to use this & open source it and give it away, and one way build a profitable business on top.

The scary part is to spend money/resources and build something and give it away. Raised $25M and gave a lot away… and successfully moved the needle. A lot of people think that Sovrin is the right way to do this.

Something's happened in the few months – Hyperledger Indie

"Independent identity"

- Babies need SSI, are they capable of being SS?
- What about things?
- What about disabled people, elderly

An entity that needs an ID, but can't give it to themselves, it is a guardian style.

Indie codebase, got moved from incubation status to active status. (One of 3 active)

- Hyperledger Fabric (IBM)
- Hyperledger Softtune (Intel)
- Hyperledger Indie (Evernym/Sovrin)

There's a point of maturity in the stack.

"They talk about what identity should be at IIW"

Self sovereign identity was really cultivated here. It starts with ideas and then to practicality.

The stack of SSI is ready for primetime?
Blockchain is experiencing the same thing.
What everyone is looking for is real world applications.

Crazy Ideas/uses for SSI Technology

- Pet identity
- IoT
- Voting
- Healthcare

Best ideas, that can be funded by an investor.
An opportunity to become a good business (an investor would put money down) and has ROI.

A broad ecosystem of successful companies, that drive adoption of the underlying technology and provide a business ROI.

What is the problem that customers will pay for?
Question: why would I use Sovrin vs a competitor technology.

OpenSSI – protocol.
A network of networks that uses that protocol. Anyone who uses it.
Working on that with Linux Foundation and IBM. Sovrin will have advantages than other ledgers.

Sovrin has advantages over BTCR (and privacy capabilities)

Credit Unions

- In control of your data

Mutual parallel authentication.

2. Notes from Ellie Stephens

Microsoft passport was a spectacular failure one of the biggest reasons is the that they tried to own it. Google doesn't do that, apple doesn't. So every time we want to solve the identity problem if they come through us, then they create a silo competitive option and we repeat the identity problem over and over.

Our idea when we built sovrin was to use DLT. Independent identity not self sovrin identity (hyperledger indy). Not all people can be self-sovereign (babies, eldery, disabled, machines). Hence independent identity. Hyperledger indy at the linux foundation 3 projects. Hyperledger Fabric (donated by IBM), Hyperlegder sawtooth (intel), Hyperledger Indy (evernym) IoT, voting, healthcare, pet identity - SSI applications everywhere. What are the very best opportunities of things that could be funded by investors

(Where R the) Karmic endpoints?

Tuesday Lunch
Convener: Heather Vescent
Notes-taker(s): Heather Vescent

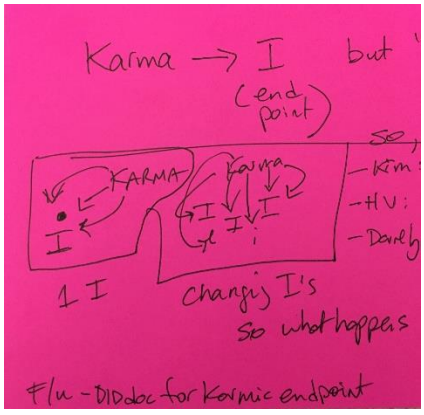
Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

We had an impromptu session following in the footsteps of my Buddhist Approach to Identity. Participants:
Heather V.
Don T
Margo
Will
Kim
Darryl
Rouven

In buddhism, there is no solid, non-changing I.
Can only experience Identity in time (like music)
What does the human/identity look like outside of time?
(What is the one story a filmmaker keeps making over and over? Kubrick's is, the story of a young man coming of age)

Where is the Karmic endpoint if no I exists?
What does Karma look like outside of time?

Karma --> I (endpoint)
But I, not static. It's always changing.



Kim: Karmic endpoints are in the DID Doc
HV: All your DIDs are in your agent/cloud/hub in the cloud. And there could be a new DID for each new I
Darryl: and those depend on what you DID. (lol)

But seriously, where are the Karmic endpoints?
Follow-up session on the DID Doc for Karmic endpoints....

What Does a Layered Identity Model Look Like? (Like OSI 7-Layer Model For Networking)

Tuesday 3A
Convener: Jacoby Thwaites
Notes-taker(s): Jacoby Thwaites

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

Jacoby has provided this link to notes + the slides presented at this session:
What does a Layered Identity Model Look Like?

User-Managed Access (UMA) – 101 Session

Tuesday 3B
Convener: Eve Maler, Kantara Initiative UMA Workgroup Chair
Notes-taker(s): Thomas Berry & Eve Maler

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

1. **Notes Received from Thomas Berry:**
   User-Managed Access (UMA) 101

   - OAuth enables constrained delegation of access to apps
     - Alice to Apps by way of authorization server and resource server (A-T-D) Authorization, Token, Directory
     - Benefits:
       - Flexible, clever API security framework
       - Alice can agree to app connections and also revoke them
   - OpenID Connect does modern-day federation
     - Benefits
       - Layers identity/authentication tech with delegation/authorization tech
       - Translates federated identity for mobile and the API economy
     - Federation user, relaying party, identity provider (standard UserInfo endpoint)

   - With other problems exist
     - To OAuth, UMA adds cross-party sharing
     - Alice (resource owner) needs to share with Bob (requesting party) [by way of client]
     - By way of Authorization server (A and T) and Resource server

   - Benefits
     - Secure delegation
     - Alice can be absent when Bob attempts access

    - Helpful error handling for client applications
    - Alice controls trust between a service that hosts her resources and a service that authorizes access to them

Authorization server :A T D R P I C

- Aggregation is not a solution: resource server exists in many Ns
    - A Authorization
    - T Token
    - D Discovery
    - R Resource integration
    - P Permission
    - I Token Introspection
    - C Claims Interaction
- Imagine what delegation means to an autonomous third-party

UMA Experience Opportunities
UX (consent):
Share Button (ahead of time)
Opt-In (At run time)
Approve (After the fact)
Monitor (Anytime)
Withdraw (Anytime) - revoke

Benefits for service providers: a summary

- True secure delegation; no password sharing
- Scale permission-ing through self-service
- API-first protection strategy
- Foster compliance through standards
-

Benefits for individuals

- Choice in sharing with other parties
- Convenient sharing/approval with no outside influence
- Centralized monitoring and management
- Control of who/what/how at a fine grain

Typical use cases

- Alice to Bob (person to person)
- Discovering/aggregating pension accounts and sharing access to financial advisors
- Connected car data and car sharing
- Enterprise to Alice (initial RO is an organization)
    - Enterprise API access management
    - Access delegation between employees
- Alice to Alice (person to self/app)
    - Proactive policy-based control of app connections

Profiled or referenced by:

- OpenID Foundation HEART Working Group (HEalth Relationship TRust)
- UK Department of Work and Pensions
- OpenMedReady Alliance

Forge Rock
Glue
ShareMedData
HIE of One/Trustee
IDENTOS
Pauldron
RedHat SSO (Keycloak)
WSO2

UMA in a nutshell

- developed at Kantara Initiative
    - V1 done in 2015
- Leverages existing open standards
    - OAuth and OpenID Connect and SAML (optional but popular)
- Specs contributed to IETF OAuth WG in Feb
- Profiled by multiple industry sectors
    - Financial, Healthcard
- UMA business model effort supports legal licensing for personal digital assets
    - Mother (guardian) manages sharing for child (data subject); child "ages in" to consent and starts to manage sharing herself
- Some 1:1 interop testing done; more soon?

Demonstration

- Patient Alice creates a policy to share with Dr. Erica; Alice selects her sharing preference and presses SHARE.
- Patient sharing is easy!
-

ForgeRock Identity Platform

- profile and privacy management dashboard — also access management module
- Rock 'N' Roll Supermarket demonstration
    - Sharing (shared resources)
    - Activity (account actions/history)

The marvelous spiral of delegated sharing, squared

1. UMA grant of OAuth enables Alice-to-Bob
2. UMA standardized an API for federated authorization at the AS to make it centralized
3. There are nicknames for enhanced and new tokens to keep them straight

RFC 6749

UMA extension grant adds

- party-to-party: resource owner authorizes protected-resource access to clients used by requesting parties
- asynchronous: resource owner interactions are async 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

Resource owner | Client + Requesting party
UX: SHARE MONITOR WITHDRAW OPT-IN APPROVE

UMA federated authorization adds

- 1-to-n: multiple RS's in different domains can use an AS in another domain
  - "Protection API" automates resource protection
  - Enables resource owner to monitor and control grant rules from one place
- Scope-grained control: Grants can increase/decrease by resource and scope
- Resources and scopes: RS registers resource details at the AS to manage their protection

docs.kantarainitiative.org/uma/wg/rec-oauth-uma-federated-authz-2.0.html

Promises BLT business-legal-technical

UMA grant details
swim-lanes slide

Client's first resource request is tokenless: this exists in WAM

- response includes a permission ticket to continue (allows AS discovery)
- Claims-based access control in the form of claims collection options
- Assessment and token issuance as guardrails
- RPTs upgraded, revocation, ...

The permission ticket: how you start building a bridge of trust

- Binds client, RS, and AS: Every entity may be loosely coupled; the whole flow needs to be bound
- Refreshed for security: The client can retry RPT requests after non-fatal...

Pushed claims scenario is the most common implementation; for wide-ish ecosystems

- AS is requesting party's IdP and the client is the RP
- RS's initial response to the client
- Client pushes its existing ID token to the token endpoint
- AS is in the primary audience for this token
- Somewhat resembles SSO or the OAuth assertion grant, where a token of expected type and contents is "turned on"

Really wide ecosystems

- (Details already seen)
- Claims interaction endpoint must have been declared in the discovery document to allow this flow
- The AS mediates gathering of claims from any source
- A key "metaclaim" to think about: consent to persist claims; kind of like a refresh token opportunity (persistent claims token [PCT])
- Resembles the authorization code grant, but can apply to non-unique identities and is repeatable and "buildable" (a model for cross party interaction)

Federated authorization

- RS registers resources: This is required for an AS to be "on the job"
- RS chooses permissions: the RS interprets the client's tokenless resource request and requests permissions from the AS
- RS can introspect the RPT: UMA enhances the token introspection response object

- RO controls AS-RS trust: the protection API is OAuth-protected

UMA features

- Registering a resources puts it under protection
- Deregistering removes it from protection
- While registered, configuration changes can be made

Resource and scope registration

- The RS is authoritative for what its resource boundaries are
  - It registers them as JSON-based descriptions
  - There is a resource...
- Scopes can be simple strings or URIs that point to description documents

Permission endpoint

- RS interprets the clients tokenless (or insufficient-token)
- RS ...

Relevance for privacy beyond "empowered flows"

- features relevant to privacy regulations
- Work on well along on an ...

(Most) legal relationships in the business model

********** ********** ********** **********

2. <u>Notes Received from Eve Maler:</u>

Here is the bullet list of topics:
• Overview
• UMA in action
• The technical big picture
• The UMA grant
• Federated authorization
• Authorization assessment
• Privacy and business-legal-technical implications

Direct link to slide deck:
https://kantarainitiative.org/confluence/download/attachments/17760302/2019-04-30%20IIW%20UMA%20101.pdf?api=v2

Relationship Lens

Tuesday 3C
Convener: Lisa LeVasseur
Notes-taker(s): Lisa LeVasseur

Tags for the session - technology discussed/ideas considered: #Me2B Relationships

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

1. There are Universal Rules of Engagement for how to treat each other when in relationship.
2. For most westerners, it's possible that relationships with purveyors/service providers outnumber other kinds of relationships in our lives.
3. Yet there is no category name for relationships with purveyors/service providers.
4. Naming these relationships is important to recognize that the Universal Rules of Engagement apply to purveyors/service providers.
5. Proposed name for these relationships: Me2B Relationships.
6. There are two tiers of relating when in relationship: (1) Relationship level (holistic) and (2) Transactional.

Discussion over: "Data as..." John P suggests Data as energy; The energy model cn be viewed as the frequency of intersection/interaction while in Me2B Relationship. The quality and caliber of the intersections reflects the quality of the Me2B Relationship. The better the relationship, the better the higher/better the energy. Slides here: https://www.slideshare.net/secret/mn5Z7cV92lAVqJ

Universal Resolver – What is it and Why it Matters?

Tuesday 3G
Convener: Nader Helmy
Notes-taker(s): Nader Helmy

Tags for the session - technology discussed/ideas considered:

DIDs, Universal Resolver, DIF, decentralized identity, software tools, open source

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

The DID spec provides a general framework for user control of a cryptographic identifier https://w3c-ccg.github.io/did-spec

Since DID is a generic framework, the way that any given DID works is defined by the DID method. DID methods are an implementation of the DID spec which identifies a particular schema for CRUD operations on the DID

C - create
R - resolve
U - update
D - deactivate

DIDs are written with the syntax did:<method-name>:<identifier>

Since there are so many DID methods, there is motivation for a common library/service that allows usage of a DID regardless of method. Every DID method is implemented in a unique way, meaning it has its own libraries, dependencies, and software stacks. In addition, each method specifies a different way of speaking to its respective blockchain, ledger, or distributed filesystem.

The Universal Resolver solves a part of this issue by giving a common interface that allows any DID to be resolved. It is a completely open-source project hosted by the Decentralized Identity Foundaton (https://identity.foundation/) and is a collaboration from many developers and companies across the world

In broad terms, Universal Resolver is a service which provides a common interface for all DID Resolution, regardless of method.
It is implemented as a set of Docker containers running side by side on a local machine. The basic architecture is 1) a user makes an HTTP call to the UR with a specific DID, 2) the UR parses the DID and determines which method it belongs to, then 3) the UR calls the appropriate method-specific driver. Every driver is an implementation of the Resolver for *one or more DID methods*.

The Universal Resolver SHOULD BE DEPLOYED BY THE DEVELOPERS USING IT
It is imperative to run a "local" version of the resolver in order to trust its results. Since the Resolver performs the verification of a DID Document and ensures the information is accurate, anyone who wishes to use the Universal Resolver should do so independently. This service runs locally and can serve your applications and demos with current and valid info about DIDs

Two separate codebases:

- Universal Resolver - https://github.com/decentralized-identity/universal-resolver
  You can think of this as the backend service. It includes the Docker containers and the HTTP interface. You can resolve DIDs from the command line using CURL

- Universal Resolver Frontend - https://github.com/decentralized-identity/universal-resolver-frontend
  This provides the web interface with clickable buttons!

Public instance (used for demo purposes only): https://uniresolver.io/

3 Questions that everyone using UR should answer:

1. How is it deployed (UR and drivers)?
   a. E.g. local or public instance, running as a hosted service, etc.
2. How do drivers talk to their target system (blockchain, ipfs, peer, etc.)?
. Running a full node, using a software library/API, etc

3. If the driver uses an API, how is the API implemented?
. Is the API speaking a particular node, a pool of nodes, a cache, etc?

Notes:

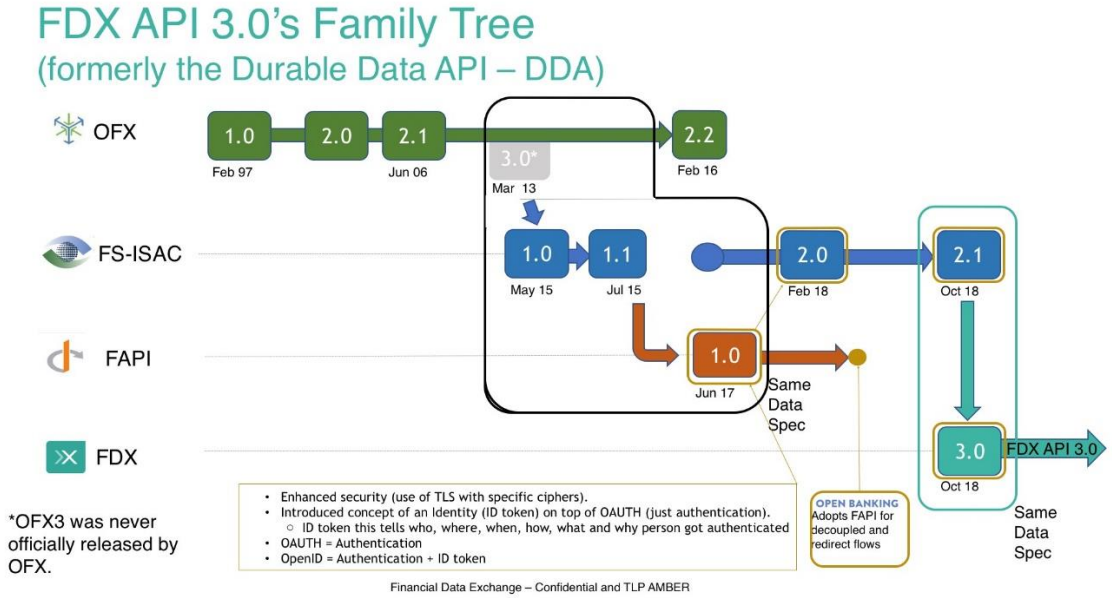
- Drivers are contributed in the form of a Pull Request to the DIF Github repo found here https://github.com/decentralized-identity/universal-resolver
- Comprehensive list of all DID methods - DID method registry https://w3c-ccg.github.io/did-method-registry/#the-registry
- It is a common misconception that the UR is a centralized service. While uniresolver.io is a public instance of the codebase, it is only used for demo purposes. The Resolver is meant to be run locally by the person verifying the results.

Open Banking: Variable Scopes, Multi-Scope Tokens

Tuesday 3H
Convener: Nick Thomas & Don Thibeau
Notes-taker(s): Nick Thomas

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

Nick Thomas (Finicity Co-founder, Founding Board Member @ Financial Data Exchange (FDX)) and Don Thibeau (Chair, Open ID Foundation) shared the history of Consumer-Permissioned Data standards leading to the FDX API v3 and the complimentary OpenID FAPI profile for Authentication and Authorization.



We shared the momentum behind FDX with 52 member organizations, including the largest banks in North America, the major aggregators, and major permissions parties. https://financialdataexchange.org/pages/members

Discussed ideas around how to solve for the dynamic issuance of multiple time-bound tokens without requiring the consumer to login each time a new scope was requested.

Key Management/Usability For Lay People

Tuesday 3I
Convener: Raghav Chawla
Notes-taker(s): Jackson Callaway

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

Key Management and Usability for Lay People

Normal folks don't even know about public-private key cryptography, let alone how it works, or if they're doing it right.

Physical keys versus software keys

Phone becoming the new key. Secure enclaves etc

Centralization happens because of usability

Consensys
- Diddery
- SeedQuest
  - key recovery, mnemonic phrases, series of video game actions as recovery string
  - have prototypes out, got some reactions
  - Procedural, shape-based memory instead of memorizing strings

Anonymy Labs
- Consumer mobile app
- Create pseudo profiles, with functioning phone numbers and addresses
- Lots of issues with key recovery

Blockstack
- 12 word seed, and password that encrypts the seed
- Also an email with a recovery link that requires password

Argens
- Social key recovery

URBit
- 64 bit seed. Just a few words, Is it memorable?
- Azimuth identity system with role-based access controls

Personal Information Value Equation

Tuesday 3J
Convener: Michael Becker
Notes-taker(s): Michael Becker

Tags for the session - technology discussed/ideas considered:
Personal Information Value Exchange Formula, regulations, Industry Alignmen

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

In the session we discussed a theoretical framework for calculating the value of personal data.

We considered:

- Personal Data Constituency Matrix
- Overlapping values
- Personal Information Exchange Value Matrix
- Three Body Problem of Regulation: Open Data, Sovereignty & Social Engineering (we need to look at this work as Ands not Ors)
- Constituency Framework: Individual, Public, Private institutions

We discussed how the above frameworks (as illustrated below) will help drive self-sovereignty, drive private and public innovation, policy, industry best practices, and regulations.

Links to material shared in session:

Personal Information Value Exchange Equation, https://identitypraxis.com/wp-content/uploads/2019/05/Personal-Informtiaon-Value-Equation.png

Personal Information Constituency Matrix, https://identitypraxis.com/wp-content/uploads/2019/05/Personal-Information-Constituency-Matrix.png

Personal Information Regulatory Three Body Problem, https://identitypraxis.com/wp-content/uploads/2019/05/Personal-Information-Regulatory-Three-Body-Problem.png

Personal Information Value Exchange Matrix, https://identitypraxis.com/wp-content/uploads/2019/05/Personal-Information-Value-Exchange-Matrix-1.png

Rubrics for Decentralized Identifiers

Tuesday 3M
Convener: Joe Andrieu
Notes-taker(s): Daniel Hardman

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

Permissioned: governed/operation vs. use/creation
Open source: multiple independent implementations
Open standard
Does the individual create and control?
Can the individual choose how keys are managed?
Does the issuer/controller have a fiduciary responsibility to DID Controller?
Does it support social recovery?
What does a single DID cost? TCO
Is resolution observable?
Are stealth DIDs supported?
Is deactivation publicly documented?
After control is lost can other people deactivate?
Possible confusion between implementations and DID methods
Does it support HD Keys?
Are transactions publicly cryptographically verifiable?
Are DIDs permanent (unremovable--still able to be deactivated but all traces can never vanish)?
Can you get the latest version and older versions? Provable order of versions?
Is the method published?
Is that method independently implementable?
did:web and the .onion TLD (truly decentralized) RFC 6761 and 7686
Is theere a centralized database?
Is its blockchain byzantine fault tolerant?
Does a single party control a majority of the source of truth? (Under what conditions can the DID controller lose capability?)
If you give control away, can you get it back?

Government IS the Solution to ID – Change My Mind!

Tuesday 4C
Convener: Michael J. Rodriguez, Mitre, mjrodriguez@mitre.org
Notes-taker(s): Scott Mace

Tags for the session - technology discussed/ideas considered:
Government credentials, public vs. private

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

Mike from Mitre. Government is the solution to identity. Change my mind.
Work with the identity access section of the air force
Trying to move to mobile and off of identity access card.
Government doesn't like any of the solutions available.

Instead of the government have vendors provide ID for us, why doesn't government just start providing our digital identity? We all get birth certificates. We get drivers licenses and passports. A national PKI. A base identification you could leverage for any org or service, banks, schools, etc.

When you die, the government finds out about it. Maybe at that point they can revoke your identity. It makes sense government should manage it. They're already in this space whether you like it or not.

Jack: I've been working in the government ID space for many non-U.S. governments. It's a pretty good ID provider. They know a lot about us. The ID proof they can issue about us and the legal framework. They do digital ID. Your passport is a digital ID. It's interoperable. Everybody can read it and use it as a formal proof of who you are. The question is how do we go one step forward and use it in every day life. Could be for identity access management, registering on a web site, opening a bank account.

Which countries in particular?

Quite a lot. India, Hong Kong, Macau, Philippines, Thailand, France, Spain, Germany, Italy. Considered Fido & OpenID, but no clear trend.

Q: All 200 governments working together?

Mike: Starting from a state level. Texas PKI, everybody born in Texas gets a public & private pair. Share trust among the CAs.

Q: Governments do claims, component parts of identity. Should be a way of claiming my digital passport. That way, every government can give you a claim, put the onus on the verifiers, not on the givers.

Mike: The infrastructure is there.

Q: Need some form of standardized verification – i.e. biometric.
Q: Government is both an issuer and a verifier.
Q: One criticism is government doing it is expensive.

Q: One criticism: government solutions can't keep up with industry solutions. Government doesn't always know where to start.
Q: The only thing government has to do is choose one of the methods to distribute claims. If they get it wrong, they can switch that out.
Q: DHS facial recognition to open an airline gate, within 5 seconds. Never provided a prior picture to JetBlue. That genie is out of the bottle, using biometrics.
Q: Identity should be a relationship to multiple sources.
Q: Issue of asylum seekers.

Mike: Soldiers scanning irises in Afghanistan.

Kaliya: They already have that. You're mixing domains up. I wrote my Master's thesis, the domains of identity. Government identity is foundational. It becomes the thing a whole set of other institutions acquire. Such as opening a bank account. What's critical, I just spent 2 months in India, when you use the national ID, it phones home to the Indian government and tells you everywhere you use it. Very different than SSI architecture where they have no business knowing where you use it. A difference between an authentication service and an identity provider. Identity is different than our ongoing use of it.

Q: Who is to say 100 years from now we in the U.S. won't be the refugees?

How Can Trusted Identities Be Accepted By Governments and Industries?

Tuesday 4D
Convener: Scott Perry
Notes-taker(s): Thomas Berry

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

- Collecting identities to add trust is too much work
- Australia: trusted digital identity framework (everything must be registered/imported)
- What would it take for a country to accept fingerprints obtained from another (identity proofing)
- Credential is issued for a service and used for someone nefarious; who is liable?
- Credit unions are getting exciting self-sovereign credentials to its customers; works within a single credit union (issuer and relying party); uses credential with another institution (bank) what is going to happen?
- The issuer can't be responsible for how the extended identity has been used.
- The elements of consent has to be trusted (i.e., donor label on driver's license)
- What is needed to trust the identification
    - Issuer of identity
    - Who is the auditor of the issuer
- what does the relying party have to care about the issuer
    - The relying party only cares about making money; more money, more risk (accepted)
- User experience is the biggest driver; more cases of use is a driver for acceptance
- Business: identity proofing shop, issue digital credential that proves identification
    - Issue: acceptance (government, medical, etc.)
    - Australia: MyGov and Medical; not interchangeable

Self-Issued OpenID Connect (SIOP) DID Auth Flavor

Tuesday 4F
Convener: Oliver Terbu
Notes-taker(s): Oliver Terbu

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

The session was organized to move forward with the Self-Issued OpenID Connect Provider (SIOP) Profile for DID Auth and clarify a few questions. We discussed the basic SIOP flow and that it would be a good fit for DID Auth for web applications as DID Auth has two major tasks to solve:

- Proof of possession of a DID
- Exchange DID + other info that allows two parties to communicate with their service endpoints or in general with each other
- Focus on Authentication rather than Authorization

The following items were discussed in particular:

- SIOP mandates specific crypto algorithm, which is RSA and ECC P-256. The conclusion was it should be fine if the SIOP responds with different algorithms if the DID Auth profile is used.

- Although SIOP is not a mandatory feature of the OIDC spec and therefore has not as many implementations as the Authorization code flow, it uses the same message format and shares request and response messages. For that reason, OIDC clients won't have an issue with adding this feature.

- There was a debate whether or not an RP has to implement both flows, plain OIDC, DID Auth enabled. The conclusion was that this is not needed and we anticipate clients that have DID Auth support opting in for the DID Auth profile only. In general that discussion triggered questions on what does it mean to RPs to integrate DID Auth which was then topic of another session on the next day.

- Similar to Identity Wallet providers. They can opt in for implementing the DID Auth based approach only, but to comply with the plain OIDC spec, they would need to be backward compatible. An RP that uses DID Auth will likely also use the service endpoints to interact with the user.

Identity @ Hyperledger: Indy, Ursa, Aries, Idemix & FabrCA

Tuesday 4H
Convener: Nathan George, Sovrin CTO
Notes-taker(s): Trent Larson

Tags for the session - technology discussed/ideas considered: Sovrin, Hyperledger, VerifiableClaims

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

Sovrin code is hosted at Hyperledger as Indy

Topics
- Identity Working Group
- Indy
- Ursa
- Aries project proposal
- blockchains & identity

Built to do verifiable data exchange between issuer & holder & verifier (who trusts issuer)
Indy: the original app w/ "blockchain" Plenum ledger
Ursa is a crypto library (in Rust, interfaces to languages & blockchains)

Blockchain requires shared, single store of data (attributes = balance)
Identifiers allow ownership of data separated from the specific keys used

Decouple the attributes from the data & only maintain them
Now we can store the IDs on the chain.
Agents interact on behalf of people, and that's an intentional legal term to represent the holder.
Blockchain is only to verify that the identifier is still valid.

New project proposal: Aries to do identity interaction and key management
Identity interactions on different chains
"public DIDs" on public networks vs "peer DIDs" on private networks
Credentials can be implemented by multiple keys
Private permissioned chains require knowledge of genesis block, then people can be added at will.
Now credentials can be used between individuals without
Revocation Registry tells what credentials are active, and they're moving to SNARKs and Merkle Trees
Credentials can be wrapped as
Sovrin is more about verifying claims than identity

For sharing credentials:
- Need a schema (data model, structure, vocab, json-ld) which are stored on an immutable blockchain
- mappings object (to define order) & encoding object (to serialize goals) allow a flattened version of the credential
- "json-ld data graphs" allow richer data representation

- "range proofs" allows proofs of a subset of the graph of data
- Need a credential definition
    - Provides: correctness proof, DID & public DID, keys, pointer to revocation registry

The only attributes on the Sovrin blockchain are:
- Trustees have their names on the network
- Stewards have their organization names on the network

Interesting demos: The Org Book - StreetCred ID - Spark NZ - ID Ramp

There Are No Scopes On Using Scopes & Claims the OIDC Way

Tuesday 4J
Convener: Mark Dobrinic
Notes-taker(s): Mark Dobrinic

Tags for the session - technology discussed/ideas considered: OAuth, Scopes, Claims

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

Inspired by the fact that the OAuth specification gives us the concept of "scope" but it is intentionally left unspecified, so everybody can use it as it fits best.

This was the original intent, the time as come where specific problems are trying to find a structured way of using scope to bind authorization data to tokens.

A short presentation introduces the concepts of
- scope as scope of access
- claims as statements that are asserted by an authority
- attributes that can be turned into a claim by some authority
- scope to represent a collection of claims, as standardized by OpenId Connect

OpenId Connect defines a number of scopes that expand to claims, i.e. requesting that particular scope equals asking for a set of claims.

Our take has taken this concept into a generic thing: allow an Authorization
Server to define its own scopes, which each can expand to one or more claims.

Other current usages of scope include so called Dynamic Scopes (or Prefix Scopes) that try to bind an action to a transaction id, to be authorized by an end-user.

Discussion resulted in the notion that the use of scope in requesting tokens should be about carrying the intent that a client has for the requested token.
Including many claims in tokens should be carefully considered, because the authorization server must not be overloaded in the knowledge it has about clients and resource servers. The name "authorization server"

could even be misleading, in the sense that it is the resource server that ultimately authorizes a request or not (based on the presented token).

It is mentioned that using tokens that expand into claims in a token would not replace the current use of scope with OAuth. Instead, it is an extension of the use of scopes, that makes use of existing patterns (in particular: the "scope" request parameter from OAuth and the "claims" request parameter from OpenId Connect)
Some discussion is about the proposed "structured_scope" approach from the OAuth Working Group, which tries to solve the transaction authorization case that is currently tried to be solved by different parties. Dynamic Scopes are solving that for PSD2, structured scopes could solve it in a different way, but the scope-as-claims pattern could also solve this by using the expected "value" part of the "claims" request parameter.

The session resulted in the conclusion that the discussion should be continued with other approaches.

WebAuthN Together with DIDs

Tuesday 4M
Convener: Christian Lundkvist
Notes-taker(s): Christian Lundkvist

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

We discussed a basic overview of the webauthn protocol and also a basic overview of DIDs, DID documents and the Universal Resolver.

We noted that the authors of the Webauthn protocol has decided that account recovery is out of scope. This means that the protocol does not handle the case where I lost my authenticator device and need to associate a new authenticator device with my account at a relying party.

We discussed using a DID-based authentication protocol for the account recovery. There were questions about if the webauthn protocol is flexible enough to support this. It turns out that the webauthn data payload has a field “user_id” or similar that can be used for a string, and here we could put the users DID. Thus it seems possible.

Since recovery is out of scope for the webauthn protocol it means that there is no need for a website implementing an authentication protocol to have to choose between webauthn or DID Auth. It would also be the case that we can avoid a political fight where a DID-based authn protocol is attempting to replace webauthn. Any relying party can implement a webauthn protocol and still experiment with versions of DID Auth in their account recovery, unrelated to the core protocol.

We discussed privacy concerns: if you supply the same DID to the “user_id” field for all the websites you sign up to then you can be immediately correlated between sites and you would then lose the benefit that the webauthn protocol will generate a new public key for each website. This could be mitigated by using a Sovrin-style pairwise DID or otherwise using different DIDs for different classes of websites.

Meta Platforms: Cooperative Network of Network Effects

Tuesday 5A
Convener: Sam Smith
Notes-taker(s): Sam Smith

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

A meta-platform is a platform that enables and fosters participant controlled value transfer across and among other platforms.

The network effect resulting from a platform (sub-network) joining a meta-platform (super-network) is that the platform's (sub-network's) value is increased by the ratio of meta-platform (super-network) to platform (sub-network) size.

Provided scaling law for cooperative network of networks effects.

https://medium.com/selfrule/meta-platforms-and-cooperative-network-of-networks-effects-6e61eb15c586

Decentralized control has the potential to cause a leveling effect that more fairly distributes value to users, limits exploitation, removes barriers to entry, and increases opportunities for disruptive innovation and value creation.

A concern comes from the fact that other leveling technologies, such as communication networks, first started as decentralized but then become more centralized over time with the associated value capture eventually becoming concentrated into a few very large business entities with higher rates of value extraction.

One can argue that the internet which started as a great leveler due to decentralized networking has now resulted in most of its value being concentrated in a handful of companies.

Once centralization occurs innovation and value creation decrease and value extraction increases to the detriment of the average user.

Although decentralization can reduce triangulation and transfer costs, its primary potential advantage is in reducing trust costs!

Direct link to additional resources + white paper:
https://github.com/SmithSamuelM/Papers/blob/master/presentations/MetaPlatforms_IIW_20190430_5A.pdf

Intro to Self-Sovereign Identity (101 Session)

Tuesday 5B
Convener: Kim Duffy-Hamilton & Heather Vescent
Notes-taker(s): Heather Vescent

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

An introduction to Self Sovereign identity, staring the BTCR DID method.
Link to presentation slides:
https://www.slideshare.net/heathervescent/introduction-to-self-sovereign-identity/

5 Radical Ways to Keep Vendors Accountable for Your Data!!
Kantara Consent Receipt: Personal Data Receipt

Tuesday 5C
Convener: Andrew Hughes, contributor, Kantara Initiative, AndrewHughes3000@gmail.com
Notes-taker(s): Scott Mace

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

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

@idimandrew Personal data receipt a.k.a. consent receipt

What is missing?
No one is going to read the terms of service, but what if there is a problem.

What's missing is a record the person can keep independent of the records of the vendor with details that can hold the vendor accountable. In sales, it's called a receipt. Date & time stamps, location, maybe ID of you through credit card data. And the price. Why are those thing useful. Returns. Insurance. Tax deductions.

You buy something and also they ask for your mother's maiden name for some reason that seems reasonable. What if they say instead, allow us to use your precise location to find a store near you.

In Kantara, consent receipt spec 1.1 published in February 2018. Downloadable. Just a data structure. At the time it was developed, privacy people involved saw GDPR coming down. We had an estimated target date for that, 2018. Prevailing view was consent would be huge. Puts the person in charge. The companies have to do what you say. Made it unusable for any enterprise anywhere. You have to provably say this is all the stuff. The advertising industry, it was required. May 25, 2018 arrived, and nobody does consent. It's not a good idea if you're a business to commit yourself to that level of responsiveness to your customers.

Q: So they took a reactive approach?

Those chose a different basis for processing data. Consent was one. Contract. Legitimate interest of the processor. Did what their lawyers told them to. If they had a contractual arrangement anyway, they continued doing that. Consent is a bad word when talking to everyone other than privacy advocates because nobody knows what you're talking about. A word in English that has no bearing at all to the word in technology. Do you call the OAuth screen the consent screen? No. It's the authorization screen. When people say consent, they mean permission and authorization.

Service provider develops a service, a person discovers the service, wants to use it, service provider offers terms, person considers terms, accept?, could be no. If yes, person and service provider jointly establish an agreement. Service provider performs record keeping. And person gets a sales receipt. The agreement also triggers payment & "consideration" by the service provider (the product or service).

Proposing the vendor optionally offers a receipt, and puts it in a storage place of the person's choosing. Will demo at European identity conference in two weeks. Nickname is Smoke & Mirrors. The Kantara Privacy Control Panel. A control panel for your privacy. Fictional products. Intended to show interoperability of receipts. A stack of receipts. "Hey Alexa, analyze my receipts." Tells you company is being fined for bad data practices. Might want to revoke that permission to provide data.

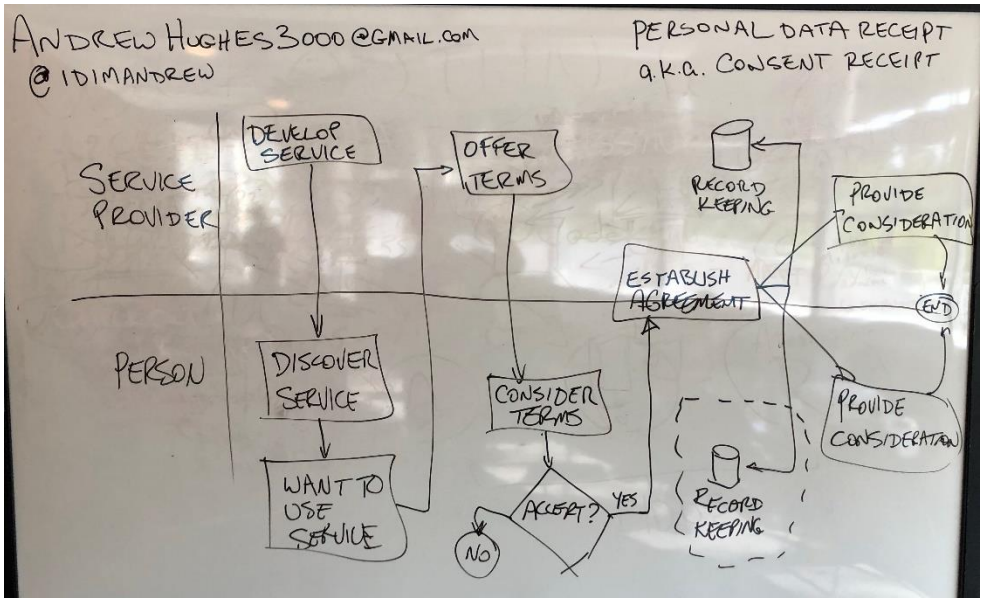
Could be applied to the IAB Transparency Consent Framework.

I dare you to think of any use case that does not fit this pattern.

Jim Pasquale: What if you neither say yes nor no, but counter-offer.

Wendell: The terms of the hot dogs are fairly clear. When you go buy other things, they come with a bundle of rights. You don't have the right to rip off that design. If I "buy" a song, you're not buying the song but a single-person performance right. That's where the terms get horrendous.

Andrew: We're building version 2. Kantara Initiative have a liaison with ISO Subcommittee 27 working group 5 concerned with identity technology & standards. Because of our liason, we have an opportunity to contribute the first draft of what we hope will define online consent records and receipts.



My Data HUB (101: The Declaration)

Tuesday 5E
Convener: John Wunderlich
Notes-taker(s): John Wunderlich

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

This session was a review of the contents of the MyData Declaration. URL/link provided by John Wunderlich: https://mydata.org/declaration/

OAuth Clients Create Token

Tuesday 5F
Convener: Sascha Preibisch
Notes-taker(s): Sascha Preibisch

Tags for the session - technology discussed/ideas considered:
oauth, jwt, jwks, opened connect, authorization, grant

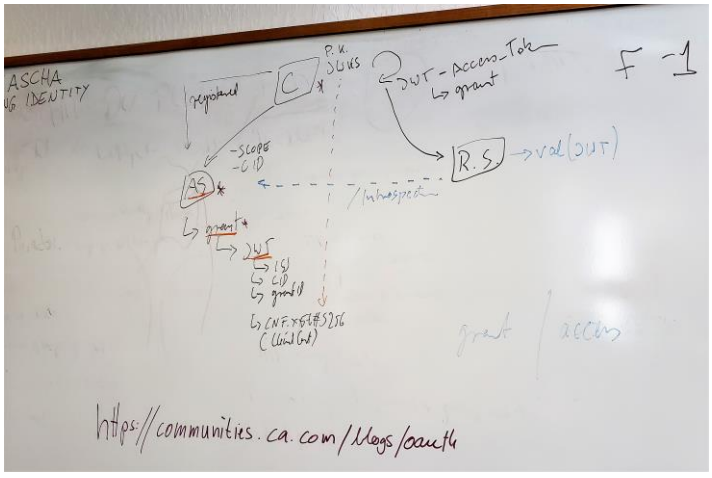
Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

We discussed my idea of oauth clients that mint oauth token based on a grant that was received by an authorization server earlier. This divides a grant from the artifact that enables access to a resource. A stolen grant is useless to other clients, token are minted just in time which makes them hard to leak or be stolen.

It turns out that there are good use cases for that. It also turns out my idea is very close to the current work of the dpop draft (demonstration of proof-of-possession). One of the authors of that draft, who joined my session, and I will see if we can join the two efforts.

Links: dpop: https://tools.ietf.org/html/draft-fett-oauth-dpop-01
blog post: https://communities.ca.com/blogs/oauth/2018/11/06/oauth-20-serverless-token-issuance

The screenshot of the whiteboard (5_F.jpg) displays parts of our discussion



The Case for An OIDC Ephemeral ID

Tuesday 5G
Convener: Davide Vaghetti
Notes-taker(s): Davide Vaghetti

Tags for the session - technology discussed/ideas considered: OIDC, transientID, identifiers

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

A brief document has been prepared to introduce the discussion and it now includes some of the topics emerged: https://gist.github.com/daserzw/813023b4e1c04d09beb732ef00d7c9e9

Next steps: refines the document, wait for/solicit some feedback, if deemed useful and feasible start to turn it into a proper OIDC specification.

Machine Identity: IOT – Security, Trust, Interop

Tuesday 5H
Convener: Mrinal Wadhwa
Notes-taker(s): Thomas Berry & Mrinal Wadhwa

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

1. **Notes received from Thomas Berry:**

    1. Relationships
    2. Chore Automation
    3. Responsibility/Liability (Relationship)
    4. Linkability/revocation (Relationship)

    Identify the "person"
    identify the "location"
    Device "trustworthiness"

    - The same data gets "housed" in many different systems

    DID provides an opportunity to break away from identity silos
    - Scalability
    - Security
    - Privacy
    - Trust
    - Reliability

Building blocks

- AuthN
- Linked Data Proofs
- AuthZ/Object capabilities
- DID documents
- Linked Data Signatures
- Verifiable claims/credentials

Decentralized IDentities

- schema, method, method specific unique string

Registering Device (DID flows)

- generated by the device and optionally registered
- The device can have 100% control of the identification "forever"

Globally resolvable

- Device identity (did:ockam:...)
- People identity (did:sov:...)

If you have a DID string, you can resolve it to it's DID Document via its method. We did not have this property of global uniqueness/resolvability across systems with older ID schemes. This breaks silos.

DID Documents

- DID documents are linked data documents that describe the DID, they contain the public keys of the DID, authentication methods, services, etc

DID identities better for key management for machines/devices

Introducing a new device to the home—both device and home can utilize discovery endpoints to register its identity within the home

Semantic & linked data

The progress made by the open web community around Linked Data can be applied to IoT; This brings semantic meaning and relationships to IoT data...

- instead of describing temperature as a key of my choosing "temperature", "temp", or "T", let's describe it with well defined semantics {..."http://IoT schema.org/", "iot:temperature": "30"} which is self describing data that defers the description of the data format to a authoritative source (verifiable claims)

DID and blockchain can provide a reliable framework for reliable and secure device management and integration.

managed custody (parents-to-children) is an interesting solution to machine/device ownership. DID can reference an owner document including properties that propagate to the child DID

- ERights has attempted to define the notion of object capabilities (roles/ownership)

2. Notes received from Mrinal Wadhwa:

Here are the links to the slides and a video recording of the slides that were discussed in the session
Video: https://www.youtube.com/watch?v=TJQ8Pt4lfuA
Slides: https://www.slideshare.net/SSIMeetup/machine-identity-dids-and-verifiable-credentials-for-a-secure-trustworthy-and-interoperable-iot-mrinal-wadhwa

Deep Dive Demo: Connect Me + ONFDO Credential

Tuesday 5I
Convener: Michela Casaldi & Vladimir Vujovic
Notes-taker(s): Vladimir Vujovic

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

https://docs.google.com/presentation/d/1dEUUSLCnLPO7WBKPhKzU78eFak1_CxQ5_sDBUq6tIcU/edit?usp=sharing

On the session we explained how we have integrated Connect.Me digital wallet app with Onfido Issuer Service, how to get Onfido ID credential, issued by Onfido on the Sovrin MainNet, how that credential can be used to open an account with financial services companies who require ID verification upon account creation. And we demonstrated the whole flow on the session

Digital Natives - How do we get them to care about digital identity?

Tuesday 5J
Convener: Robert Phares
Notes-taker(s): Robert Phares

Tags for the session - technology discussed/ideas considered
Digital Natives, Identity Theft, Social Networks, Identity Security, Personal Data Protection Regimen, IdP

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

"I don't care what Facebook knows about me."
– the comment at the Day 1 IIW breakfast that sparked the idea for this discussion.

Working definition of a Digital Native: Someone who was raised in a digital, media-saturated world.

Discussion: digital natives demonstrate an inherent trust of "The Internet" and social media.
Statistically speaking, this puts them at greater risk of Account Takeover attacks, Identity Theft, and fraud.

The data protections of GDPR, CCPA, et al. represent a welcome change to corporate responsibility but are late to the game in protecting consumer and individual identity.

Personal, practical use of Social Media sites:

- Any time you click "like" on Instagram, Facebook, etc. you're providing valuable, harvestable data as to your personal preferences. Be aware of this fact.
- Instead, consider sending a text directly to your friend or the content creator.

Link to slides: https://drive.google.com/file/d/1U-rncQDp0rTBKVwDsKvxTZTPJU2L1Bb6/view?usp=sharing

Wyoming Laws & Regulations

Tuesday 5L
Convener: Christopher Allen
Notes-taker(s): Paul Dietrich

Tags for the session - technology discussed/ideas considered:
Wyoming, state laws, federal law, laws, legal, regulation, legislative, blockchain, privacy, identity

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

recap on Wyoming identity history

- passed 5 major bills in 2018
- HP101 — changes the way the corporation works.
- LLCs which were invented in Wyoming
- stockholders no longer have to be represented by a name.
- All they need is a public key.\
- All you need to give notice to shareholders is a public network address (DiD like)

Wyoming also defied the rules for a token offering. Still not legal as federal laws trump state laws.

2019 —
1000s of new companies domiciled in Wyoming.

legalized some legal rules for corporation to appear on blockchain.
corporate governance can be done with blockchain.
this is still managed by a registered agent

Wyoming rule that there is a 2 year perfection on bitcoin,

Chris tried to get orgbook like tools for companies within Wyoming. That is, something like orgbook for corporations. That didn't happen for historical reasons.

Determined that in 2020 they could establish limited state bank
Democratic chair rom Wyoming asked Chris to vote on what could we do about identity and privacy that might fit in and align with values and mission in state of Wyoming.

Ideas to propose:
KYC — propose that Wyoming have a band rely on a 3rd party for KYC with indemnification within limits. Unfortunately, federal law trumps this due to FDIC since that requires everyone do their own KYC.

Make it that under civil court, the specific performance of turning over keys should be prohibited. Instead the party
should transfer the bitcoin (or other digital asset) directly. The reason is that they key may also control other things like DID, other wallets, FIDO etc. The private key is a digital asset that is not meant to be shared to traded.

Biometric laws — Illinois has a requirement that all biometric information be collected only with there permissions of the users. (e.g. using a photo to do identification). etc. Considered this for Wyoming, it might be too late.

Should Wyoming do something with GDPR or California privacy. May be too soon and see if they get better.

If they do, its important to consider the penalties in CA and GDPR.

Discussion of specifying requirements for open source for children etc.
Require that for state procurement that everything has to be vendor neutral, standards based.
This is not Chris's portion of the recommendations.

An argument around rights not property. Property is extrinsic and alienable, but personal information is not. What can be said to form a libertarian argument around protecting data.

Idea to have Wyoming accept state tax payment in bitcoin. This was explored the first year but there were complications with the way the state keeps its bank account which fell under federal rule.

An idea forbidding sale of data but only allow licensing of data. The discussion also lead to establishing self-determination. How to extend the right to control their physical person to the right to control their digital person (data).

Further conversations at christophera@lifewithalacrity.com

Ask Me Anything with Heather: Sovrin Foundation

Tuesday 5M
Convener: Heather Dahl, Executive Director/CEO Sovrin Foundation
Notes-taker(s): Heather Dahl

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

Our session focused on how to become more involved with the Sovrin Foundation.

I've compiled 9 Ways to Become Involved with Sovrin.

1. Sign up for our monthly newsletter. Scroll all the way down on Sovrin.org home page to do so. We publish monthly. It's your best way to get all of Sovrin's news and announcements in one place.

2. Join the Sovrin Alliance.

3. Become a Sovrin Steward.

4. Begin participating in one of our Working Groups. (Send note info@sovrin.org to sign up)
    - Governance Framework Working Group
    - Global Policy Working Group
    - Guardianship Taskforce

5. Join Sovrin's Rocket Chat chat.sovrin.org

6. Take a look at our Developer Getting Started Page and begin participating in the Indy Working Group & Chat room calls.

7. Become a contributor to the Sovrin Blog.

8. Follow @SovrinID on Twitter.

9. Join Sovrin Official on Telegram.

Digital Identity for Refugees & Disenfranchised Populations: The "Invisibles" and Standards for Sovereign Identity

Tuesday (Announced during Closing Circle)
Announced by: Drummond Reed for Jeffrey Aresty
Notes-taker(s): Jeff Aresty

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

Link to paper: http://bit.ly/digital-identity-refugees It will be published in June

A Note from Jeff Aresty with some background on how the paper was developed:

IBO will be issuing the attached white paper http://bit.ly/digital-identity-refugees, **Digital Identity for Refugees and Disenfranchised Populations: The "Invisibles" and Standards for Sovereign Identity** in conjunction with the presentation we are making at the World Justice Forum. The "Invisibles" is what led you (Joyce), Timothy and Phil to individually connect me with Manny, who traveled with me to Bangladesh in December to help me begin the pilot. After we returned, Manny invited Tey to join the project, and, both are presenters here at the Forum this week, and, co-authors of the White paper. Manny, Tey and Kristina are planning the follow up trip to Bangladesh for later this month.

The key distinction our approach has with other standards efforts is that we start from the premise that to develop appropriate governing standards for SSI, we need to start from the premise that the state needs to let individuals and private organizations drive the effort. Our pilot project is based on this approach. One of our presenters, Scott Cooper, will be heading over to **ISO** in Geneva right after the conference, for follow up meetings to work with IBO on our standards approach, from the ground up. We definitely want to coordinate our efforts with IIW and IEEE.

To make new identities meaningful to refugees and other disenfranchised populations, **IBO** used our PeaceTones initiative to find musicians from these communities who would work with us to create an album, and, in the process, create intellectual property they would own. Last year, one of our supporters, a human rights lawyer and activist, David Levy, (https://www.linkedin.com/in/david-levy-4a080498) worked with PeaceTones to take our efforts to the next level. He traveled to several countries and refugee camps to compile an album with video called World United in Song. The album recently launched. https://peacetones.org/projects/world-united-song/ **IBO** then partnered with Ethan Baer, the founder of edm.com (https://www.linkedin.com/in/ethan-baer-b20b0633) whose company has offered their services to PeaceTones help us manage the contracts and distribution for the 24 artists who are on the album. So each of the World United in Song musicians has both been paid for their work and digitally signed a contract with PeaceTones. We are completing a licensing 'synch' agreement this week with http://heavyhittersmusic.com/ to monetize the album. The musicians will be able to access their earnings with their new digital identity. That's how the Invisibles and WUIS link together.

The first video for the album is available here (with 10 more to be released this year): https://www.youtube.com/watch?v=sHrAf-ArjIo

As well, the album is streaming on all platforms, here's the Spotify link if anyone is interested: https://open.spotify.com/album/5TZlMnvnY7JtbCo60WgQzs?si=EIrplBhvReOtJxrcu8uFvw

Wednesday May 1

Women's Breakfast

Karyl Fowler @TheKaryl
The coolest, smartest room I've ever been in. Meet the women of #IIW Proud as hell to be part of this group & to have the opportunity to learn from/work together to give users the identity

ownership and privacy we all deserve.

A Process for Discovering Truth: Can Credential Chains (or Other ID Tech) Help Create Authentic Voices? Learning from Historical Research Practices of Museums & Archives

Wednesday 6A
Convener: Sarah Allen
Notes-taker(s): Sarah Allen

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

Session notes

- overview of digitization challenge at the Smithsonian in 2013, and exploration of linking meta data
    - social network of dead people idea (discussed at IIW 19 Identities of Dead People)
    - realization at prior IIW that all the living people would become dead people someday (IIW 17 - Data and ID after Death)
- genealogy & "truth" challenge
- Internet Archive doing project with wikipedia to cross-reference articles with physical source (e.g. books)
- certificate chains
    - Expert ⇒ linked to all claims, if found to be not fraudulent can revoke credentials
    - Institution ⇒ claims
    - Amateur researchers / citizen scientists
- How to stitch primary source material into authority
- Problem of attribution in case of name changes, marriage
- Examine "network of provenance"
- Having an idea is not enough to claim invention
- Idea of linked relationships, maybe the social network (of historical figures) is the important data to capture — yet how do we know? This is captured in the primary source materials, records of visits, journals, letters
- Problem
    - Modern truth is re-written on the fly
    - "Notability" threshold in wikipedia pages for people
    - Trust in "anti-vax" community, single trusted source of truth in a community, not dissimilar to each of us who have trusted sources
    - Trust and deconstruction of Big 3 media (bygone era of network TV) and the need to rebuild what trust is (what is our consensus) To replace no trust (current era)
    - Altering history, deep fakes
- Chris Savage "Managing the ambient trust commons"
- Sloan foundation looking for ways to establish trust at scale

- what if we were able to capture (and inspect) the trust chain?
- Use case: reassemble artifacts collected in one expedition collected in one event and distributed to many different museums / archives
- Related to git and signing commits

Related Work

- 2013 research: Crowdsourcing landscape (slides, full notes)
- 2014 Smithsonian People Project — exploration of Named Entity Recognition (NER)
- 2019 explorations w/ notes about usefulness
    - The Semantic Lab using Wikibase (because reasons), eg with Linked Jazz and their cool tools (on the right-hand side)
        - ... but where's the source?
    - Zooniverse.org has projects that I feel are along these lines
        - the source is open but I wonder about the accessibility of their data sets
    - FamilyHistories.info has ideas for indexing
        - source and data are open but links may be broken so write collaborator Trent if you'd like to see it fixed
    - FromThePage.com transcription tool
        - but proprietary and rather costly

Next Steps

What to do to push this process forward? Brainstorm here

- What problems might we be solving?
- Learn / Contribute To / Report On existing tools?
- Create a set of standards for any dataset that purports to support truth discovery (eg. data locations, dates, contributor identities, reference codebases, ideally with some cryptographic signatures on it all)
- Curate collections of data sets that help get at the truth
- More philosophizing

Specific next steps (Sarah is exploring options for pilot project this summer)

- Clear Problem Statement
- Pilot project ideas (could be small, focused technical approaches OR small-ish data sets where we can validate how people would add links as they add data)
    - Wordpress plugin (or jekyll, hugo)
    - SF Japanese community stories (Wendy has a connection here, Sarah to follow-up in June)

OpenID Connect For Identity Assurance

Session 6B
Convener: Torsten Lodderstedt, Daniel Fett, Bjorn Hjelm
Notes-taker(s): Bjorn Hjelm

Tags for the session - technology discussed/ideas considered:

Based on a proposal on Identity Proofing with OpenID Connect (https://iiw.idcommons.net/Identity_Proofing_w/Open_ID) presented at IIW 27, review proposed extension of OpenID Connect for providing Relying Parties with verified personal data (in accordance with local/regional regulations and laws) to address use cases of identity verification of a person. The proposed extension can be found at https://openid.net/specs/openid-connect-4-identity-assurance.html.

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

Presentation from the session can be found at https://www.slideshare.net/TorstenLodderstedt/openid-connect-for-identity-assurance.

Discussion:

- We discussed what data is required to verify a person's identity and whether compliance to various regional regulations (eIDAS, NIST SP 800-63, etc.) is required for all data input.
- There are additional (non-PII) attributes (one example given was AML, or Anti Money Laundering, level check and other types of watchlists) that may be required for certain use cases.
- We discussed what types of documents and methods that could be used to establish a person's identity, whether an RP (Relaying Party) could request the use of a specific method/documents, and sample use cases for to exemplify the various requirements.
- There was a discussion on whether a level of identity proofing was sufficient (such as IAL1/IAL2/IAL3), conveying how the identity proofing was done, and whether the intent is to convey verified attributes. On the verified attributes, there was a concern that this could get very complex given the various use cases and regional variations.

It was requested that participants post specific input on the draft specification to the OpenID Connect working group (https://openid.net/wg/connect/) mailing list (openid-specs-ab@lists.openid.net).

FastFed: Easy Connections IDP – App + Governance: Who Should Have Permissions in the App?

Wednesday 6C
Convener: Matt Domesch
Notes-taker(s): Matt Domesch & Thomas Berry

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

1. **Notes received from Matt Domesch:**

   Session Summary:
   High-level introduction to the OpenID Foundation FastFed working group draft specification. Discussion of its implications on Identity Governance (access, permissions, workflow, and lifecycle) for users within an application, which Identity Providers have historically not been responsible for. Will discuss with the WG how best to resolve the inherent conflict, either by a) not including Provisioning in the spec; b) including Provisioning in the spec, and ignoring governance; c) encouraging a private IDP<->Governance Provider interaction that lets each do their part without further complicating the spec.

   Link to presentation: https://domsch.com/IIW28/FastFed-Governance-IIW28.pdf

2. **Notes received from Thomas Berry:**

   Presentation: Identity Governance Using FastFed
   OpenID Foundation
   SaaS apps to companies IdP

   AWS login; tenants; login to FastFed; IdP and App are hooked up after a couple of clicks.
   - discovery of IdP
   - Metadata for SAML/OIDC (hand-shake)
   - OpenID/SAML/SCIM

   Standards provide common attributes between IdP and App

   Oath, Google, AWS, SalesForce...

   FastFed 1.0 Draft

   Just in time provisioning when the user login to the system; utilizes SCIM to provide the user data to IdP

   - IdP is not the canonical source of the identities; identities have to come from somewhere else.
   - Access: Which users should have access to the application?
   - Permissions: which permissions within the target service; what if there are hundreds of things to manage in the application?
   - Workflow: access requests—approvals
   - Lifecycle: joins, moves, leaves; what actions should be taken

   All of this is not typically performed by IdP; Identity Governance!

Governance Provider provides the birthright, workflow, certifications, auditing and logging
GP Private/manual updates to IdP
SCIM between IdP and application

Must turn on governance at the beginning instead of later in the implementation (schedule).

How to do FastFed with Explicit Governance
Governance Provider ——Private exchange, could be SCIM—-> Identity Provider —-AuthN—> Application
Governance Provider ——SCIM, provisioning/deprovisioning/updating users—> Application

Identity Provider would continue providing user authentication to application

Comment/Input:

- Most applications decouple SSO capabilities (authentication/authorization enforcement) from the application; all of the FastFed functionality should be provided (packaged into) by IdP.
- addresses the SAML use case, but SAML doesn't provide bootstrap
- This would depend on pre-catalog of Application/IdP
- Existing IdP/Federation solutions present a deployment problem

If we were to remove (moving) provisioning from IdP to GP,

- IdP is the source for identity
- Group membership is specified by business policy in GP

FastFed with IGA = Governance from the start

By splitting the FastFed concept of Identity Provider into two parts, the IdP and the GP, we can allow richer governance...

Pre-employment/post-employment use cases

- Comment: FastFed shouldn't try to address this workflow; out of scope

Developing Standards: Involving Non Tech People?

Wednesday 6F
Convener: Heather Vescent
Notes-taker(s): Ellie Stephens

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

If your goal with standards is to solve real business problems, if you could parallel path the development of implementation tools will lead to real adoption. Nobody knows how to do it. Ratifying a standard and people taking advantage theirs a lag. There's a lack of implementation tools. Then you an involve biz ppl from the get go and lead to real adoption.

A biz requirements document had to be written. The technical working group has to meet the biz requirements

Long history in standards work with Telekom. Involved in internet standards in b2b alliance deliberately partnering with and including users in the process. We're working with Don Norman, father of user-centric design. Lab at UCSD. This is all nascent but my vision. We have academic and expertise.

The problem we are facing are not tech problems. It's design.

It's not rocket science. UX experts (anthro, socio). A virtual user community a dedicated and available. Creating a certification mark to know that my tech is treating me with dignity. It's user facing so everything has to be very understandable.

Are users helping you develop standards protocol ?

Create a code of practice. We want an interoperability spec but we're far from it. Intended to be understandable by people.

Very important. Goes back to the implementation tools. As a reader of standards, the barrier to entry is really high. I don't have time to read the full standard of every standard. There's a marketing gap. I don't need to know the details, I just need to know "Is this right for me?" A name a logo, the human side to it, and implementation tool to quickly try this thing out. Web Authentication standard.

Blown away by the fact that the visceral user community isn't. Will end users contribute to specs and standards?

At least code of practice, but we don't know how it will look from there (Telekom example) Nobody does it.

It's not unlike the way the web was. I started my career doing usability testing. The small startup I Was in wanted to test the product with users. I never thought of applying that to standards. UX Usability in recent years has taken off. The tech should mold to what a human should actually do rather than the other way around.

Do people do emotional association? Positive negative? Does usability testing get down to emotional reaction to tasks. We're a teenager in this tech space?
How do you get people on the roadway booking along to recognize opportunity to step aside from being a user to being a beneficiary

It's really about the relationship that you have with that service provider. The technology arc we're on allows us to have a richer relationship

Of course it makes sense we have a relationship arc with our providers as well, but the pain of leaving and changing is too high we often

What is the mechanism for bringing the language to users and back?

Anyone here have example using user data to influence a standard?

If you ask a user they'll say I want X, Y, and Z. 75% of what they want already exists they just don't know what they want.

What info can I give a developer to influence how they write the spec so they consider this vast body of experience? I don't know how to communicate the information to influence the spec.

It was expected the user wouldn't have to do anything. Now the user needs to take precautions etc. we are asking them to do stuff they wouldn't ordinarily otherwise.

The soft factors are evolving. Some of these standards failed because of a human usability. Key dependencies based on the wet wear.

This whole IEEE7000 ethics group. If ever, this group should be thinking about users and the same cast and crew (technologists). The use of use cases as a proxy.

That's really important. Standards do a really great job of covering all the cases.

This iterative process. In SSI, we cannot really include the users there right now because they can't experience SSI in the real world. What frustrates me in this discussion is that we have very experienced techies and they have this idea of decentralized identity not directly coming from techies and then they grab the conversation and it stops. We have this technical part and the specifications part and the political part and we just focus on this one here. We can't include the user at this point.

I develop products and services for tech that doesn't exist today – we can test the ideas today, even before the technology is implemented. I don't want to not include people. It's challenging to be a leader. Step into the space to learn more. It's even harder for tech experts. I don't want to shut them out so they can take less room and make more space for others.

How to start to translate this into engagement with standards body. Doing product discovery calls and writing three paragraphs helps the developers. We're wondering how we connect these to standards bodies.

We talk in our language and we have a problem ourselves with our own language. If we eradicated SSI from our conversations with the outside world. Listening to real world people.

Even the word identity doesn't really resonate. I just want to know who am I working with and am I safe to work with them.

This SSI thing, that work needs to start happening now. It's a great academic idea and we viscerally get. I need to know how that will look to my last pass or logging in experience. It smacks to me like more work.

Security is not easy. How do you get feedback that's code able?

My first intro to SSI was yesterday and my first question was how does this apply to my personal experience (example of daughter entering a bar not having to flash an ID with home address on it).

Often the problem we think we're tackling isn't the one we think we are. SSI is a solution but telling someone SSI is the solution isn't going to arrive where you want.

Let's do a rapid fire ways to involve people in the standards? I'd like to factor in real life use cases.

Not understanding if these are recommendations for the standards body or for individuals.

To create the RFID tech specs, there was a business group that then determined how this standards group

We can create partnerships between and within the standards groups themselves

The 3 Ps whats the **purpose**, the **process** for your own involvement, what's the **payoff**
Outreach and discoverability. I am interested in contributing to specs the I have a problem.

Productising standards. We're trying to package standards the standards development process for different stakeholder and we need that full continuum and that translation has to resonate at different levels.

As a marketing person I am not invited to be part of these things.

As an organizer, I need to step back and volunteer and I did the CCG survey. I want a volunteer. I put it out and got a non typical suspect when we presented the results and that he was successful and used my power as a leader. You have to step back and the people in power and unless you step back and make the space new people won't join. The peer programming model and I'd love to see that in peer leadership.

Radical candor around this is the way you can engage and this is what we are going to do with it.

Ways 2 involve people in the standards?
Welcome humans (welcome center) / industry consortium, your voice/experience is important/useful —> invite + make welcome non-technical people
Update discipline of standards development (Agile, scrum master)
Business requirements (biz group)
Care and feeding process for participants —> expertise, expectations, valued
Understand current state - experts in this role
Discoverable - status, problem, solution
Networking for personal/professional development IRL
Look to civic engagement for ideas

Alice to Bob: Self Sovereign Interoperability Without Censorship US Federal Regulations

Wednesday 6G
Convener: Adrian Gropper
Notes-taker(s): Adrian Gropper & Ben Gregori

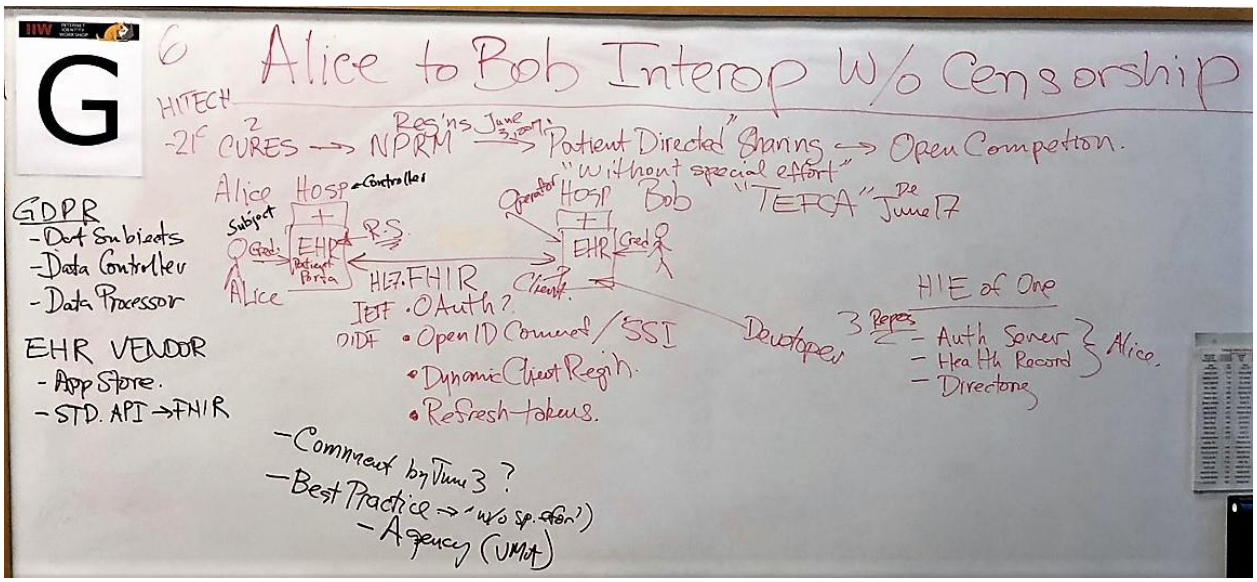
Tags for the session - technology discussed/ideas considered:

->21st century cures -> NPRM Regulations (June 3rd) -> Patient Directed Sharing -> Open Competition

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

1. **Notes received from Adrian Gropper:**
   Platforms can be designed to promote competition or to hinder it. Using health information networks as an example, we discussed the ways technology regulation might be used to promote competition. The role of self-sovereign credentials and signed software statements was discussed.

   Link to "Patient-Directed Access for Competition to Bend the Cost Curve" – The Heath Care Blog: https://thehealthcareblog.com/blog/2019/04/18/patient-directed-access-for-competition-to-bend-the-cost-curve/



********** ********** ********** **********

2. **Notes received from Ben Gregori:**
   21st Century Cures: End of Obama admin, bipartisan law aimed to fix consolidation and anticompentitve behavior (21st century cures Act) – after 2 years, the held and human services from Trump issues regulations that are pro-competitive to fix the High Tech pact (Gov't spent $40bn in computerizing health records)

- "Without special effort" – important phrase. 99% of times, the patients who want to take records out of a network have to go through hoops (in person verification, fees, provide other documents. Doctors have to do the same thing.

NPRM Regulation is "good" – it would be a major step forward into the self-sovereign patient exchange

- Open banking initiative in Europe: it's the same type of thing, saying that if you have an account and you want to pick a different credit card/or other services, you should be able to take it away from that institutions (bank) to another one. Banks should allow interoperability with credit cards
- Same idea, just applied to health sector.

The Term of Art in the law, is "Patient Directed Sharing" – meaning that there are two ways to transfer data re: HIPPA

- Federation based: data requests from another HIPPA covered entity can be moved to another HIPPA complient entity without patient consent.
- The sending or receiving institution wants to control how it moves for business reasons, so the
- If the gov't does it right, instead of silos of networks where patients can only use services within a network, the patient can easily move data between networks.

Why is this interesting from an identity POV?

- Alice uses a patient portal, with a credential that attaches her to the IT system of the institutions using the portal.
- Bob uses a patient portal at a second hospital, with a credential that attaches HIM to another IT system (in another network, another country, etc).
    - When Bob is only *partially* in control of the IT system, how can Alice express consent, you want software that enables Bob to MOVE credentials between networks without barriers, because they are HIS records.
- Protocols:
    - (HL-7) FHIR – when Alice directs sharing with Bob, she needs to restrict access to certain types of information (some medical history, not all). When HER system interoperate, they must adhere to a standard that, in healthcare, is baked into an API (called FHIR) for the apps to be fungible. Then, the regulation gets to dictate whether or not the EHR has to use FHIR…so they can enforce standardization rather than the EHR provider wanting to.
    - (IEFT) OAuth2
    - (Open ID Foundation) Open ID Connect/DID+SSI
    - Dyamic Client Registration -
    - Refresh tokens

NOTE: GDPR separates people into
Data controllers _ those who collect data
Data processors – those who process data (this is outsourced most of the time)

- In this model, the hostpial that hodls the records, would be the data controller
- Alice is the data subject of the records

From a standards perspective, the problems are:

1. To create a comment – by June 3rd (spend an hour look through summaries of the law and which part look okay)
2. What is the best practice, and who in this community,
3. When we realize this real-world situation, and we understand what these standards are, we need agency in this process (UMA)

- what is the responsibility of the developer, who signs the software statement that enables a client to be registered dynamically? Is it signed by the patient? Is it signed by the receiving IT admin in the receiving system?

- HIE of One:
    - Auth Server
    - Health Record

Directing – shouldn't be government because there's an incentive to keep a closed garden approach and to be conservative.

DID Communication: What is Message Routing & Why You Want It In Your Life.

Wednesday 6H
Convener: Sam Curren
Notes-taker(s): Sam Curren

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

Message routing allows a wide variety of routing topologies.

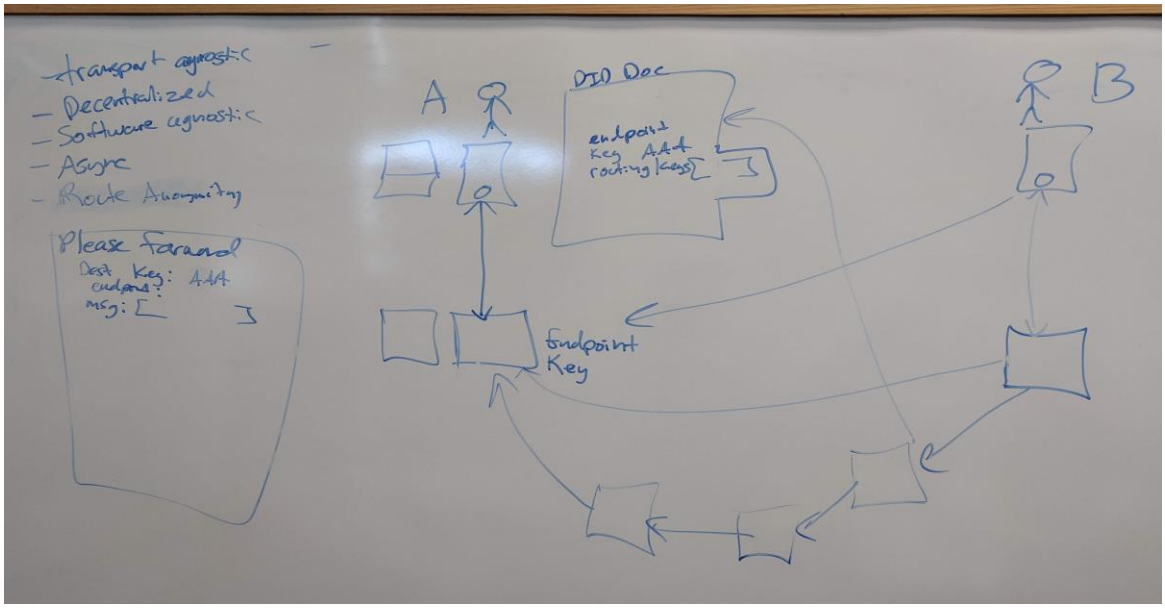
Most common situations are simple.

Some situations can be very complex to match the thickness of your tinfoil hat.

Basic Forward messages and DID Doc conventions allow very simple mechanisms that are easy to use in practice.

Indy HIPE about Mediators and Relays: https://github.com/hyperledger/indy-hipe/tree/master/text/0036-mediators-and-relays

Indy HIPE about forwarding: https://github.com/hyperledger/indy-hipe/tree/master/text/0022-cross-domain-messaging



XACML/ABAC/UMA 2.0 And SSI Policies

Wednesday 6I
Convener: Matthew Hailstone
Notes-taker(s): Matthew Hailstone & Eve Maler

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

1. **Notes received from Matthew Hailstone:**

Copy of white board from session - https://photos.app.goo.gl/HpDbo89kzfY2519X9

2. **Notes receive from Eve Maler:**

One topic we discussed in this session was the HEART profiles and how they define scopes for OAuth, and scopes and resource types for UMA, to allow for redaction of sensitive health data. A HEART webinar/workshop was given on 23 Apr 2019, for which a recording is available.

Let's Build a Decentralized Social Network

Wednesday 6J
Convener: Pete Rowley & Ricardo J. Méndez
Notes-taker(s): Phil Wijs & Ricardo J. Méndez

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

Photos here

- We already have some! Examples:
  - Mastodon (federated Twitter), first one to really gain traction
  - Pixelfed (federated Instagram)
  - Both are built on ActivityPub
  - Diaspora, which does its own federation thing
- ActivityPub
  - Federation protocol
  - Christopher Webber was a co-author
  - Only 3 actions: New item, delete item, update item
  - Your identity is attached to the server where you create the account
  - Webber is expanding it for secure authentication flows through the Spritely project
- Federation
  - Trivial example: e-mail
  - A single domain can host a bunch of users
  - Several trust boundaries

    - All sites communicate through a standard protocol
    - Allows one host to view the users an updates of one in another (Mastodon can view updates from Pleroma, Friendica and others)
    - Every server can do whatever it wants, e.g., establish its own internal content rules
    - Needs care early on to ensure that not all users end up in a single server
    - It's decentralized but not fully distributed
    - Can be self sovereign if you host it yourself
    - Creators for both Mastodon and Pixelfed periodically close access to their instances to ensure people user other instances, avoid becoming a centralization point themselves
- Problems for users
    - User discovery
    - If federated, identity provider might die
    - Account recovery
- Possible approaches for key recovery
    - Social recovery, e.g., DarkCrystal for Secure ScuttleBut
    - Multi-party computation, e.g., Kzen's ZenGo
- Decentralization axes
    - Something that is distributed among many servers but organizationally centralized (Google crunching data across farms).
    - Something that is organizationally decentralized but it's logically centralized (it's in a single state the whole time, e.g., Ethereum)
    - Something is logically decentralized doesn't need every node on the network to be on the same state (Mastodon, IPFS)
- Secure Scuttlebutt
    - Can be fully encrypted
    - Uncensorable
    - Have a private key
    - Write for a public key
    - Completely peer to peer
    - Doesn't need an internet connection
    - When we sync, all messages go to the other system
    - Eventually the messages make their way to you, but there's no guarantee
    - Usability issue: you never know if the person will receive the message
    - Unclear if it scales
    - Not as efficient as always-on social networks, different trade-offs
- Other notes and questions
    - How do I bring my identity and network with me?
    - Our networks and identity should live on our smartphones
    - Facebook wants to do "privacy" but it won't really be private if you know who's being assigned what ads (even if the data is analyzed on device). It's more of a sales pitch.
    - Samsung and Apple make money on devices and value-add services.
- Marketplaces can be a way to fund this
    - A lot of talk about data marketplaces. "Sell your data and get paid for it". Terrible idea and ignores privacy-as-a-commons.

    - Data analysis marketplaces. Someone wants to run a study and only cares about the result, not the raw data. There's an intermediary that can gather a bunch of data, crunch it privately, and spit out a result. End users would opt in.
- Health care and privacy
    - People need medical care and they're trying to find a way to cover the cost of healthcare. A pharmaceutical company may need your data if you're testing a new drug. Your data is worth a lot of money to them. In a self sovereign way, you own your data and it's cleaner for them to have your data.
    - Australian health care system is set up MUCH different. But you may want to choose who you give your data to. Does the person that is handling my data protecting it enough.

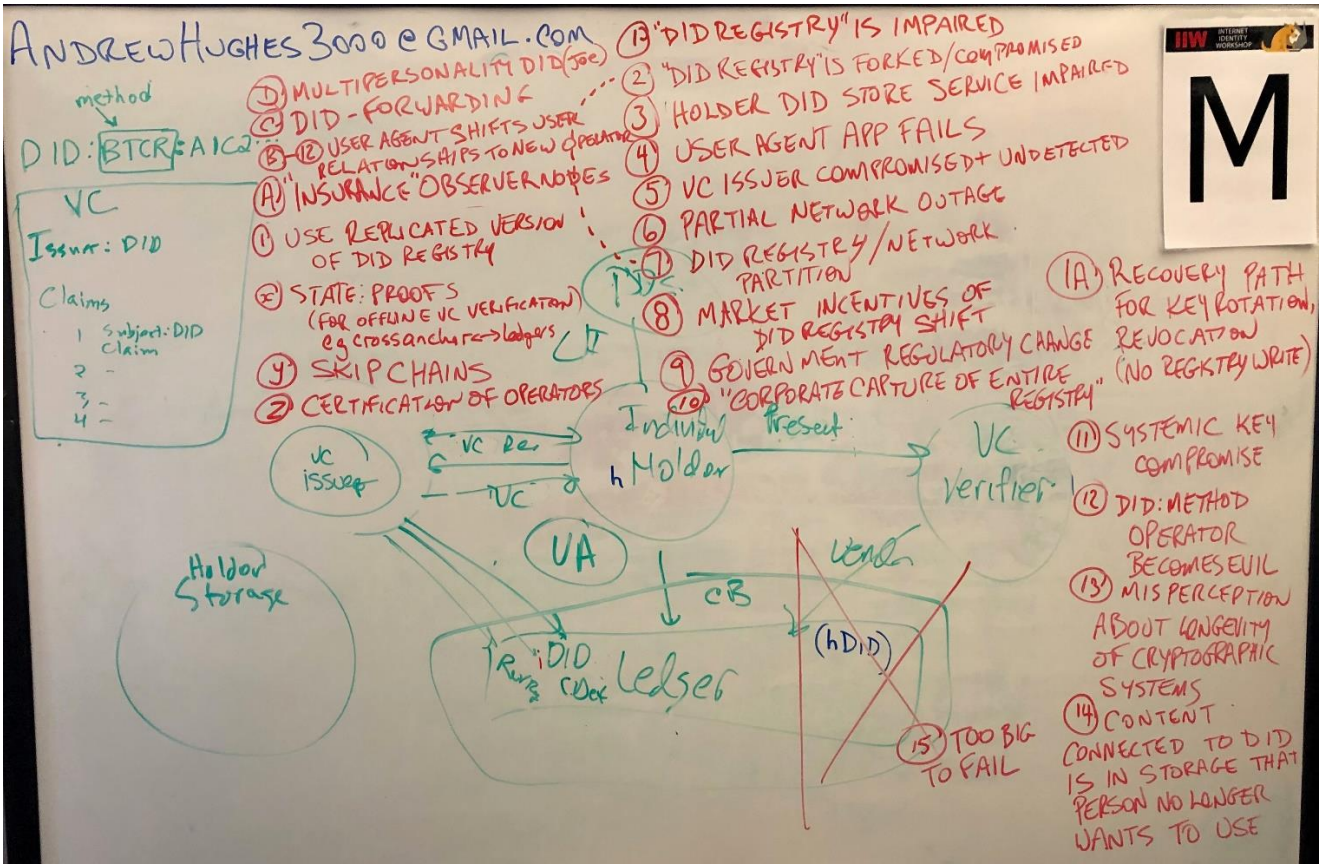
What's Supposed to Happen when a DID Operator Goes Out of Business?

Tuesday 6M
Convener: Andrew Hughes
Notes-taker(s): Andrew Hughes & Nicholas Rempel

Tags for the session - technology discussed/ideas considered: OAuth, Scopes, Claims

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

1. **Notes received from Andrew Hughes**



********** ********** **********

2. **Notes received from Nicholas Rempel:**

What is supposed to happen when a critical piece of did infrastructure goes down?

Hypothetically 20% of the critical infrastructure goes down. How to we plan for this?

[VC Architecture drawing]
Possible fail cases?

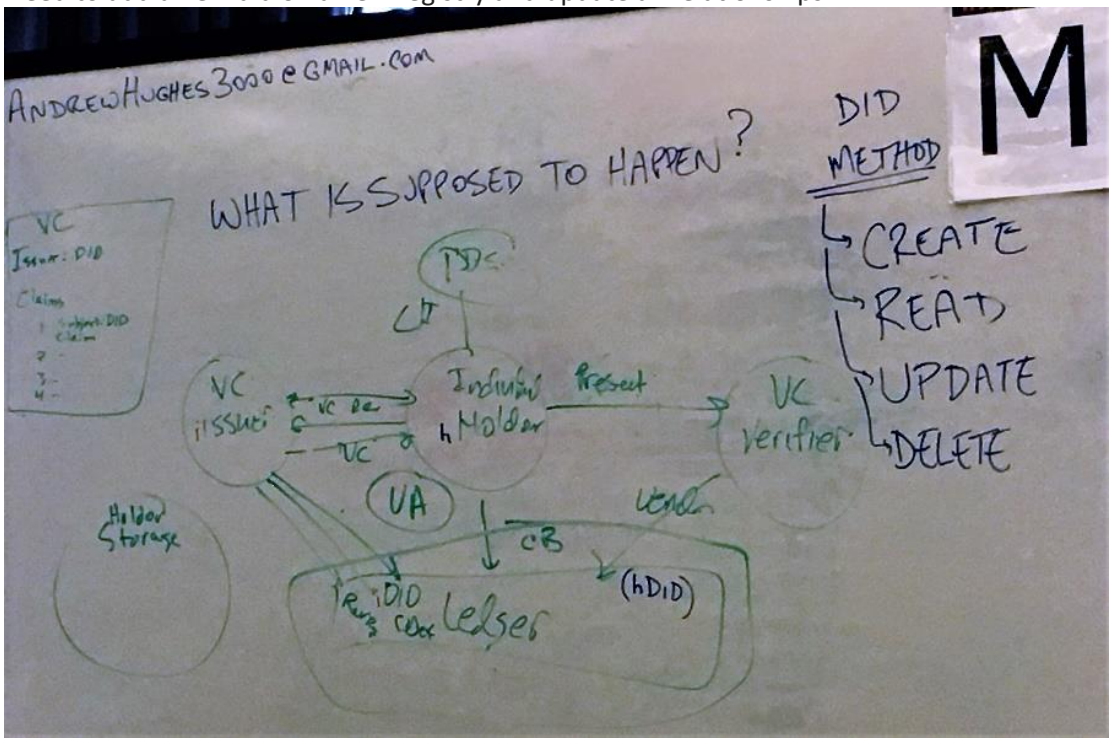
- DID registry is impaired

solutions:
- Replicate version of the registry
- DID registry ledger is forked
- Holder DID store service impaired
- User Agent app fails
- Issuer compromised
- Partial network outage
- DID registry/network partition
- System key compromise
- Recovery path lost - no key rotation
- Entire did registry is a bad actor
- misconception about longevity of cryptographic systems

Fallback/Mitigation
- Blockchain/ledger solves many problems
- HL Indy includes state proof. Verify proofs offline
- “Skip chains”
- Auditing/Certification
- Insurance observer nodes - business that replicates chain for a fee
- DID forwarding?

Is there an option for a mass migration from one did registry provider to another? Can a single DID be ported to a different registry? No.

Need to add a new did on a new registry and update all relationships.



XYZ Transactional Authorization

Wednesday 7A
Convener: Justin Richer
Notes-taker(s): Aaron Parecki

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

1. **Notes received from Aaron Parecki:**

   there are a lot of extensions to OAuth 2.0 to help it fit into other places, PKCE, UMA, OIDC, etc

   a lot of these applications and extensions have added their own bits and pieces over time

   if you take all of the oauth 2 specs and stack them up it's a big pile, and they aren't even necessarily compatible with each other

   what if we took a step back and instead of saying how do we make oauth do these things, try to solve this better

   oauth.xyz

   current draft spec at oauth.xyz

   it's still fairly early, but has implemented some parts of this

   two of the big things that are problematic of oauth 2
   - it relies too much on passing data in the front-channel
   - it doesn't have a good underlying data model for what a client or resource is

   in this protocol, there is still an authorization server, but it's defined as a single URL. it's equivalent to the token endpoint in oauth, it's backchannel only, takes JSON in and returns JSON out

   what the client does is it talks to the authorization server and says this is who i am and this is what i want. this is represented in this JSON object.

   by the way this is a strawman, so please burn it down, but not with the argument "this isn't how oauth 2 works"

   the client says this is who it is, name, home page, etc. this allows the client to show up and declare this to the server. this feels funny in an oauth 2 world where everything is assumed to be preregistered. but this is just user facing decorative information which gets self declared in client registration today. notice that there are no functional URIs or keys. this is like a dynamic client registration request.

   the client and server has the option to support a "handle" request, so instead of passing it by value it can pass by reference which it may have gotten from preregistration or previous communication.

next: interact. this is how the client can interact with the user. this says the client has the ability to redirect the user and can be redirected back to me. this is the auth code flow. there are a couple other modes, but this is where you declare it. this is also where you declare your state parameter since it should change every transaction, it's required, and sent in the back channel.

next: resources. this is very loose right now. Torsten Lodderstedt has been doing some interesting work in fleshing out this area and the ideas will probably merge. can either send a list of strings like oauth scopes, but you can also declare this is in more detail the kind of things you want. in this example, actions, locations, but torsten has a different data model which is probably better.

the key is for a client developer, if the API is built in such a way that it has a set of predefined resource sets, those get handle identifiers and you can send the handles in. or you can say "i only need read access to this small subset"

next: user. this is from UMA. this is the ability for the client to push information about the user. UMA calls it a pushed claim. if the client knows something about the user, it can pass this assertion about the user into the authorization server. oauth 2 doesn't have a place for this, but UMA does, but it's not as well defined or supported. the people who have use cases that oauth 2 doesn't fit, this is one of the things. the client needs to be able to say "on behalf of this user i need to get these resources". This can also be passed in as a reference handle, which is like the UMA persistent claims token.

finally: keys. A big gap in OAuth 2 out of the box is the ability to bind keys in the client software to the resulting tokens. We want clients to be able to declare at transaction request time, these are the keys that I have and prove they have access to the keys.

that's the request. the response has a similar set of potential sections.

there are few bits to point out and then get in to how interaction works.

first, this is the authorization server telling the client, I need you to get the user involved with me, so send them to this interaction URL. the client takes that URL exactly as is and sends the person there.

this first handle is the transaction handle. when the client comes back from the transaction endpoint, or if it's polling, or if it needs to refresh an access token, etc, this is how it references this transaction and all of the decisions/claims/rights it's associated with. in this example it's a bearer shared secret, but there could be other ways to manage it, including any keys that have been presented and proved need to be proved again when this handle is used.

the client_handle and key_handle come back optionally from the transaction request and say that's great you can give me just this handle next time you come back instead of providing all the client metadata key metadata etc. it's effectively dynamic client registration but it's built into the protocol.

Interaction
this example is basically the auth code flow. the client says I can interact with the user by redirecting them and then you can redirect back to me. When you come back to me, you can redirect to this URL, and here is this state value. This should be sounding familiar. When the server processes this, it decides from that request, I need a user to approve this -- this is not necessarily a known client, this is not a continuation of a previous transaction, etc -- whatever reason, the AS decides I need a user. So it tells the client to send the user to this URL (interaction_url), and when you get the results of that here's a

transaction handle to continue it. This URL, unlike OAuth 1 and 2 and UMA, is a fully formed static URL that the client does not add anything to. This URL is already a reference to this entire transaction at the AS. Yes this means the AS is stateful, and sure there are ways around this but it's an implementation question.

As far as the client is concerned, it gets a URL and sends you there. Meanwhile, the AS interacts with the user, so we're in classic OpenID/OAuth territory, ask them to identify themselves and ask for authorization. Unlike OAuth, this mechanism also can stand in for claims gathering endpoint in UMA 2. It's important when we define this in the spec text that we make it more generic. This needs a little more thinking.

In this mode, the auth server knows how to send you back. It takes the URL that the client presented at the beginning (callback URL). Just like in OAuth 2, the auth server adds a couple parameters to the callback. Went back and forth on this, because if we require the client to generate a new redirect URI every time, we can get rid of the state idea. But instead, the state parameter is required, and the AS sends back a hash of it as well as the interact handle.

The client will look at the state value and match it up. Just like in OAuth 2, I tried to design this where the client is the stupidest piece of software in the system. The client takes that handle and sends it back to the authorization server.

Right now it sends it back to the transaction endpoint both the first handle and second handle. In this example, the transaction handle is sent as a plain bearer value but the interact handle is a hash, not sure where the right balance between bearer and hashing is yet.

The client also needs to continue to prove possession of its keys, so if the client had a JWK then it would need to include a JWS in this.

At that point, AS looks up the transaction handle and figures out ok whatever the user did plus whatever the client did is that enough to issue a token.

Question: Daniel Fett - you're using a state mechanism here, why not PKCE? (Debate about whether PKCE replaces the need for state in OAuth 2).

The other interaction method written up and implemented here is the client says "I can get the user to interact but not directly, I can tell them a URL and tell them to punch in a code, but I can't send them there or get anything back", like the OAuth device flow.

The interaction URL you get back here is allowed to be static, and then also returns a user code. While the user is using their secondary device, the client keeps calling the transaction endpoint with its handle and checks whether the user is done, just like OAuth device flow.

The response includes a "wait" value, and importantly, every time you get a response you get a new transaction handle. You never reuse a transaction handle. This is based on UMA 2 and some consider best practice on refresh tokens in OAuth 2.

Eventually the interaction ends with a token response.

Tokens have the opportunity to be better defined here, but they aren't better defined yet, except by saying they can be bound to keys like how existing OAuth mechanisms work. Since we have methods for binding keys we can bind those to the token. We can still do bearer tokens, or bound to any key the client has presented, or potentially to keys the server issues along side the access token itself. For example the server can issue a key pair that it expects the client to use again.

It's important to have the capability to bind various kinds of keys at runtime to transaction requests and to access tokens. By binding them to transaction requests it also binds to all the sections in that request. This gets bound to keys, instead of in OAuth how there is a vague notion of a "client".

Refreshing tokens -- when you get an access token, if you still get a transaction handle along with the access token, that's the AS saying i'm going to remember all the decisions i made when I issued this access token. That can be used to get a new access token.

Question -

George Fletcher - do you cover things like downscoping? or are you punting on that and saying go get an entirely new token?

Justin - as soon as you're allowed to modify a transaction, even if it's downscoping, does that change the meaning of the handle?

George - if you don't do that, it means you expect clients to manage multiple handles

Justin - the response can already come back with a bunch of handles that represents various parts of the request, so maybe the client sends most of those back, but not sure. Leaning towards that being a separate token request like "this is what i have give me something new"

David Waite - if you have tokens that are bound to the client, you might not need downscoping as much, since it means you already have the assurance of the client

Justin - one of the reasons we have downscoping in OAuth 2 is that it's relatively difficult to get a new token, so the idea was, you ask for as much as you think you need at the beginning, but then when you go get the access token you get only what you need at the time. In the real world, that's being pushed in the other direction, which is asking for a minimal set to get started and making it easy to upscope.

Eve Maler - thinking of these transactions as things that can be referred to legally is great. Some things that still need fleshing out - introspection, revocation. Those should be addressed here because OAuth punted on those and they've been bolted on after the fact.

Also interestingly, this gets rid of the mixup attack or the AS attack, because the answers are all coming from one endpoint. You get rid of a lot of the necessity of having a separate discovery document. I'm not convinced you could do all of this by just having one call yet but maybe? But I really like the idea of having an AS defined by this singular URL that the client and resource servers have to talk to. Nat tried to do this in OAuth/OIDC years ago with linked data models, this is a simpler way.

Natalie Nguyen - I don't quite have an understanding of all of the problems, so at face value it looks like you're taking a relatively unopinionated model like OAuth 2 but coming up with an opinionated model and not allowing flexibility and extensibility that OAuth had. In doing so, what are the problems that you're solving.

Justin - check out my talk What's wrong with OAuth 2. It's a small sampling of the answer to that question. Some of it is covered on the website, a lot of the problems are related to

overuse of the front channel, and a lot of what's been developed is to cover up our use of the front channel.

Last IIW, Aaron and I were talking about an early version of this, and worked on a way to do this handle mechanism on top of OAuth 2. Aaron built a prototype of posting the initial request instead of putting it in the query string with minimal changes to his existing OAuth server.

The modularity in OAuth 2 in a lot of ways is fantastic, but in a lot of ways we guessed where the extension points are wrong.

If you look at the examples on oauth.xyz, I would want lots of extensibility in the sections you see there to support things I haven't thought of. The core syntax and processing stays the same but the data model can be extended. The extensions become what to do with the data rather than how to pass data around.

If you look at PKCE, it fails "open" in some disturbing ways, so I want to avoid those kinds of things here.

Aaron - how do you plan for the unexpected extensions that may be needed to fix problems that will be found with this in the future?

Justin - having the request and response portions with a well defined core, and defining the extension mechanisms very clearly. In the real world, you come up with a great idea, like deprecating the implicit flow, and people light the internet on fire because people don't want to change. It's a tough question though and gets into standards definitions.

IIW Book Redux (Part 2)

Wednesday 7B
Convener: John Jordon
Notes-taker(s): John Jordon

Tags for the session - technology discussed/ideas considered: VON, Agent Demos

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

1. **Link to presentation provided by John Jordon on Tuesday (Part 1) & Wednesday (Redux):** Http://IIW.vonx.io
2. **Duplicate notes provided by Jim Wowchuck, from Part 1 (Tuesday 2A):**

Key understanding: a demonstration of an identity authentication, issuing, relying party connection and document/chat exchange using authenticated identities.

Steps were described and followed as per slide 1 (photo attached).

Most of the session was walking through participants through the process and providing ids for delegates.

Discussion followed on about the increasing integration between different agent providers using a set of criteria as discussed on slide 2 (photo attached).

There was continued discussion about a Connectathon last February where 6 different systems were verified as connecting. Evernym was not a system that passed, but this was not held as a lack of ability as much as direction of activities – they had more important features they were working on.

Acceptance that even with non-connecting apps, all family protocols have many of the features but with slightly different protocols.

Healthcare & SSI, Use Cases For All

Wednesday 7C
Convener: Leah Houston
Notes-taker(s): Scott Mace

Tags for the session – technology discussed/ideas considered: Healthcare, SSI

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

Leah Houston MD www.hpec.io

I am a physician and had my identity stolen. Our identity as physicians is not only being tangibly stolen by health companies, but also poached from the background as well. Hitech coerced physicians to adopt EHRs. It was designed to capture your data as patients, my data, to deny you services, deny me payment. They see what the average is after doing analytics, everybody below this bar doesn't get care, doesn't get services. Leads to this crisis in healthcare. SSI is what we need. Important people realize for an individual patient to have sovereignty, they need to interact with a self-sovereign system. I found Dr. Adrian Gropper, working on a self-sovereign system for patient records. Maria is also working on patient privacy and data.

Maria: Why didn't personal health records work?

Adrian: They are very expensive for physicians. Also require patients to do work. Transiting a personal health record makes it hard for the doctor to process into their workflow. Also in the long run, we start having implants, things being monitored 24x7. You can't stream that through a PHR.

Maria: Certified nurse midwife. We had an EHR, women could access, for out of hospital birth. But I'm new to SSID.

Adrian: This is the teachable moment.

Leah: How many people want to take your healthcare records with them? (Most raise hands)

Q: I would love to control my health data no matter where it sits. But my MRIs are huge.

Q: My wife wants them. The healthcare companies are doing data migrations and they're doing them wrong. I want access to them no matter where they are.

Q: Is HIPAA a two-way street?

Q: There is the need for portability. Encryption at rest and in transit is good.

Adrian: There's a ton of guidance. You have an absolute right to request your records for yourself or to be sent wherever you want. As long as the doctor has a reasonable way to send it. You could say I want it in encrypted form, the question is do they support the kind of encryption you want? Sometimes yes, sometimes no.

JohnnnyCrunch: Try going to an external healthcare provider, providing records from your Google drive. This is the role of where the DID method specs could manage the automation of compliance for BAAs. It's the physician who signs the document attesting to the validity of your records. The interesting issue, do I sign it with my self key or my organization key? I as a doctor want to keep my own medical records, all my cases, but if I leave organization A, all of my records are tied up in that EHR. What rights as a physician do I have to access those records? The answer is a Web of trust right now. Epic had no idea if I was practicing as a hospitalist at Stanford, or as an independent physician.

Adrian: What matter is what Alice the patient chooses to identify Johnny the doctor as. Could be via email address. May have a Direct email address. Johnny has a DID has some info associated with it. Johnny has two verifiable credentials: his license, and the hospital. Certificates held by each. Alice doesn't need a credential. Only patient portal user ID and password. The third actor is the user agent from some company. Could be Epic. The user agent Johnny uses to access Alice's records wherever they are. FIDO has a self-sovereign public/private key pair. Trust me, I was built by YubiKey. Just pointed out the certificates in HIPAA and healthcare that matter. And no others.

Q: NPI?

Adrian: We recommend, also Fred Trotter, the NPI address have a Direct email address to be linked. Very useful thing. It doesn't change anything. Just a well-known place.

Q: I don't know how well NPIs are working. The spec has three.

Johnny: People don't know how to manage it. This is how it is today. If want to export record out of EHR, travel to India. How does the flow state work today?

Adrian: I'm not sure how it can ever work. Figuring out how to get a hospital to sign a health record or a piece of a health record is very difficult. To layer on top of FHIR signatures of any significance in a health record makes me laugh.

Leah: The information in EHRs is invaluable to me as a doctor. It doesn't matter if the health system is willing to sign that certificate. You know your medical history for the most part. I personally believe you should have one medical record. Lots of inaccuracies filling it out multiple times. HTM vs. hypertension.

Adrian: It's called Apple Health. Does that meet your requirements?

Q: Works with Sherpa? 98.6?

Q: Who the early adopter customers might be?

Leah: I would like to think it's the individual patients. Pick up their decentralized identities as soon as they're usable enough.

Q: Mothers are early adopters.

Adrian: When you take this away from the hospital, now you can join a patient group. Whether expectant

mothers or chemo patients. They should make it easy for other patients to navigate the system. Nothing to do with how you use Apple Health. Can interact with licensed practitioners without interference and censorship of the hospital.

Leah: First step is untether the physicians from these systems. In a digital space so when they are having a conversation with you, you should adopt this platform, it's interoperable.

Q: Lobbyists want to push one commercial thing over others.

Leah: Each physician is caring for 600 to 1000 people. If there's enough of a network effect. Both physicians and patients are pissed off at the system.

Adrian: And neither has any economic power.

Johnny: We have a sick care system. More and more there are engaged patients.

Leah: Cardiologist told me I will be fired if I take a certain number of people in the cath lab. Physicians are terrified of the system.

Adrian: We want a system that does telemedicine by default. As long as you assume telemedicine by default, it makes sense. An easy way to organize what we're talking about here.

Johnny: I track my dad's healthcare through my Apple health. It's tied to the device. When I present, doctors are thinking I have my dad's symptoms.

Adrian: 100 times more important as machine learning and AI gets going. No way to factor in social determinants of health. It's not to prevent identity or harm to individual patient. It's the decision making algorithm. You have to do all of this in the context of how will society use the data, including non-HIPAA data, to determine the value of putting in a stent.

Johnny: This is a slippery slope. A machine learning method, your fitbit data. You can end up in a high-risk pool.

Leah: The data is dirty.

Johnny: It's a money question. What's the value of her life. This is why mammograms are done at age 40. Colonoscopies are the same way at age 50. If you suddenly put a price point, then you have a personal responsibility you are ignoring, the leap would be you are paying a higher premium. Gets into anonymization of data, plausible deniability that it's me.

Leah: I need to fix malaligned incentives. People getting in sometimes too much healthcare. Would anybody sign up for a self-sovereign record system now?

Protocols vs APIs: Resolving The Programming Paradigm Difference Between DIF and Indy

Wednesday 7F
Convener: Daniel Hardman
Notes-taker(s): Daniel Hardman & Eugeniu Rusu

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

1. **Received from Daniel Hardman:**

Here is the link to the slide deck that informed our discussion:
https://docs.google.com/presentation/d/1FfvSfcjnjIbDkT9yUADI-7CJxjlm42eOZB534dXYRSs/edit

********** ********** ********** **********

2. **Received from Eugeniu Rusu**

The main goal of the session was to identify key conceptual / design differences between DIF Identity Hubs, referred to as Hubs, and Indy Agents, referred to as Agents(capitalized), and perhaps align the architectures to ensure that the implementations are compatible by design.

One of the first arguments made during the session was that the established client - server architectures that emerged from the caller / callee paradigm do not suffice for the problems that both Hubs and Agents aim to solve. This approach was deemed restrictive in a number of ways, mainly:

- Assumes two participating parties (server - client / caller - callee)
- The server / callee maintains the state and is always authoritative of it
- Interactions are modelled in terms of request / response loops, which manifests itself throughout documentation, tests, and error handling flows.

This can make it difficult to reason about the overarching protocol / subprotocols the individual interactions are a part of, e.g. in the case of error handling, it might be unclear if an error that happened at step 3 of a protocol (out of 5) means that the entire interaction should be repeated, or only step 3.

The argument was made that in order to more naturally model complex / multiparty interactions between agents online, "protocol" based thinking should be adopted. Protocols have the following characteristics :

- Multiparty (e.g. online auction where multiple buyers interact with one seller, the peer did method specification).
- Have clearly defined roles (e.g. buyer / seller), which are decoupled from being the caller or the callee.
- Relevant state is distributed across the participating parties.
- Subprotocols can be employed for things like error handling (e.g. if a vendor did not understand the buyer's order, they can ask them to repeat the order, without having to restart the entire interaction).

Further differences can be found in the linked presentation.

It was also pointed out that in some cases the request / response flows cannot be satisfied by the transport itself (e.g. simplex communication channels).
Furthermore, in some cases agents can be offline, only reachable through push notifications, or only reachable indirectly (through other parties / relays).
It is important to keep these factors in mind to make sure Hubs and Agents can accommodate a large spectrum of use cases.

After this introduction, the discussions related to conceptual differences between the designs of Hubs and Agents have started.

It was pointed out that a number of interfaces exposed both by both Hubs and Agents are not contentious (e.g. collections, stores), and that the responsibilities / characteristics of Hubs / Agents are similar (e.g. holding keys, acting as a fiduciary to an identity owner).

One contentious point seemed to be the "Actions" interface exposed by DIF Identity Hubs. The argument was made that this interface is designed with the client / server model in mind, and that despite the fact that hubs can form a mesh network without one central / governing instance, a strong perception of two party API-like interactions still persists. This argument was rebutted by participants involved with developing identity hubs, pointing out that the design of the aforementioned interface allows for multiparty interactions, and that the protocol state accumulated throughout the interaction is evenly distributed between the relevant participants.

As the session progressed, some participants noted that the language used to define Hubs / Agents and their responsibilities is at times ambiguous, and that some terms are overloaded. It was mentioned that this can lead to confusion, and foster the perception that the two initiatives are much more different than they actually are.

For the rest of the session, discussion was centered around the "Actions" interface in an attempt to clarify any confusion and false assumptions present in the group. It was concluded that the best way to reconcile the different understandings is to implement a protocol (e.g. the Indy Introductions protocol) using both Indy Agents and DIF Identity Hubs.

It was also decided that a further session should be scheduled to address any remaining questions.

Approach to Bottom-Up Standardization of Claim Content Structures

Wednesday 7G
Convener: Marton Csernai
Notes-taker(s): Marton Csernai

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

A general takeaway from our session was that the topic of Standardization of Claim Content Structures might be too early in the IIW community but it will probably become relevant in the future.

Remarks: Additionally to claim contents, it would make sense to include other aspects of the credential creation process into the proposed standardization mechanisms. For example, it is really important for banks and insurance companies how and based on which standard process or regulation an attestation (validation of the identity claim) has been done during the KYC (Know Your Customer) process. For example an attester could state that the credential creation process adhered to a specific version of the NIST Digital Identity Guidelines (https://csrc.nist.gov/publications/detail/sp/800-63/3/final). A system like KILT could do this by the attester putting self-attested claims into the credentials as legitimations, stating which protocol was used during the creation of the attestation.

The discussion about standardization started already in the DIF Credential Manifest (https://github.com/decentralized-identity/credential-manifest/blob/master/explainer.md).

GIT + DID (Part 2.1)

Wednesday 7H
Convener: Dave Huseby
Notes-taker(s): Thomas Berry

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

- DIDs for repos
- DIDs for DID docs int-repo
- What does CRUD mean in this context

did:git: foo_bar_<keyid>

Is there an identifier that can represent the tree?

did:git:<sha1 of genesis commit>:<path to did doc>

Root of trust is you're talking to the same git tree

PGP signatures are not self resolving; no public keys

1. Build a signing tool to add signature on commit
2. Signature would included as did string
3. Before you want to commit you have to send a did document
4. Then, the repo itself can be self-verifying proving a proof of work

Git as a blockchain “we get our revenge”

The original maintainers of the chain need to have consent

- need genesis (of your trust)
- Signed by initial maintainers
- SHA1 (git going to SHA-2 [or better] at some point [by end of year]) of commit is unique identifier for the repo

multi party computation (MPC)

You now have the ownership key of the blockchain
They just have to sign something to anchor to the chain

“I want to write a unit test to check if the code meets a spec” W3C can verify

- Single DID doc
    - Well-known name (.git/genesis), or better name: “we got this” “not the did doc you’re looking for”
    - DID doc blocks for keys of maintainers

Commentary:

- DID spec includes a query spec; W3C won’t publish a version that includes it (not true)
- It includes resolution and did referencing
- What would a path mean? What would a query mean?
- In a pull request in the did spec, if there is no path, then it has to invoke a service endpoint
- Path = repo relative path to did doc
- SHA1 genesis is the repository
- Git as blockchain; push is a transaction to the blockchain

Making A Map of All The Working Groups Working On SSI/Decentralized ID + How It Fits Together & Making a Weekly/Monthly/Yearly Calendar (Part 1)

Wednesday 7I
Convener: Kaliya Young & Pam Dingle
Notes-taker(s): Kaliya Young

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

We started out brainstorming all the groups we could think of and clustering them.

DIF

Identifiers Names and Discovery
https://identity.foundation/working-groups/identifiers-names-discovery.html
-> SideTree protocol
-> Universal Resolver
Members of the Working Group are engaged in development of protocols and systems that enable creation, resolution, and discovery of decentralized identifiers and names across underlying decentralized systems, like blockchains and distributed ledgers.

DIF Storage and Compute
https://identity.foundation/working-groups/storage-compute.html
Secure, encrypted, privacy-preserving storage and computation of data is a critical component of decentralized identity systems. As with identifiers and names must be self-sovereign to the owning entity, a user's identity data must remain private, only accessible to the entities they allow. DIF members are actively developing specs and reference implementations for provider-agnostic, run-anywhere solutions that provides these features.

DIF Claims and Credentials
BiWeekly on Thursday
https://identity.foundation/working-groups/claims-credentials.html
Join this group to contribute to the standards and technology that create, exchange, and verify claims and credentials in a decentralized identity ecosystem. For example, a cryptographically verifiable credential that proves an individual has a college degree or is of a certain age. Our members focus on specs that are vendor agnostic and based on industry standards.

DIF Security <- New

DIDAuth
We will have the DIF DID Auth WG page soon. Meetings are bi-weekly: Next meeting is May 23th, 7-8 pm (CEST) - In the meantime, the group agreed to have the following charter and scope:

The purpose of this working group is to design, recommend and implement a universal authentication protocol that relies upon open standards and cryptographic protocols, including DIDs and DID Documents. Recommendations and development of specifications, protocols, and formats for data structures used for authentication. The Working Group's areas of activity may include, but are not limited to, the following:
- Define the formats and protocols necessary for authentication using DIDs and DID Documents which we intend to recognize as formally DIF-approved

- Implement DIF-approved DID Auth proposal
- Develop tools for validation and programmatic interaction with DID Auth.

Interop Project

Indy
https://github.com/hyperledger/indy-node#about-indy-node
Hyperledger Indy is a distributed ledger, purpose-built for decentralized identity. It provides tools, libraries, and reusable components for creating and using independent digital identities rooted on blockchains or other distributed ledgers so that they are interoperable across administrative domains, applications, and any other "silo."

AREIS (Indy Agent) -
https://github.com/hyperledger/indy-agent
Agents come in all varieties. Some are simple and static; these might be appropriate for IoT use cases that are hard-wired for a single connection. Others are complex and cloud-based, suitable for enterprise use. Still others run on mobile devices for individual users.
Wednesday Noon Pacific

Indy SDK
Wednesday 7am

Peer/Pariwise

W3C

Credentials Community Group
https://www.w3.org/community/credentials/
The mission of the W3C Credentials Community Group is to explore the creation, storage, presentation, verification, and user control of credentials. We focus on a verifiable credential (a set of claims) created by an issuer about a subject—a person, group, or thing—and seek solutions inclusive of approaches such as: self-sovereign identity; presentation of proofs by the bearer; data minimization; and centralized, federated, and decentralized registry and identity systems. Our tasks include drafting and incubating Internet specifications for further standardization and prototyping and testing reference implementations.

Part of this Group meets in
DID Spec and DID Resolution Spec
Weekly Meetings
https://docs.google.com/document/d/1qYBaXQMUoB86Alquu7WBtWOxsS8SMhp1fioYKEGCabE/edit#
Will become the DID Working Group
Verifiable Credentials Working Group
https://www.w3.org/TR/verifiable-claims-data-model/
Credentials are a part of our daily lives; driver's licenses are used to assert that we are capable of operating a motor vehicle, university degrees can be used to assert our level of education, and government-issued passports enable us to travel between countries. This specification provides a mechanism to express these sorts of credentials on the Web in a way that is cryptographically secure, privacy respecting, and machine-verifiable.

WebAuthN
Standard: https://www.w3.org/TR/webauthn/

Working Group Page: https://www.w3.org/Webauthn/
The Web Authentication Working Group published Web Authentication: An API for accessing Public Key Credentials Level 1 (WebAuthn) as a W3C Recommendation on March 4, 2019. This specification defines an API enabling the creation and use of strong, attested, scoped, public key-based credentials by web applications, for the purpose of strongly authenticating users. As a core component of the FIDO Alliance's FIDO2 set of specifications,

Activity Streams 2.0

https://www.w3.org/TR/activitystreams-core/
This specification details a model for representing potential and completed activities using the JSON format. It is intended to be used with vocabularies that detail the structure of activities, and define specific types of activities.

OpenID

OpenIDConnect Self-Issued

https://openid.net/specs/openid-connect-core-1_0.html#SelfIssued
OpenID Connect supports Self-Issued OpenID Providers - personal, self-hosted OPs that issue self-signed ID Tokens. Self-Issued OPs use the special Issuer Identifier https://self-issued.me.
The messages used to communicate with Self-Issued OPs are mostly the same as those used to communicate with other OPs. Specifications for the few additional parameters used and for the values of some parameters in the Self-Issued case are defined in this section.

Kantara

Consent & Information Sharing Work Group

https://kantarainitiative.org/groups/ciswg/
Project VRM and other related parties wish to build a framework around which a new type of personal information can be enabled to flow, and in doing so improve the relationship between demand and supply. Our contention is that when individuals are forced to sign organization-centric privacy policies/ terms of use then this places limitations on the information that will be shared. If such constraints were removed, and capabilities built on the side of the individual, then new, rich information will flow – including actual demand data (as opposed to derived/ predicted demand). The goal of this working group is to identify and document the use cases and scenarios that illustrate the various sub-sets of user driven information, the benefits therein, and specify the policy and technology enablers that should be put in place to enable this information to flow.

Consent Management

https://kantarainitiative.org/confluence/display/consentmanagement/WG+-+Consent+Management+Solutions+Home - Consent Management Solutions are used to manage the full lifecycle of an individual's consent for the processing of their personal data. That consent needs to be: freely given, specific, informed and unambiguous.

Consent Receipt Standard

https://kantarainitiative.org/confluence/display/infosharing/Consent+Receipt+Specification
A Consent Receipt is record of authority granted by a Personally Identifiable Information (PII) Principal to a PII Controller for processing of the Principal's PII. The record of consent is human-readable and can be represented as standard JSON. This specification defines the requirements for the creation of a consent record and the provision of a human-readable receipt. The standard includes requirements for links to existing privacy notices & policies as well as a description of what information has been or will be collected, the purposes for that collection as well as relevant information about how that information will be used or

disclosed. This specification is based on current privacy and data protection principles as set out in various data protection laws, regulations and international standards.

IEEE Blockchain for Healthcare https://transmitter.ieee.org/blockchain-in-healthcare/

IEEE Data Governance 7000 series

P7002 Data Privacy Process

https://standards.ieee.org/project/7002.html

This standard defines requirements for a systems/software engineering process for privacy oriented considerations regarding products, services, and systems utilizing employee, customer or other external user's personal data. It extends across the life cycle from policy through development, quality assurance, and value realization. It includes a use case and data model (including metadata). It applies to organizations and projects that are developing and deploying products, systems, processes, and applications that involve personal information. By providing specific procedures, diagrams, and checklists, users of this standard will be able to perform a conformity assessment on their specific privacy practices. Privacy impact assessments (PIAs) are described as a tool for both identifying where privacy controls and measures are needed and for confirming they are in place.

P7004 Child and Student Data Governance

https://standards.ieee.org/project/7004.html

The standard defines specific methodologies to help users certify how they approach accessing, collecting, storing, utilizing, sharing, and destroying child and student data. The standard provides specific metrics and conformance criteria regarding these types of uses from trusted global partners and how vendors and educational institutions can meet them.

P7005 Employment

https://standards.ieee.org/project/7005.html

The standard defines specific methodologies to help employers to certify how they approach accessing, collecting, storing, utilizing, sharing, and destroying employee data. The standard provides specific metrics and conformance criteria regarding these types of uses from trusted global partners and how vendors and employers can meet them.

P7006 Personal Data AI Agent

https://standards.ieee.org/project/7006.html - This standard describes the technical elements required to create and grant access to a personalized Artificial Intelligence (AI) that will comprise inputs, learning, ethics, rules and values controlled by individuals.

P7012 Machine Readable Privacy Terms

https://standards.ieee.org/project/7012.html

The standard identifies/addresses the manner in which personal privacy terms are proffered and how they can be read and agreed to by machines.

ISO

TC 307 Blockchain Process Policy

- Blockchain and distributed ledger technologies -- Terminology
- Blockchain and distributed ledger technologies -- Privacy and personally identifiable information protection considerations
- Blockchain and distributed ledger technologies -- Security risks, threats and vulnerabilities
- Blockchain and distributed ledger technologies -- Overview of identity management using blockchain and distributed ledger technologies

Other Things

JLINC (JSON-LD Link Contracts) for Data Sharing Governance

https://jlinc.org - The protocol is open (anyone can use it) but it is not at a standards body.
JLINC is an open protocol for sharing data protected by an agreement on the terms under which the data is being shared. The agreement is known as an Information Sharing Agreement, and can be a reference to a standardized agreement (a Standard Information Sharing Agreement or SISA) or a one-off specialized contract. The base profile is HTTP-based, but any protocol that affords methods for initiating and responding to data transactions, along with metadata (headers) accompanying those interactions could be adapted.

NIST 800-63-3
ERC 725
FIDO

Then we organized it into a map of where the different groups and their work fit in a map of the ecosystem.

Events:
Interop-a-thon proposed
Internet Identity Workshop
MyData
Rebooting Web of Trust

We also named many companies in the space.

Transmute	digi.me
Veres One	*Inonyom*
Trusted Key	*Sphere Identity*
Ockam	*SelfKey*
Consensus	*CULedger*
Sovrin	*BCGov*
Jolocom	*Blockstack*
Civic	*Inrupt*
Bloom	*Lifescope*
Yubico	*Evernym*

Map of the Agents and Hubs

Common amongst all of them are these things

DID Communication
* Base Encryption (Wallet People Port Civic)
* Message Typing
* Routing
* Alignment w/ crypto key types (secret management)

Increase compatibility in future w/o hair pulling in the future.

Things in play in decentralized web land include the
Fediverse https://fediverse.party
Activity Streams - https://www.w3.org/TR/activitystreams-core/

Agents

based on ARIES at Hyperledger
    * Key Management
    * Credentials
    * Protocol Support
https://wiki.hyperledger.org/display/ARIES/Hyperledger+AriesIM

Projects/Companies based on Aries
* IDRamp - https://idramp.com
* Mattr (SparkNZ) - http://www.sparknz.co.nz/
* StreetCred
* connect.me http://www.connect.me
* T-Mobile (Axel)
* Germen Credentials @University
* NL Bank Consortium
* BlockPass - https://blockpass.org
* Some Banks are folding into existing applications
* IBM - https://www.ibm.com/blockchain/solutions/identity
* ATT

HUBS

Personal Data Stores
    * Can store encrypted things at Rest
    * Actions -> Meta Protocol
    * Synchronization between Hubs
MSFT and WorkDay

Other Projects

Transmute - Workflows approach - https://www.transmute.industries

digi.me waiting for the - https://digi.me

LifeScope - SOLID - https://lifescope.io - https://solid.inrupt.com

3Box [Ethereum] - https://medium.com/uport/announcing-3box-and-ethereum-profiles-dba9841e0952

Privony - Michael Becker's Company - https://privowny.com
HIEofOne -http://hieofone.org
Wault for Health - https://wault.wymsical.com
Blockstack - https://blockstack.org

* PICO Labs aligned with ARIES - https://picolabs.atlassian.net

WALLETS

** narrowly defined around holding credentials*

uPort - https://www.uport.me
Civic - https://www.civic.com
JoloCom - https://jolocom.io
BlockchainCommons key recovery airgap- https://www.blockchaincommons.com
Sphere - https://www.sphereidentity.com
VeresOne Web Profile - https://veres.one

Just Crypto
* *electron*
* *Pillare*

Data Fiduciaries FTW

Wednesday 7M
Convener: Joe Andrieu
Notes-taker(s): Ben Gregori & Joe Andrieu

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

2. Notes received from Ben Gregori:

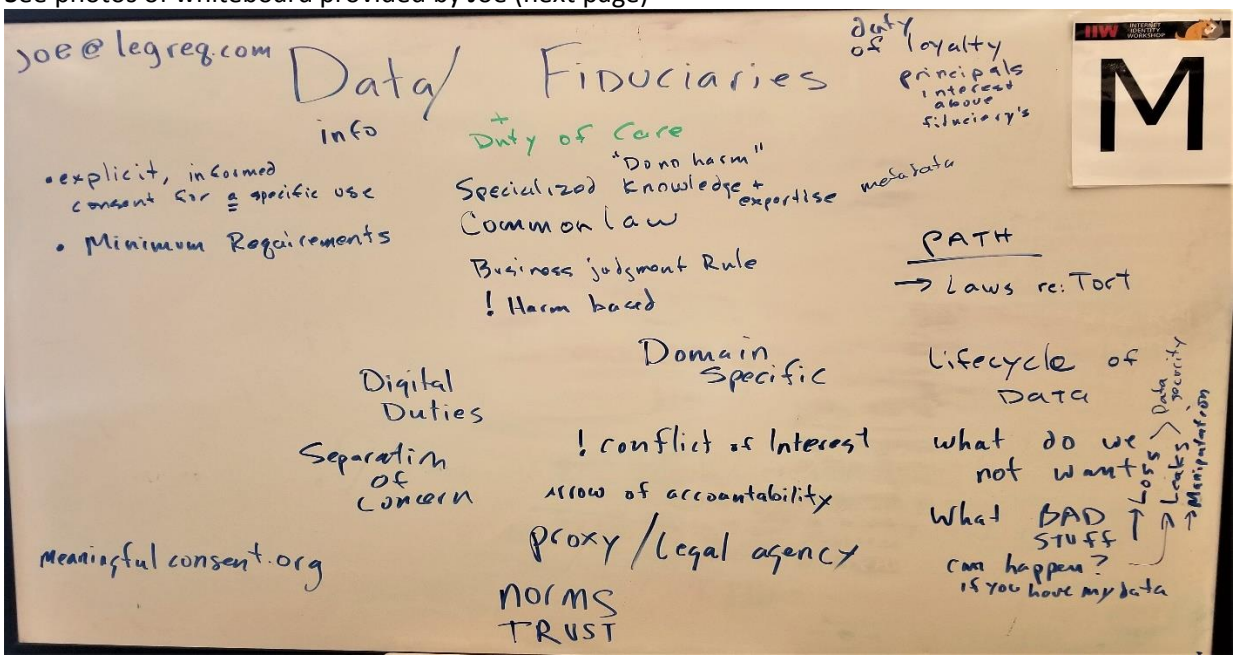
Joe@legreg.com
Explicit, informed, consent for a specific use
Minimum requirement
Meaningfulconsent.org
Trust is Domain specific – how does this translate to the digital realm? (I trust my accountant differently than my babysitter).
Derives from Common Law
"Do No Harm", Duty of Loyalty, principals interest above fiduciaries
********** ********** **********

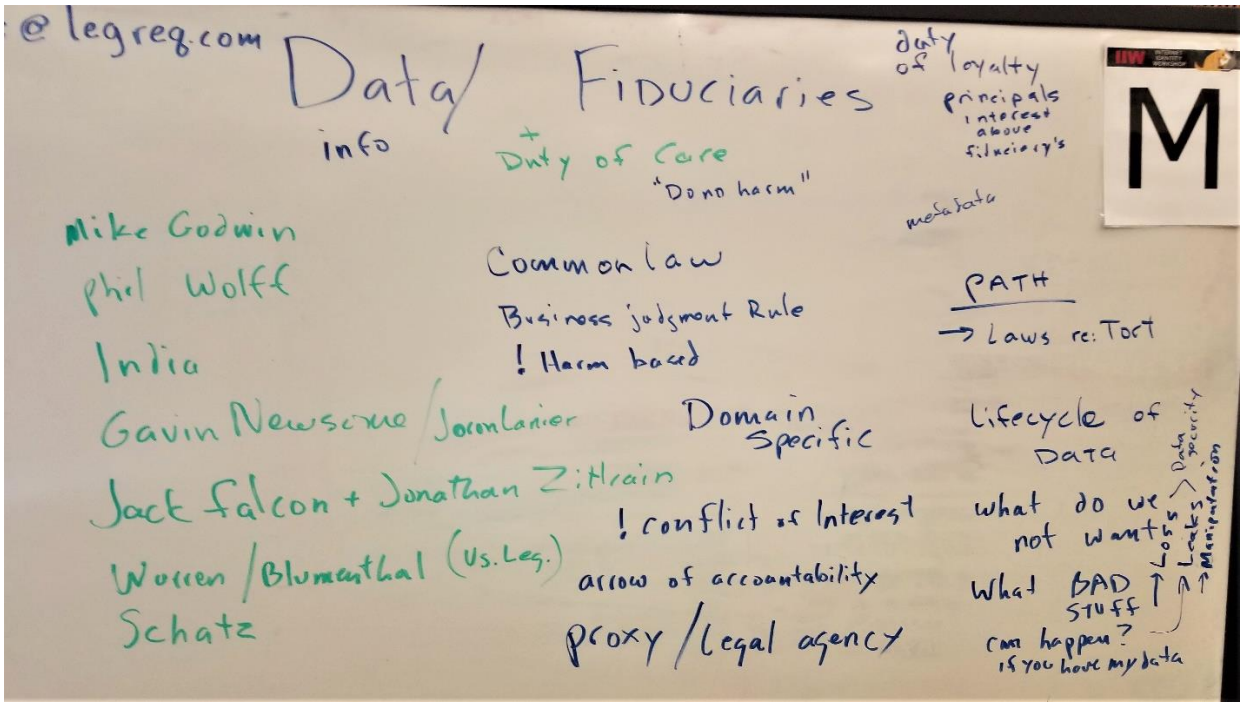
3. Notes & photos received from Joe Andrieu:

Url/link to white paper by Chris Savage:

https://law.stanford.edu/publications/managing-the-ambient-trust-commons-the-economics-of-online-consumer-information-privacy/

See photos of whiteboard provided by Joe (next page)





Street Cred: Indy Catalyst Agent & Agent Framework What Are They? How You Can Issue/Hold/Verify Credentials Easily

Wednesday 8B
Convener: Nicholas Rempel, Andrew Whitehead, & Tomislave Markovski
Notes-taker(s): Nicholas Rempel

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

A joint session with Nick Rempel/Andrew Whitehead from BC Gov (Indy Catalyst Agent) and Tomislav Markovski from Streetcred ID (Agent Framework)

Indy Catalyst Agent (Nick/Andrew – BC Gov):
What is it? How you can install it and issue, hold, and verify credentials today.
slides:
https://docs.google.com/presentation/d/12SY33tfD0R_33SEx6T6JxtOT6NBID03wsqiMnvDp8ic/edit?usp=sharing

Agent Framework (Tomislav Markovski – Streetcred ID)
Architecture overview and how to use it to create agents.
slides: https://drive.google.com/file/d/1HDc_OBbT-0ggGFhyqqmw3TALrxI0K51c/view?usp=sharing
Further reading: iiw.vonx.io / agentbook.vonx.io / vonx.io
OPEN SOURCE!
https://github.com/bcgov/indy-catalyst
https://github.com/streetcred-id/agent-framework

Product Mapping Needs: User, Admin., Compliance, Exec.

Wednesday 8C
Convener: Kurt Milne
Notes-taker(s): Kurt Milne

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

Small group discussion about what changes as we move from federated to self sovereign frameworks.

Helen from Soverin Foundation led primer. Thank you!

Check out book Complete Guide to Self Sovereign Identity: By Heather Vescent and Kaliya Young.

OAuth 2.0 From Single Page Application Assisted Token

Wednesday 8D
Convener: Daniel Lindau
Notes-taker(s): Mark Dobrinic

Tags for the session – technology discussed/ideas considered: OAuth, Single Page Applications, Assisted Token flow

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

Recently Implicit Flow was deprecated, what should be next. Instead of forcing a SPA into the code flow, the "assisted token flow" draft describes how that could solved with a new flow.

It is based on a new endpoint, /assisted-token.
On this endpoint, the client can be even more simple than with implicit flow.

Upon initiating the flow, the AS returns a document that uses JavaScript postMessage to follow up whether the user needs to be authenticated.

Noted that this could be vulnerable for phishing attack.

The result is that the AS returns a page in the IFRAME that post back the access token to the framer through a JavaScript postMessage.

The AS serves up all the library code to perform the assisted token flow, which does not involve the client to invent this.

The token is issue from the /assisted-token endpoint, and not from the /token endpoint.

The client needs to identify, so the AS can respond with pages that are protected to be served under known client domains.

The assisted token flow only specifies how to get a token; it's up to the app to use it for requests to the Resource Server.

Storing the Access Token in a cookie helps protect it after the SPA receives it.

Suggested benefits
- No need for CORS on the token endpoint (reduces complexity)
- The implementation is provided fully by the AS (hidden from the client)

Ease of use is the goal, in particular ease of use for client developers.

Valuable take-aways:
- provides good libraries
- provides a flow without redirections
Some concern: how can this approach be generified? It's not a general solution as it is.

Then again: it doesn't necessarily needs to be generic.

Make sure to relate this draft to OIDC's Session Management spec.

Considering the opinion to prefer adding the complexity to the token endpoint, not to have to expose a new endpoint.

Post the link of the draft to the OAuth list again:

User Interaction needs to be in a pop up, so postMessage can still reach the opener-frame.

Also see old spec: webmessage post back response mode.

Be careful: prefer not to open AS in an iframe ever.

Anonymous Saliva DNA Extraction Kit using Block Chain

Wednesday 8E
Convener: Daniel Uribe
Notes-taker(s): Daniel Uribe

Tags for the session - technology discussed/ideas considered:

#Blockchain #genomics #privacy #gdpr #dnawallet #non-fungible-tokens #CPPA

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

Discussion:
How to pair a Saliva DNA extraction kit with a Public Address in a Blockchain to serve as a pointer to an encrypted private data container (IPFS) so the user can access/buy sequencing laboratory services without risking their identity. The DNA Lab, after processing the saliva sample, can deposit the "Raw Data" to each user's DNA Wallet within the Network. Blockchain is utilize to issue smart contracts for each transaction to represent the "informed consent" or the "permissioned region of the genomic map" that each 3rd party can access/see/download/process etc. (P2P Genomic Firewall).

Key Understanding: Distributed Storage, Non-fungible-Tokens (for personal genomic variants), ERC-721, Smart Contracts, Privacy over IP, Dynamic Permissioned data vs. static informed consent, P2P Genomic Firewall).

Action Items: Solve Private Keys custody for non-technical users (most of all) to increase adoption.
Next Steps: Pilot program 100 users.
URL PPT: https://www.dropbox.com/s/v0fepme3jaodkf5/presentaci%C3%B3n.pdf?dl=0
URL Video: https://vimeo.com/297883843

Privacy Chain Overview & Update

Wednesday 8F
Convener: Wendell Baker
Notes-taker(s): Wendell Baker & Michael Becker

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

1. **Notes received from Wendell Baker:**

   IAB Privacy Chain Working Group – link to presentation:
   https://docs.google.com/presentation/d/14op9-wsNqXOvZt65PrVs_-kgoKvzbGaZAzhDoWzVi5c/edit?ts=5cccbc5d#slide=id.p

2. **Notes received from Michael Becker:**

   Michael Plumber @GroupM is leading commercial end of the PrivacyChain discussion,

   Wendell Baker @Verison is spearheading tech discussion (note: Verizon has its own implementation to manage consent receipts for over 20 million consumers; however, it is also supporting the development of an interoperable standard so that consent receipts can work across companies.)

   We discussed the IAB Privacy Chain, a blockchain-based protocol and 'system of record' that allows companies to track users' privacy consents across complex data supply chains. IAB released the protocol Oct. 2, 2018.

   According to the IAB "PrivacyChain was designed to solve for a major industry problem: as the data ecosystem has fragmented and companies collect or update hundreds of millions of consents a year, it has become incredibly difficult to ensure that all members of a data supply chain have the most current consents. The protocol will allow companies to more easily manage and control how they handle and share users' personal data, while providing users control over opt-in and opt-out."

   See IAB Release, https://www.exchangewire.com/blog/2018/10/05/iab-tech-lab-releases-privacy-chain-for-public-comment-interbrand-releases-2018-best-global-brands-report/

   The PrivacyChain code is on GitHub, https://github.com/InteractiveAdvertisingBureau/PrivacyChain

   Similar topic, IAB Transparency and Consent Framework (TCF),
   see https://iabtechlab.com/standards/gdpr-transparency-and-consent-framework/.

   IAB has had success in development these type of standards, e.g. IAB Open RTB Standard.

   Challenge

   * It is difficult for publishers to manage consent receipts; ideally find some standardization amongst CMPs.
   * Manage legitimate interests for access to data
   * Solicit and manage positive consent and identifiers across companies that can be verified and

audited

* Managing different tracker methods: cookies, Digiturst IDs, IDFA, GPSAID, Universal Id
* Develop standardized agreements across verticals
* Industry needs organization to run the hyperrledger to mange consents
* Addressing fraud issues (Brands lose $6~$19B lost every year to ad fraud)
* Understand business model - how much would a brand pay for consent compliant traffic

Other Consent Receipt Frameworks

- Kantra
- JLINC
- Other CMPs, consent management platforms

PrivacyChain to role out in phases - V1: Consent, V2: handle context and data attributes; key features: Write consent, verify consent, revoke consent.

User visits publisher site, provides consent>>Publisher SSP (Supply Side Platform) signals that it has audience member that has given consent, places "receipt" in hyprledger<>Brand/Agency DSP (Demand Side Platform) checks PrivacyChain to verify const consents, if there is consent bids on ad and delivers content.

Initially there is no plan to integrate PrivacyChain with personal data stores; would be useful to discuss how personal data stores play in this process so that individuals can also have a record of their consent.

"Hey Kids, Let's Build a Trustworthy, Decentralized, User-Focused Web Ecosystem!"

Wednesday 8G
Convener: Richard Whitt
Notes-taker(s): Richard Whitt

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

Building an ecosystem that incorporates SSI and other user-empowering technology concepts

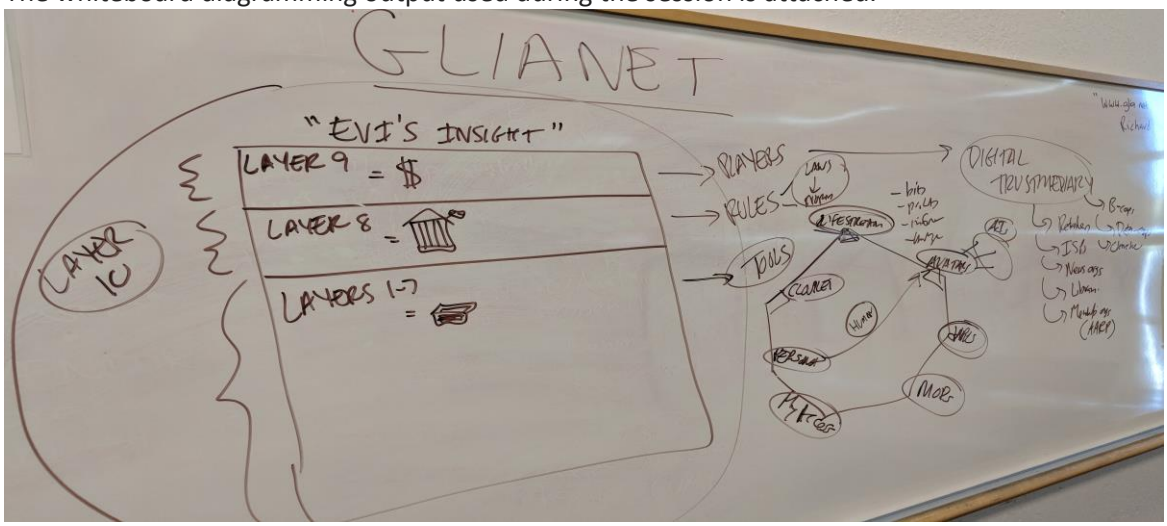
The session revolved around GLIAnet, a project (www.glia.net) being run by Richard Whitt in his capacity as fellow at the Mozilla Foundation. The premise of the project is that the current Web ecosystem is plagued by deficits of trust, accountability, and user control, and nothing short of a new cross-functional, cross-sectoral organizing approach is necessary. The GLIAnet ecosystem was discussed, centering on a modified version of the OSI stack as inspired by software engineer Evi Nemeth: Layers 1-7 (Code, or tech), Layers 8 (Players, or money), Layer 9 (Rules, or politics) and Layer 10 (Humanity, or all of us). In each of those

Code/Players/Rules/Humanity layers, concerted action is both possible and necessary to drive real societal change.

Discussion focused on the seven proposed technology layers of the GLIAnet ecosystem: data "lifestreams," personal AI "avatars," self-sovereign identity "personas," localized "cloudlets," decentralized "dApps," modular owned devices "MODs," and personal "MyAccess."

The participants voiced general agreement with the diagnosis, and the proposed remedies, while providing useful input on the feasibility of various options. Several noted that the ME2B movement, and the digi.me online platform, are two examples of particularly good fits to the "big tent" approach being proposed for GLIAnet.

The whiteboard diagramming output used during the session is attached.



Where have all the Trust Frameworks gone?

Wednesday 8H
Convener(s): Don Thibeau, Andrew Hughes, Bjorn Hjelm
Notes-taker(s): Karyl Fowler (Transmute) & Thomas Berry

Tags for the session - technology discussed/ideas considered:

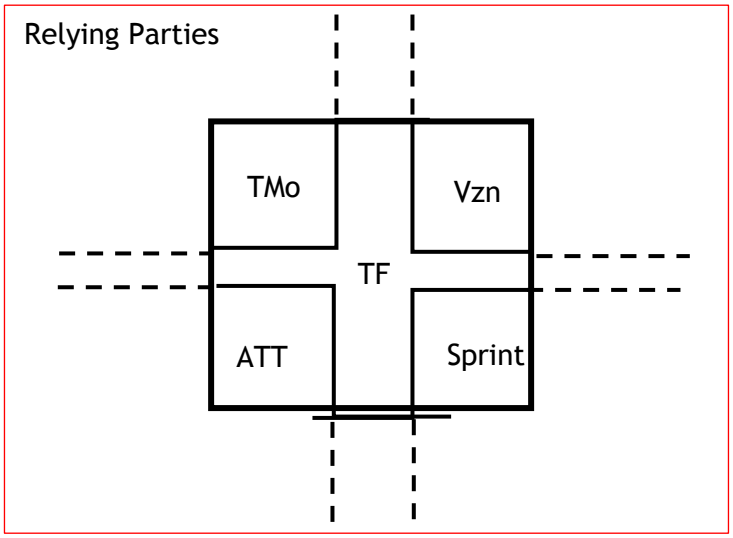
Trust frameworks, multi-party contracts, relying parties, spectrum of verification

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

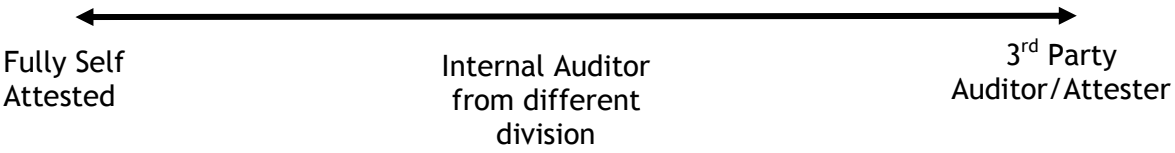
1. **Notes received from Karyl Flower:**

- Primary Use Case explored: Project Verify: telcos (Verizon, TMobile, AT&T, etc.) are considering entering a trust framework with each other.
    - Starting Hypothesis: this type of agreement can *only* be done with a trust framework
- Starting point for discussion: What is the burning business problem "trust frameworks" solve?
    - Answer: Businesses should implement trust frameworks because they:
        - Are more scalable, multiparty agreements
        - Risk Mitigation
        - Cost (reduction/efficiency/etc.)
        - Brand: Market Differentiator, unlocks new business models/opportunities/unique services, reduces time to market
- Today we have 3 ways to do business/interact:
    - 1 – bilateral contracts
        - most used today but not scalable
    - 2 – Loosely coupled SLAs
        - good when companies want to agree to keep operating at the "status quo" without bilateral/formalized contracts
        - Don't clearly assign liabilities
    - 3 - Trust Frameworks
        - Multiparty agreements/contracts that specify:
            - Technical standards [compatibility/interoperability]
            - Legal responsibilities and liabilities
                - "we can't operate efficiently without clear liabilities"
            - Level of performance commitment and accountability
                - Including what can and cannot be done (for example how data can and cannot be used)
            - Risk-based [in most cases]
                - Where do you want the risk?
            - Way more scalable

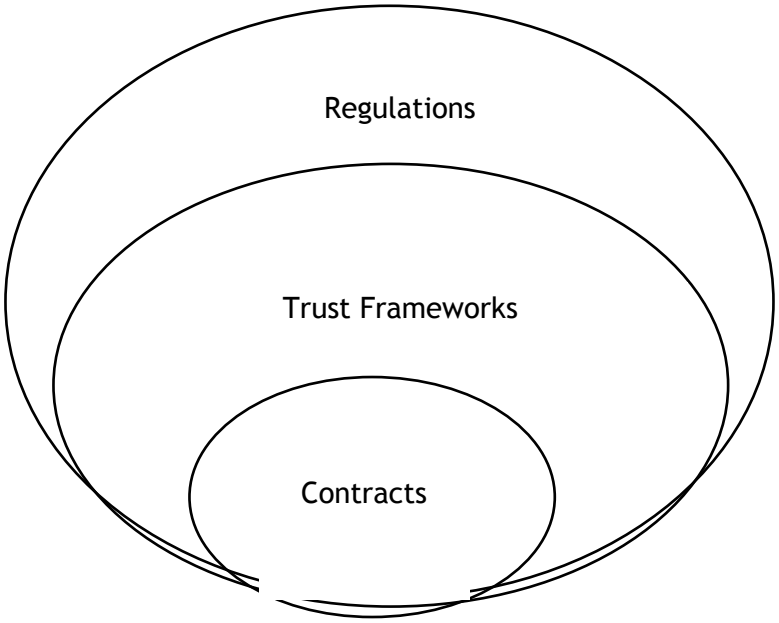
- In order to enter/establish and implement a trust framework:
    - Companies "must agree on trust attributes, including measures of security, performance guarantees, etc.
        - Includes defining the criteria for what everyone should expect these attributes to be, on what level and how to enforce or certify compliance [with a third party or self-certify as an alternative]
    - Companies also must identify relying parties [like banks in the case of the telco use case]
        - Determine a way to standardize criteria here too
        - Relying parties benefit/are more likely to engage just knowing that a trust framework is in place
- "Trust but Verify" conundrum:
    - "sales talk" often is not or cannot be held accountable for assertions, so how do we reduce the risk that they are not lying (ex telco commits to one level of performance, but sales reps are communicating something else, etc.)
- Auditors ARE attesters:
    - Hey take the risk of public verification of XYZ (e.g. companies complying with a standard or trust framework)
    - They don't dictate *how* companies comply – just verify what you are complying with and whether you are compliant
        - Some trust frameworks can help companies standardize how they are complying, like Kantara Trust Framework makes NIST assessment criteria more tangible
- ASSERTION RISK:
    - Companies take this risk in claiming compliance "referential trust"; an auditor verifies this claim
    - Quality assurance is the result
- There are only 7 "web of trust" auditors globally
- Whether a 3rd party [like an auditor] is required to interpret our contract and attest to compliance after signing depends on the levels of risk involved
    - For example, if I require all of my cloud vendors be ISO 2701 compliant, I can check myself [perhaps in the ISO registry] to verify whether they are ISO certified
- Project Verify Trust Framework (TF):



- Spectrum of "Trust but Verify":



- Relying Parties (like banks) want to know that telcos are all complying with the same thing; often RPs dictate acceptable certifications
- Relying Parties (RPs) get these unique things from a trust framework:
  - Risk reduction
  - Unique Services
  - Reduced time to mkt/market defense [depends on other variables too]
  - Reduced costs
- Trust Frameworks can enable/allow for greater participation
- Trust Frameworks can be ***proof points***
- Purchasers have ultimate power to dictate requirements
- Regulations can be [and often are] part of trust frameworks
- Law:
  - Private Law: contracts [live within public]
  - Public Law: regulations
  - Mere compliance with the law isn't a trust framework



- **Group point of debate: what is the longevity of trust frameworks?**

********** ********** **********

2. **<u>Notes received from Thomas Berry:</u>**

Business Trust Framework is trying to solve

If one wants to federate or interoperate with a diverse class of partners

- bi-lateral contract
    - Everyone understands them and uses them every day
- loosely coupled SLA
    - No need for contractual relationship, but provides an understanding/relationship-framework
- trust framework
    - Contractual; multi-party contract
    - Sum of two parts
        - Technical requirements of inter operation
        - Legal responsibilities
            - What are the standards each party must be compatible
            - What are the legal requirements for the business relationship
        - Commentary:
            - Not purely legal

What do you expect the trust attributes to be (that can be used for auditing)? Examples

- Sovereign foundation is going to have self-assertion to demonstrate compliance
- CA Browser uses a framework for compliance

Is there a way to define the role and expectation in a common way to address security and privacy of data/users in the various sectors a relying party (RP) would operate.

Needs to describe to other relying parties the standards that you intend to meet.
Trust Framework is needed to foster a two-way trust
TF should address what you're entrusting the party with (accountability of the trust relationship)

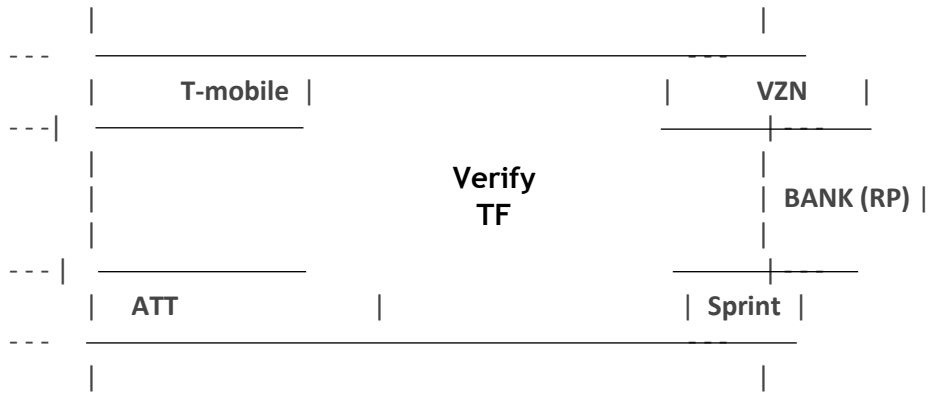
Trust, but verify

- Self-certification is an oxymoron; lowest level of risk mitigation
  - Sales talk isn't necessarily beholden to accountability
- Trusted party needs to take a public statement of compliance
  - Attestation is needed to verify the party is meeting obligations/expectations
- What is the value of the interoperability; auditors are not needed on every aspect
- Trust Framework must have an accreditation program if level of assurance established by trust is necessary to support the trust.

Within the TF here's what I expect to do and here are the rules

- Instead, just send out the requirements
- Attestation comes in that the requirements map to the parties processes and compliances
- Assessment criteria can be common

Use Case



The parties may be operating outside the framework

Trust Framework: Multi-Party Contract
- Trust Framework is contractual [private law that lives within public law]

What are the technical requirements to be a member of the "TF club"?

- all parties agree to be audited for trust-worthiness by independent audit
- Internal auditors are required to meet certain standards
  - Internal auditors can be held liable for not meeting those standards

TF

- risk mitigation
- $$
- Brand reliability/Market differentiator

RP

- Risk reduction
- Unique services/data coverage
  - Ability to ubiquitously trust in service players
- Time to market
- Cost

Any contract must be legally conforming

- compliance to the law
- Private, public, and regulatory
- The contract will be lawful

Relying Party Compliance/Governance should drive utilization of trust framework

Continuous Access Evaluation Protocol (CAEP)

Wednesday 8I
Convener: Atul Tulshibagwale
Notes-taker(s): Jordan Wright & Atul Tulshibagwale

Tags for the session - technology discussed/ideas considered: Taxonomies, Semantic Interoperability, labels, international standards

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

1. **Received from Atul Tulshibagwale:**
   Here is the link to the slides from the presentation:
   https://drive.google.com/file/d/11ZhOWmDmLfSS1UURBL89KCA8c93vNYeN/view?usp=sharing

   ********** ********** ********** **********

2. **Notes received from Jordan Wright:**

   Agenda
   - What is continuous access evaluation
   - Why is it needed
   - How does it work

   What is CAE
   Continuous Access and Evaluation allows independent organizations to react quickly to changes in information related to shared user sessions, including:
   - Access context (IP, GEO, device posture)
   - Device and app health
   - Updated authorization decisions based on internal and external updates

The idea is to create a standard to make this easier, especially to support interoperability between multiple parties.

Why now?

- The Zero Trust Networking (ZTN) model makes endpoints the weakest link
    - The endpoint becomes more important from an attack point-of-view.
- Mobility adding opportunities for compromise
    - For mobile devices, sessions can last for a long time, so reevaluating it regularly can be beneficial.
- Standard drives interoperability between independent parties
    - Each service need not integrate with each identity or device management provider

Use Cases

- IP/Geo location based access re-evaluation (public location, untrusted geo)
- Sensitive content
    - Maybe access should be cut off when the user is in a public location
- App vulnerability
- Suspicious user activity
- Helping security of long-lived sessions

Discussion Question: "Who determines suspicious activity"

An example may be an endpoint security program which may
May also be a CASB, firewall, basically anything has the ability to identify suspicious information and relay that information to other parties.

Architectural Model

[See Attachment]

The Relying Parties can receive updates from policy service providers via an asynchronous pub/sub interface.

The two areas CAEP is interested in is:

- Express Context updates
- Evaluation of updates

Protocol Messages

- Based on SET's (RFC 8417)
- Subject identifiers include
    - User session (SAML Request Id or OIDC token)
    - Certificate serial or hash
    - Device identifier

- Events include
    - Context update
        - This user moved IP addresses
    - Device update
        - The device status is now rooted, or has malware
    - App update
        - The properties of the application have changed (e.g. a vulnerability in the app was discovered)
- Session authorization update
    - The user's role has changed, or the user needs re-authorization

Protocol Methods

- Single endpoint at each party used for all protocol messages
- Receive expression of interest
- Receive updates

- TLS mutual auth - SETs not signed
- HTTP POST - express interest
- PATCH - provide an update
    - SET
- PATCH response type depends on expectation

Discussion: There may be multiple parties involved besides an IDP or SP.
We're not trying to restrict who can generate events. For example, the IDP can express interest to other providers to receive updates.

Question: When you say both parties have to stand up an endpoint, are both parties clients to each other?
This is a server-to-server protocol. We're not imagining this to be used by clients. Each element has the ability to publish events as well as take action based on its position in the network.

Trust is established via mTLS between the peers in the network.

Event types themselves are not in the scope of CAEP interaction.

Question: Does CAEP try to solve the problem of: you're willing to let the user browse the website without having a high-level of faith that they are who they are, and building trust over time?

This can be done by expressing interest in various providers. "Tell me if this user changes aspects of their session" This spec isn't handling session confidence.

There was a discussion that we may define a minimal set of SET's.

Question: Who is responsible for managing the pub/sub queues?

Not talking about subscribing to a topic. Instead, you have an expression of interest via a HTTP post between peers. I tell IDP I'm interested in a session (the topic) and that's what determines.

Question: How much overlap is there with RISC?
RISC is geared towards events, while this is more people involved and more data vs. events. Consideration to review IFMAP and others to see if there's overlap.

Action Item: Work with RISC group to determine how we can best collaborate, if at all.

Question: Is this an alternative to the OpenID Session Management Protocol?
There is a backchannel, but openid doesn't do anything other than lock them out. This is a more nuanced aspect of changing session state.

Idea: It may be useful to separate the event document vs. the transport.

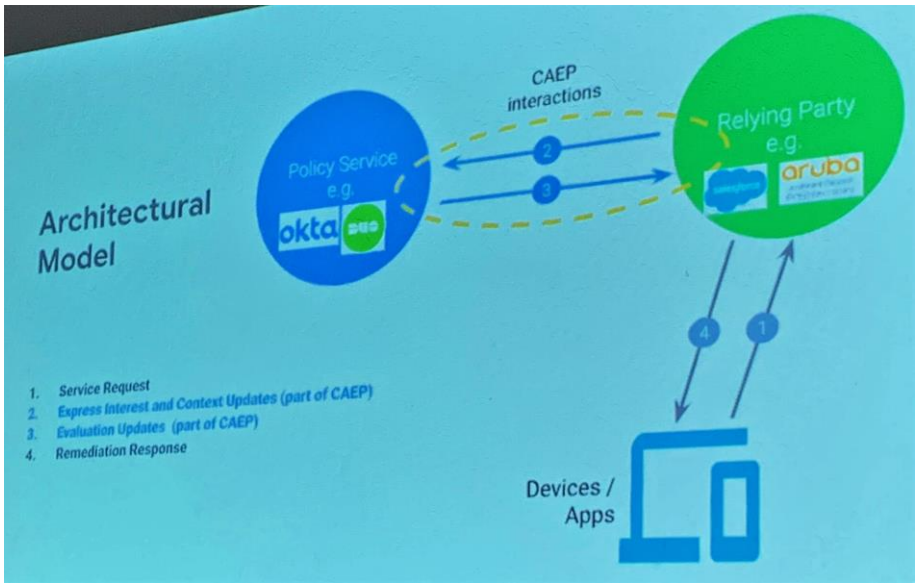
Idea: Instead of expressing interest to terminate the session, you could express interest to continue the session.

Here, we're just saying you're interested in the session. In an environment where I'm the IDP, depending on how you manage tokens, you may have no clue the user is logged in to a Relying Party. This isn't a standard for that problem.

Question: Should we have some kind of a heartbeat?
What you could do is use the expression of interest and get an OK (repeatedly).

Action Items

- Decided this is worth considering as a standard
- Will set up a mailing list to discuss next steps
- Will work with RISC group to determine how we can best collaborate, if at all.



Taxonomy and Digital Identities

Wednesday 8J
Convener: Jim Wowchuk
Notes-taker(s): Nicholas Racz & Jim Wowchuck

Tags for the session - technology discussed/ideas considered: Taxonomies, Semantic Interoperability, labels, international standards

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

1. **Notes by Nicholas Racz:**

   Jim Wowchuk unfurled the necessity of taxonomic definitions and having semantic interoperability between different representations of similar data ('date of birth' vs birthdate)

   Theoretical: We elaborated on a hierarchical taxonomy of a user and had active discussion over its implementation.

   Action item: Suggestions on who or what organization would be best to establish an initial set of tags. Considered ISO, IETF, W3C, OECD, etc.

2. **Presentation link provided by Jim Wowchuck:**
   Link to a shortened version: https://bit.ly/2DYuduc

   The long version can be found at:
   https://vanguard2018-my.sharepoint.com/:p:/g/personal/jwow_vcs_com_au/ETimta7svhJFjj5J4POx4tYBYtCI3PpCHti8C2a1afxBiA?e=01IotH

Verifiable Credentials Q and A?

Wednesday 8K
Convener: Paul Dietrich
Notes-taker(s): Paul Dietrich

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

Dan Burnett and Stephen Curran (Indy community) joined to answer our questions.

VC was written without requiring DIDs. Why. What are the intended applications? Claims issued by domains about other domains?

DIDs were actually spawned out of the VC work. VC does not define identity or identity systems. They are really about a set of claims provided together about an identifier.

Generally we can think of VC as signed authenticated data that can be shared between parties and clearly identify the issuer of the credential.

VC verify the issuance of the claim, not the truth of the claim.

DIDs arose out of this work in the following. When trying to define the identifiers required for VC, they looked at email, domain name etc. it became clear that there wasn't an identifier that could not be taken away.

When I receive a credential from an issuer using DID1 and share that to a verifier using DID2. How does the verifier connect that DID1 and DID2 are the same entity.

Stephen — In the indy hyper ledger work this is called blinded link secret in Indy terminology. Its a piece data derived from a holder private key.

Or what going into credential is the public DID of the holder. (Indy does not do this).

VC spec has a place to say there is a subset to the claim. Credential Subject: ID is the ID of the subject.

The blinded secret replaces the ID in the subject identifier.

When presenting a credential (a set of claims). indy has selective disclosure where you report only some of the claims in a credential.

There are quite a few places in the draft that leave options to remove stuff like ZKP etc. Can you explain?

This is for the standard development process. If they are not absolutely sure that they will get full testing support for the features, they mark it as such so they don't have to repeat steps in the standards process to remove.

Can you share some future expectations on revocation? Is it expected that the verifier? It seems like the burden is on the verifier to check for revocation and on the issuer to post revocation?

(Further Notes lost due to dead laptop battery).

How Can We Detach Users From Centralized Social Media?

Wednesday 8L
Convener: Matt Vogel (@yadablokchain) (yadacoin.io)
Notes-taker(s): Cameron Boozarjomehri (@cboozar)

Tags for the session – technology discussed/ideas considered:

- Social Media
- Decentralized Technology
- Decentralized Identity
- Identity vs Pseudo Anonimity

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

- What is "Social media" Beyond the great data powerhouse (Facebook, twitter, etc)
    - A space for interaction and sharing that is as close to real world interaction as possible
    - This includes the opportunity to interact "without identity" that we don't always know or need to know whose we are talking to
    - The need to move away from algorithms for something more "organic"
    - Penetrating "Walled gardens" for a distributed share everywhere ecosystem
        - Comparison of most natural to most curated (In Person -> Text -> email -> Facebook)
        - It is important to understand there is a "cost" to sharing
            - Social costs
            - Economic costs
            - Interaction & attention
- What is "Decentralized Social Media"?
    - Moving away from centralized content moderation to a more adhoc community approach
    - Moving toward freely shared content and "organic engagement"
- Moderation should be incentivized by the community in a bottom up approach
- Control of the interface and what is displayed should be a conversation between the individual and the organization
    - Social media moderation impacts how we experience
    - Context is critical to how a platform operates
        - Transparency is a product of an understood context
        - You must make it clear to any user why they are seeing what they are seeing either through notification or controls (both of which must be accessible)
        - Empower users by giving them control over how they consume content so that context becomes explicit

DID Communication Message (JWE Encryption)

Wednesday 8M
Convener: Kyle Den Hartog
Notes-taker(s): Kyle Den Hartog

Tags for the session - technology discussed/ideas considered: DIDComms, encryption

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

This is the current format that is used to handle encryption with a standardized serialization format that is similar to JWEs.
We also discussed:

- what it would take to get this fully JWE compliant.
- what we need to do in the future to improve this cryptographically as well as reducing the size of messages by changing the serialization format using CBOR.

Link to resources from discussion:
https://github.com/hyperledger/indy-hipe/tree/master/text/0028-wire-message-format

Karma DID Method: Buddhist Approach to Identity

Wednesday Lunch Session
Convener: Heather Vescent
Notes-taker(s): Michael Becker

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

Team discussed the precepts of [Tibetan] Buddhism to see how it might align thoughts on Identity

Questions raised?

- If there is no persistent "I", what does this mean for Identity management? [There is no singular identity, it is all about context]
- What is identity?
  - Is an identity a construct of attributes? Some say no.
  - Is identity a collection of mapped experiences?
  - Is identity a collection of relationships? Should relationship be the first "class" object for identity?
- How does one define self? The I?
- Can views of class or attribute be used designate an identity
- Should identity primarily deal with [dynamic] relationships and not specific things?

The team discussed a number of identity thought experiments/frameworks

- Ship of Theseus, https://en.wikipedia.org/wiki/Ship_of_Theseus
- The Trade-Off: The Four Noble Truths and Five-fold Path to Digital Sovereignty, https://identitypraxis.com/2018/06/26/the-trade-off/
- The Five-fold path to digital sovereignty, https://identitypraxis.com/2019/04/27/youre-being-scored-what-it-means-for-your-privacy/
- Liebnets view of identity, two balls equally the same, same attributes? are the different balls? Is the only difference positioning?
- Alan Westin framework of Privacy
    - Privacy Fundamentalists; Privacy Pragmatics; Unconcerned
- Daniel Solove, Taxonomy of Privacy
- Becker 7 states of privacy awareness - unaware, helpless, indifferent, apathetic, impaired, empowered, enlightened
    - Comment: the emotional state one manifests is based in context

Domain-Specific: Governance Frameworks – What Are They & Why Might You Need One?

Wednesday Lunch
Convener: Drummond Reed, Chris Raczkowski & Soverin Gov Framework Work Group
Notes-taker(s): Drummond Reed

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

1. **Notes received from Drummond Reed:** Drummond Reed and Chris Raczkowski

   We had a small group meet over lunch to talk about domain-specific governance frameworks (DSGF). This is a term from the Sovrin Glossarythat refers to governance frameworks designed to define the "BLT sandwich" (business, legal, and technical policies) for a particular verifiable credential or family of verifiable credentials.

   We introduced the "SSI stack" defined in Appendix D of the Sovrin Glossary and explained how the Sovrin Governance Framework was a generalized SSI governance framework that laid the foundation for DSGFs. The concept of DSGFs is explained in more detail in Appendix H of the Sovrin Glossary.

   We then explained that the Sovrin Governance Framework Working Group is launching a new Task Force called the DSGF Task Force that will be producing a template for DSGF and a DSGF Author's Guide. It will also be coordinating work on several of the first DSGF including:
   - The CULedger MyCUID Governance Framework
   - The Truu Medical Credential Governance Framework
   - The DignifID Animal Guardianship Framework

Chris then explained the mission of DignifID to provide SSI for animals and pets and talked about the DignifID Animal Guardianship Framework. He introduced Andrew Rowan, former CEO of the Humane Society International, who is one of the principal advisors to DignifID on the development of the DignifID Animal Guardianship Framework.

We closed by inviting attendees or anyone interested to join the all-volunteer Sovrin Governance Framework Working Group (details are at the link).

Linked Secrets & ZKPs

Wednesday 9A
Convener: Rouven Heck
Notes-taker(s): Rouven Heck & Daniel Hardman

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

Notes from Daniel Hardman:

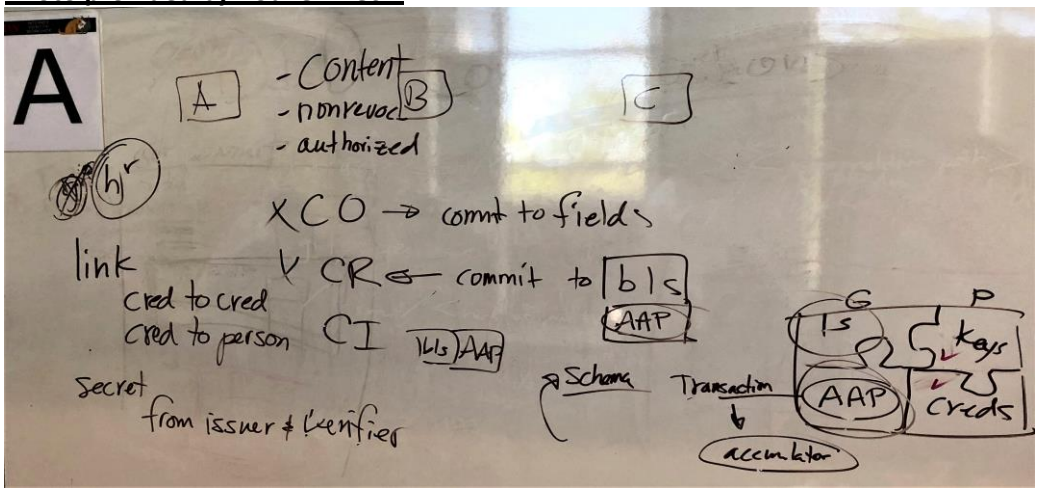
A general analysis of how Sovrin deals with the "what happens if I lose my phone" problem, which includes some references to this topic at about the same level of detail that we had during the session: https://sovrin.org/wp-content/uploads/2019/03/What-if-someone-steals-my-phone-110319.pdf

A deeper look at agent authorization policy (device revocation and related features) in the context of an overall DKMS strategy: https://bit.ly/dkms-v4

A general, no-math-intense explanation of cryptographic accumulators: https://github.com/hyperledger/indy-hipe/tree/master/text/0011-cred-revocation#background-cryptographic-accumulators

The crypto guys who can explain the math behind this mechanism and its more recent snarks impl include Mike Lodder (mike@sovrin.org) and Brent Zundel (brent.zundel@evernym.com)

Photo provided by Rouven Heck:



Women In Identity: Plans for 2019, How Do We Create Success?

Wednesday 9B
Convener: Pam Dingle
Notes-taker(s): Wendy Hanamura

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

1. **Notes received from Wendy Hanamura:** Attendance: 24 women, 2 men
   HISTORY: 2-3 years ago we founded Women in Identity. Global group.
   There are many Women in Tech groups, but few groups dedicated to mentoring each other within a sector. @WomeninID
   - Visibility is a core issue. How do we fix that?
   - How do we create a community so we know we aren't alone?

   Big learnings from previous conversations: Many women are not able to defend themselves. But when it comes to advocating for another woman, women will go to the mat for each other. One tactic for instance, instead of self-promotion, nominate another woman.
   Challenges:
   - Shared tools—shared repository and way to communicate. (Slack; Rocketchat)
   - Place to aggregate contacts;
   - place where people work together;
   - a safe place where we support each other; a place to vent about the bullshit in the industry
   - mentoring relationships;
   - networking for collaboration and opportunity
   - how do we get past the 5 women gatekeepers—their minds are the database
   - Can we make this not hierarchical
   - How do I know what it takes to build a protocol?
   - How do you get involved in a space if you are not technical
   - Making room and advocacy for non-white men & neural diversity & diverse body types

   MAIN GOALS for this Session:
   1. tell you how to join the Women in Identity group
   2. Share the website—how to contribute content; places to register if you want to speak at conferences;
   3. Create a listserv
   4. Create a requirements document for developing the website in the future
   5. Those who want to be on the volunteers list, let Pam know and she will add you

   IDEAS:
   1. How to build a cross-silo group
   2. How do we create mentors?
   3. Get the marketers, create resume-building positions;
   4. Co-present with other women to open doors

RESOURCES:

1. **Google Group**—womeninidentity.org
2. **Hyperledger Women** (Ambassadors) – NOTE: became primarily famous women who don't do much to work for the group; now work all done thru Jira; tag yourselves; one issue: reputation is based on Github/engineering commits and not on organizing prowess.
3. **Created a List**: Women in Identity to follow on Twitter (by Ellie Stephens)
4. **Created a list**: TOKEN WOMEN – Women in Blockchain (Ellie Stephens)
5. **Jobs list on Rocket Chat**

A. Self Introductions:

Name, position, and twitter handle/email

B. **Who is looking for work: Who is looking for help**?

C. What is your most important website content: (# voting for that)

- Job board (10)
- Conference speakers (15)
- Mentors (10)
- Website content (8)
- Special interest groups (2)
- Interviewing other women in Identity (5)
- Chat (1)
- Events (4)

Vectors of Trust

Wednesday 9C
Convener: Justin Richer
Notes-taker(s): Thomas Berry

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

Topic: RFC 8485 Vectors of Trust

P Proofing
C Credential
M Management
A Assertion

OMB 0404 Trust Frameworks

Full attribute provenance.

How assured can you be about “that” person.

If someone has a really strong credential, in order for that to mean anything that has to be proofed to a real identity.

Other end of the scale, every attribute I get something about you, when was it last time it was verified; is that verified?

If you’re a relying party and get info about the person and its attributes, calculate that to determine if the person should login... can’t do it. Give them a numeric value and an RP can do the math.

You have an anonymous whistleblower that isn’t tied to an identity; the proofing should be explicitly zero; but, you need to make sure the “account” hasn’t been taken over by someone else.

800-63 rev 3 also has a multi dimensional approach to identity assurance

Vectors of trust comes from the computer science array, not mathematical concept
Need the real-world identity proofing from the credentialling

Proofing: How do I know you are YOU
Credential: Are you using (password|token|MFA)
Management: How is the association managed from proof to credential
Assertion: how does this get carried across the network (signed ID token, encrypted, multi-holder of key)

All of this gets “boiled-down” into a framework.
As defined by RFC 8485:
P1 All attributes have been self-asserted
.Cc you used a password
.Cb some holistic thing was used
.Mb approved management
.Ac passed by the browser

P1.Cc.Cb.Mb.Ac can now be thrown into a data structure without encoding

This is really simple to parse without a dedicated parser library.

The IdP can make this statement as part of the ID token “vot”:”P1.Cc.Cb.Mb.Ac”
sub:...
iss:...
exp:...
vtm:http://tools.ietf.org/html/rfc8485

RP can now simply look for the accepted vot:
I need a P1
And, maybe other parts of the category if necessary.
Could be easy as relying on the IdP to establish proof of identity

Use Case: Need something more than a cookie, the authentication can be requested/proofed-credentialed, etc.

The string within the construct of a trust framework can be translatable into a level of assurance (i.e., LOA2); although the RFC doesn't define LOA at all, but it does state it is perfectly acceptable to have a set of translation rules to take the vot value and return a LOA value... If it turns out you need to know when "this" was validated and "who" did the validated, vot doesn't get in the way of the query when it is needed.

NIST IR 8112 scratches around the edge of this, but doesn't define a protocol but does provide a framework with metadata of attributes.

VoT allows RPs that want to be smart to do so.

Trust Frameworks

- VoT only makes sense within the context of a trust framework
- IdP and RP need to agree with the VoT as it applies to the mutual trust framework

NIST document (unreleased)
Defines a set of vectors of trust values for new 800-63rev3
Does not have a publication target yet

IAL maps to P proofing
AAL maps to C credential
M management
FAL maps to A assertion

If you have your own trust framework, this can be extended:
X - hair color

IANA registry for extension categories of VoT framework

NIST framework brings priority of categories

Used as custom within health care space (integrated with OIDC IdP)

DID Communication Message Types

Wednesday 9D
Convener: Sam Curren
Notes-taker(s): Sam Curren

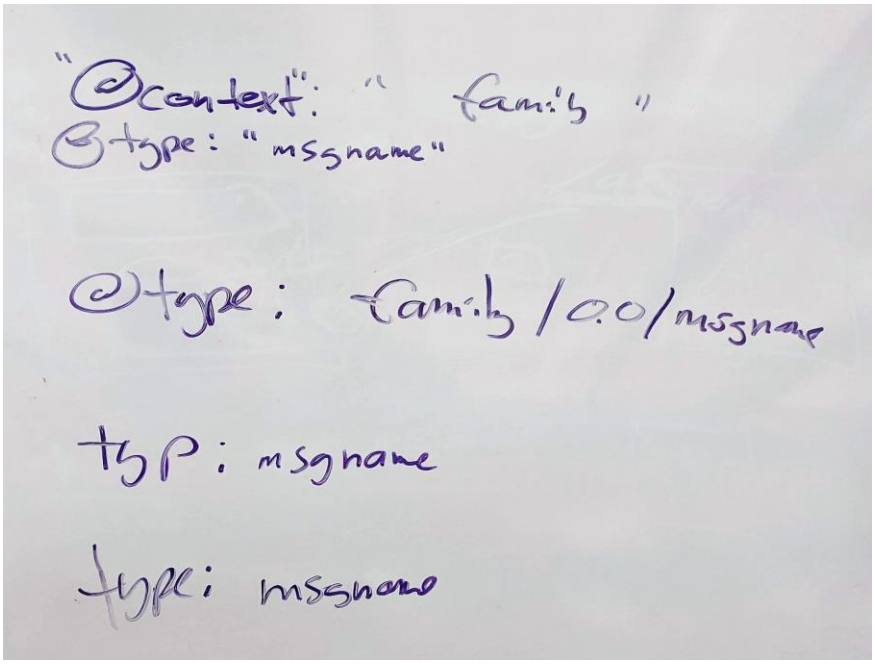
Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

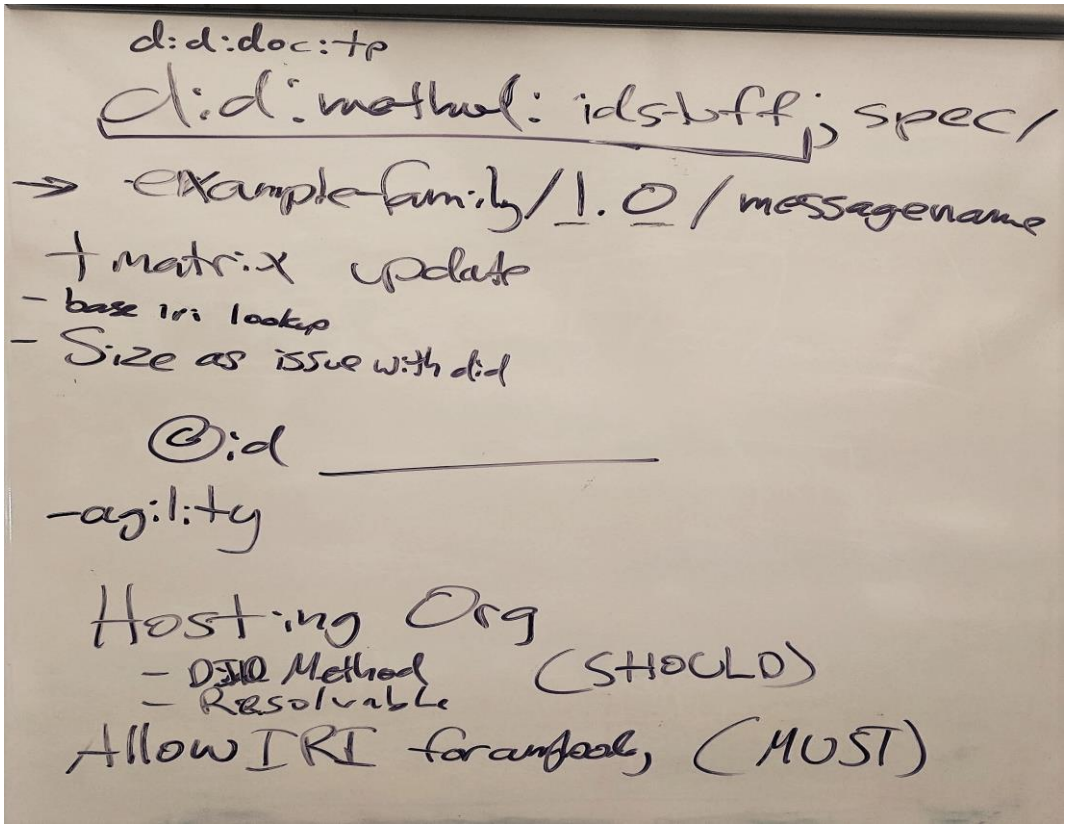
3. **Received from Sam Curren:**

We discussed current patterns used to designate types, the indy current method, and pros and cons of DID url resolution.
Conclusions:

- The Indy model will work generally, but needs to be updated to current DID spec resolution.
- Types are specified with @type in the json-ld way, but without resolution.
- URIs are a MUST
- Resolvable URIs are a SHOULD
- DID based is a SHOULD, and MUST for standards organizations.
- Indy HIPE about message types: https://github.com/hyperledger/indy-hipe/tree/master/text/0021-message-types

See pictures of whiteboard notes on next page….





Self Sovereign Commerce (VRM, Me2B, Progress Report & TBD's)

Wednesday 9F
Convener: Doc Searles
Notes-taker(s): Kurt Milne

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

Summary - The online commerce universe has been sucked into black hole of surveillance commerce.
1995 netscape - ecommerce - why not take shopping cart from 1 site to another

Project VRM - now in 13th year
Evangelism project - goal to get market moving
Berkman Klein Center - internet and society at Harvard University

Have wiki - top level list of development
573 subscribers

VRM = Vendor Relationship Management
VRM goals, principles, tools

Progress and TBDs - link list

Picos - DiD enabled
PIco labs dot org
Now can do zero knowledge proof with your things

Consumer attitudes changing

- Care about privacy
- Care about self sovereignly - aka “agency"
- Rejecting surveillance capitalism
- Pushing for laws and regulations

Building community

What hasn’t worked:

- Not much analyst attention
- Little investment
- No developer coherence around category label VRM
- No succession plan

Customer commons - knock off Creative Commons
World wide association of customers

Me2B alliance
GLiAnet

Me2B - certification mark for consumers to indicate if technology product is a good actor - fairness, fair trade.

Start with code of practice - going to interoperability spec
Goal 10 vendors on board this year

Focus on consumer, not B2B

Various categories

Q: Idea - add to peer review/ end user review sites?
Capterra
g2crowd
Trustpilot
Trustradius
PEERLYST

Social contract - ground in universal principles

- Comprehends manners and norms
- Inform with codes of practice

Ad tech - Behavioral based online advertising - soon to be regulated

Wish list:

- Publishers - OK to show advertising if not tracking
- Tent casting - where we choose to be qualified leads we control
    - Minimum disclosure for agreed use
- Infra for zero knowledge proofs
    - Building up to zero knowledge commerce
        - Disrupts surveillance economy
        - No single actor has all info - commerce, shipping etc.
        - Verifiable credentials
        - Zero knowledge credential eco system

Discussion - shift to seller oriented benefits

Not. Business model for Zero Knowledge Commerce

Make more money without tracking

Getting paid for data, and getting better value with better data

Data connectivity wins over data aggregation

Control that data stays in a certain context

Discussion - shift back to consumer protection

Sellers doing something today - that we want them to stop doing
What framework do we need to make those changes

Framing - evolution of problems / Labor laws, food safety laws, privacy laws

Consumer evil create by new technology

Right way to make right sales - more data

Cost of data exceedingly low
Damage capability of correlating data - skyrocketing
Study - Terms of service click through - if restate as “the implications of this agreement are …” agreement rates go down.
Cheap fast toxic relationship
Chem industry- large benefit, but need to control risk and cost

Treat customer data as toxic

Cryptographically provable - ripe for abuse

- Pete's example - collect data on Doc - never use the data to improve service
- Trader Joe’s - strategic choice to not collect and use customer data (? Any)

Getting and retaining you - driven by how fast you would customize
Zero incentive to not do that.

Paradux: Recovering from Maximum Personal Data Disaster (When It Is Lost)

Wednesday 9G
Convener: Johannes Ernst
Notes-taker(s): Johannes Ernst

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

Usually we talk about too many people having access to too much of our personal data.

Paradux is about the opposite: what happens if some part (or all) of your personal data suddenly disappears, due to natural disaster, or …? What if you yourself have amnesia, or are out of commission temporarily (or permanently!)

In this session, walked through the Paradux presentation: https://upon2020.com/talks/paradux/ and code at https://github.com/paradux/paradux/

Got tough feedback, but I think Paradux survived unscathed and fit for purpose. Many new ideas what else Paradux could be applied to, and perhaps some new source code contributors.

Are Crypto Wars Coming? Issues & Solutions

Wednesday 9H
Convener: Steve McCown
Notes-taker(s): Ben Gregori & Steve McCown

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

1. **Notes received from Steve McCown:**

   Summary of the session:
   In the 1990's, 'crypto wars' emerged when society began using strong encryption that governments couldn't crack. Now that strong crypto use is pervasive online, is our digital society heading towards a new round of 'crypto wars' or are there alternatives?
   Link to presentation:
   https://www.slideshare.net/stevenhmccown/are-crypto-wars-coming-144775751
   ********** ********** **********

2. **Notes received from Ben Gregori:**
   Do we want Encryption or Security from law enforcement?

   What are back doors? They allow root access into a device, performed by secret accounts/passwords, intentially weak cryptography

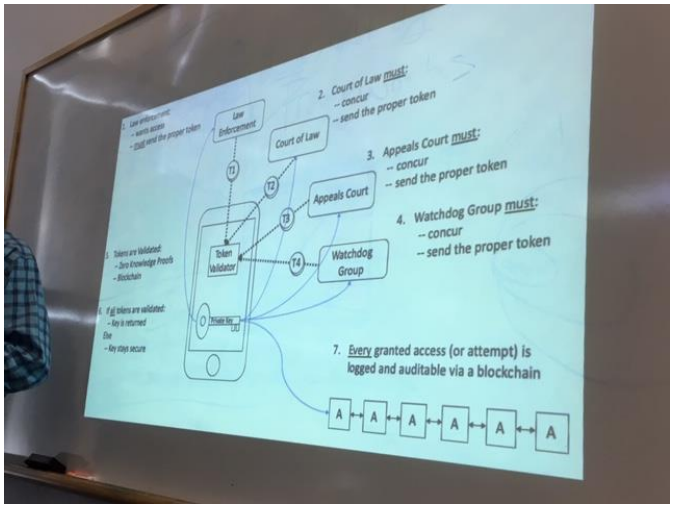
   Ex.
   - Cisco had 0-day attack enabling CIA to remotely control 318 products (Wikileaks 2017)

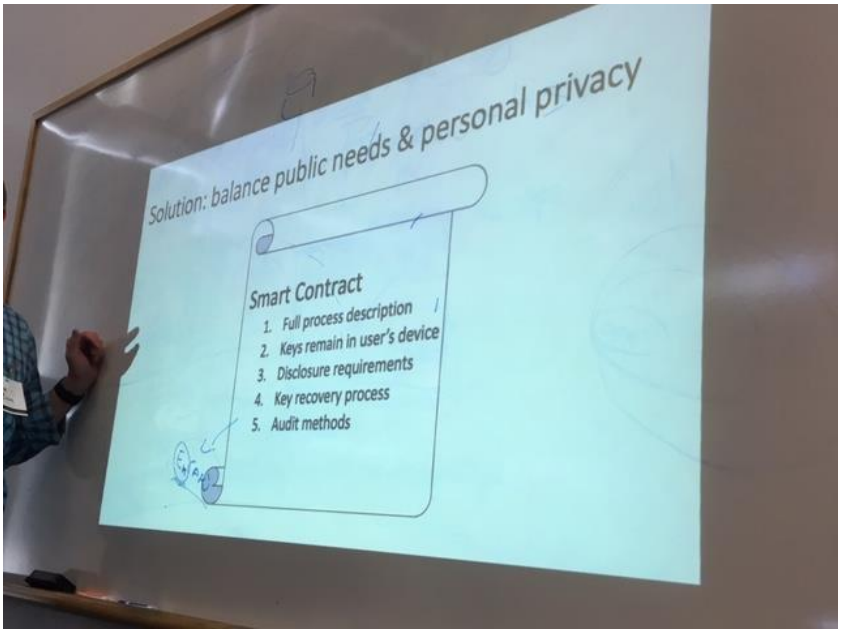
- VW created *static keys* open 100M VW vehicles

Problems:

- Insider abuse (pseronal, political, financial)
- External hackers
- Uncontrolled execution

“Responsible Encryption” literally means backdoors





Workshop On A Layered Model of Identity For Interoperability

Wednesday 9I
Convener: Jacoby Thwaites
Notes-taker(s): Jacoby Thwaites

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

Link provided by Jacoby Thwaites to working google slides document (participants edited this) and edited summary slides at the end. Workshop on a Layered Identity Model

App Level Proof of Possession Dpop/pop A Case Study

Wednesday 9J
Convener: Mike Engan
Notes-taker(s): Mike Engan

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

The deck presented at this session is found on the link below:
https://drive.google.com/file/d/1l4lfdKnMWzDcH378xvu6Jt-aExI33wIs/view?usp=sharing

Spent most time discussing the pro's and cons around pop chaining, and if it was worthwhile to endure the complexity to add the ability to chain signing through the various microservice layers.

Privacy Engineering In Context + Relational Integrity

Wednesday 9L
Convener: Cameron Boozarjomehri (@cboozar) & John Wunderlich (@PrivacyCDN)
Notes-taker(s): Doug Hawake

Tags for the session - technology discussed/ideas considered:

- Interesection of Relationship & Identity
- Expectations & Limits of Sharing
- Role Context plays in sharing & identity
- P7002 Functional & Non-Functional Reg for Privacy

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

- Problems:
  - Privacy is hard to tack down
  - Want to understand context when looking at identity
  - Relationship declared on Blockchain Agnostically
  - How to define software relationship that implement constraints of real-world relationships

- Discussion:
  - Delegation on limited context
    - Data should include reference of "ownership"
    - Data schemas are often mixed/adhoc
    - Notice and choice are critical to context
    - What is consent in a given context?

  - Open Question: How do you define scope of authorization?
    - "Just In Time" Notifications: improve transparency by only requesting permissions in the context of the purpose that defines the need for the authority
    - What is the context for enabling others to act on behalf of a data subject in a limited context?

  - Context for privacy and sharing is understood through the perspective of the endpoint/consumer
  - Purpose od use should be as clear as possible
  - Norms that define context are often implicit, meaning communicating them to consumers can cause confusion
  - Historically it was understood we only get 1 chance to give notice and get consent for privacy expectations in the context of a product or piece of software.
    - This won't be valid in the future
    - Consider the "Just in Time" model where consent is given only when that feature desmans a specific (not yet provided) permission

Misc:
For more on John's work with P7002 go to: http://sites.ieee.org/sagroups-7002/

- Cameron hosts a podcast on unexpected implications of technology (among other things) found at http://smallstuff.show/

Notes transcribed by Cameron Boozarjomehri on John's Computer

#Smart Custody

Wednesday 9M
Convener: Christopher Allen @ChristopherA
Notes-taker(s): Alan Jasper

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

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

Base scenario – a first world person has digital assets. How to protect them from disasters, such as natural disasters, fires, compromise, attack by adversary.

Adversaries – 28 personas. This approach defends against 10 of them.

Includes systemic network attack.

The process to follow can be read at

bit.ly/SimpleCustodyColdStorage

Describes the recommended procedure, based on setting up a local ledger on an offline storage device.

Create a set of 3 metal plates with the key stamped on it. There is a titanium version. Put in a home vault or a bank vault.

Test twice a year. Write a document telling people you trust, e.g. spouse, how to recover after you're gone.

More documents being drafted.

Fiduciary responsibilities.

There was a discussion on custody-as-a-service solutions/service providers – pros and cons.

Discussion on what assets could be stored this way, such as keys to other wallets, passwords to online financial accounts, social media, etc. Consensus was most but not everything.

Seed Quest 3D Game Mnemonic Easy & Fun Demo Seed

Wednesday 10A
Convener: Sam Smith (et al)
Notes-taker(s): Sam Smith

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

SeedQuest is a 3D game mnemonic for key or cryptographic seed recovery.
In this session we demo'd a release version of the app. This is an open source framework. It provides a novel unique method of convenient key recovery.
Link to presentation:
https://github.com/SmithSamuelM/Papers/blob/master/presentations/SeedQuest_IIW_2019_Spring_10A.pdf

Me2B Alliance Introduction

Wednesday 10B
Convener: Lisa LeVasseur
Notes-taker(s): Carolyn Tacket

Tags for the session - technology discussed/ideas considered:
Consumer trust, supplier certification, consumer education

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

Check out the deck!
Vision Statement – room prefers option A

Intention is not to reinvent the wheel — consolidating existing specs to create a unified certification
Integration of accessibility across all categories

Not the tech itself, but a question of business models as well as design and UX

Basic education about the cert but also about what the harms are:
- What does it mean when a vendor is sharing my data with a vendor broker?
- Translating tech and legal terms to consumers so they have a better sense of the choices and what's at stake

How to strategically influence the policy and regulatory landscape
Consider it a trade association
What comes across is piecemeal, particularly in regulatory processes — it is really powerful to bring all the considerations together

Useful to small vendors to not have to explain what's different about it from Day One. Creates a showcase and establishes that alternatives are possible, which opens the door to the market.

Unified vocabulary is absolutely necessary to move forward

Standards aren't looking at users or usability at all, this is a big departure from that. Creating a user panel for testing.

Code of Practice / self-certification first. Interoperability eventually down the road. Then following that with consumer outreach.

Engineers are conditioned to data monetization business models. But there are entrepreneurs who are ethically aligned starving for capital. Funding aspect has its own life cycle and need for leadership, but is essential for the overall success of the project.

Code of Practice has to be founded in shared principles.
What are some shared examples of when you have switched from a bad actor to a good actor and why?

Possibility of collaboration with B Corporation
Brand recognition is the value add to companies, but a network of certified companies is the value to consumers. Chicken and the egg at the initiation phase.

Important element is educating businesses how to do it right

Making money on data isn't inherently evil. But need to be transparent about how it's happening. And consumers need to be empowered between getting their services through subsidized and non-subsidized alternatives.

This is inherently a marketing service for companies
Simplifying this, especially in the first round, will make it more usable for suppliers. Need buy-in on a set of principles.
Enforcement mechanism is bad press

Nobody knows how to ask questions about privacy for third-party plug-ins – something like this would be helpful in an enterprise setting
Effort to get on vendor evaluation checklists

Trying to certify at least 10 suppliers by the end of this year

Me2Balliance.org à sign up for the mailing list if you're interested

Important understand the timeline of having a full universe of certified suppliers that would make it possible for someone to be fully Me2B certified

Important to prioritize the consumer education piece àcertification needs to be meaningful to everyday people. Needs consumer-driven demand to be the pull-through.
Encourage coordination with organizations like EFF, EPIC, Access Now, etc.

How to Issue That? The DIF Credential Manifest

Wednesday 10D
Convener: Martin Riedel
Notes-taker(s): Martin Riedel

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

- Introduction to DIF Credential Manifest Spec (https://github.com/decentralized-identity/credential-manifest)

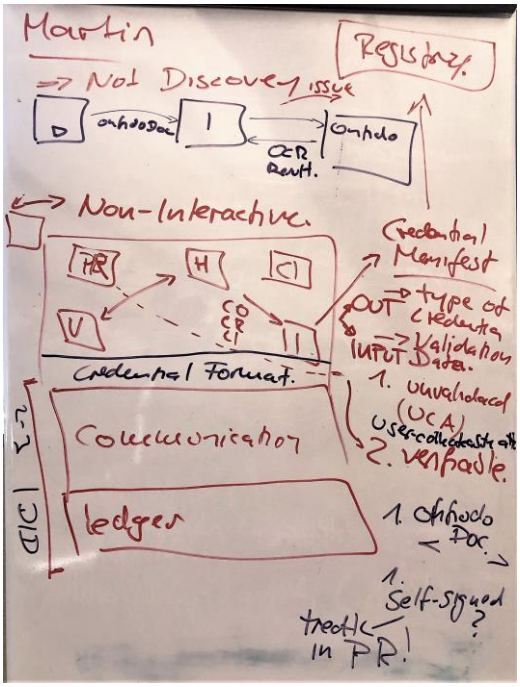
- Specifically excluding lower levels of an SSI like Ledger or DID comms.

- Outcomes:

—Unverified collected information should still be designed as self-signed information transfer.

— With unverified and verifiable Requirements the Credential Manifest should contain a static description of a Presentation Request.

— Credential Manifest could/should evolve into secure displays specification to collect self-signed / unverified information in a secure way.



The Peer DID Spec: Making Useful DIDs Without A Blockchain or Any Other Central Truth

Wednesday 10E
Convener: Daniel Hardman
Notes-taker(s): Daniel Hardman & Sam Curren

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

Received from Daniel Hardman:

We discussed the peer DID method spec. It is located at https://openssi.github.io/peer-did-method-spec/index.html.

We also discussed the connection protocol. It is located at https://github.com/hyperledger/indy-hipe/blob/master/text/0031-connection-protocol/README.md

Received from Sam Curren:

Managing SSI (A Relying Party Perspective)

Wednesday 10F
Convener: George Fletcher
Notes-taker(s): George Fletcher & Aaron Parecki

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

Notes received from George Fletcher:
We discussed a quick overview of the SSI Model. Basically that the goal is to provide a similar experience that users have today with their physical wallets where in they can present credentials from their wallet to entities of their choosing without the credential issuer knowing about the action.

We then discussed that relying parties (or service providers) all have an identity life-cycle to manage even if they are using an external service for identity management. The key aspects of the RP Identity life-cycle we discussed are:
* Onboarding / Registration
* Authentication
* Account Recovery

Onboarding Registration
The key differences between existing methods and SSI is that the expectation with SSI is that the user will have all the credentials they need in their wallet and the RP will ask the wallet for the credentials that it needs. The big issue for the RP is that they don't have any idea what credentials a user might have in their wallet. Especially as the model gets adopted, the credentials in wallets are going to be very varied and this is an issue for relying parties. Additionally, the claims a relying party requires at registration time vary widely based on the service the relying party offers. This can range from just needing self-asserted data to very robust verified credentials (for say opening a bank account).

Authentication
The biggest issues here is that DID Authentication (as currently defined) just provides some flows that can be used but the specifics of those flows are unique to the DID Method used by the SSI platform. This is problematic for relying parties as they have to have different code for each integration. Otherwise, the UX flow can be made pretty similar to existing flows and that's good for users.

Account Recovery
The SSI view of account recovery is "don't lose your private keys". From a relying party perspective this isn't a viable solution. Additional recovery methods need to be defined because real users will lose their private keys and need to get back into their accounts.

Other topics discussed
1. Fraud - there are new attack vectors with the SSI model and just normal registration fraud needs to be handled (it's easy to create a pub/priv key pair and self-assert data). Many relying parties don't need verified credentials and won't want to pay for them as a way to limit fraud.

2. Account Linking - there is a strong likelihood relying parties will need to support account linking as they will have both an SSI wallet and an existing identity at the relying party. It's unclear what the user experience is, or security impacts are, of supporting such linking.

3. Opportunities - there are some benefits of the SSI model due to the fact that the DID provides a discovery mechanism of services supported by the holder of the DID. This means its possible to discover a way to query for updated user information without involving the user which would be an improvement over the current practice of asking users to update their data when they sign in.

********** ********** **********

Notes received from Aaron Parecki:

Notes: Relying Party Lifecycle Management

* someone shows up to use your thing
* then they come back and you need to authenticate them
* users are going to lose their credentials and you'll need some sort of recovery mechanism
* under GDPR etc users will say you need to forget me and you need to deprovision them

we have these lifecycle events regardless of which authentication mechanism exists

from a RP perspective, SSI is an authentication mechanism

The RP has to separate the user's credentials from the identity storage where user info is stored.

Onboarding

common patterns are to ask the user for a bunch of information. any RP has to deal with fraud, even if all your service is is leave comments on blog posts. in many cases today, fraud at an RP is done by asking the user for a mobile number.

Eve - do you really mean relying party, or are you a service provider?

George - whether we use an internal component to authenticate users, or ask an external idp, it's the same for us so we are a relying party

Possible SSI Registration Flow

one of the issues is as an RP, how do I know what's in your wallet? how do I know what I can ask for?

I might need to know whether you're over 13, but do I trust a random bank in a country I don't know to issue a credential that says you're over 13? so I need some way to say which providers I trust to verify your age. it's unclear how to do this well.

when can I ask for a zero knowledge proof?

Lessons learned from OpenID Connect: what RPs always needed has been a way to communicate to the user, usually an email address. This won't change for a very long time.

Do I ask for an email address, and how do I know it's verified? If I get an email address from gmail.com, do I only trust google to issue that claim? or do I do my own email verification?

In practice I don't see a way to actually get all the information needed for registration in a verified way, so more likely we'd end up collecting what we can from the user to prefill the registration form.

Protocol Challenges

Right now, each DID method defines its own syntax for the JWT claims, so it becomes really hard to actually support all the methods.

Common Pattern: Authentication

* enter your username
* open a yahoo app
* app prompts is this you trying to sign in
* confirmed and you're signed in

Possible SSI Authentication Flow

If you did ask the user for a unique (to your system) username, then you could prompt the user to enter their unique username for that RP and it would know how to generate the appropriate JWT challenge.

Question - if you ask the user to enter a username, then this discloses which DID methods that username uses, so it's a slight leak.

Yes, just like any identifier-first flow right now, like currently happens with Google or Yahoo.

This keeps the user experience flow the same.

DID-Auth - proves ownership of a private key. Should other mechanisms also be allowed?

Account Recovery

Normal account recovery process - put in the email address, tell the user the phone number on file and verify it somehow.

Possible SSI Account Recovery Flow - don't lose your keys, back them up, etc. there is none. I don't think this is viable from an RP perspective.

if a person logs in to a paid service with DID-Auth, then they come in and say I lost my keys, what do I do? Maybe if it's a paid service they have a credit card and I can prove ownership of the credit card and then assign a new DID?

The existing account recovery problems that RPs have don't change with SSIs. Hopefully the one change is that it will reduce the number of recovery flows since it will be easier to log in without a password. But it won't eliminate them completely.

So then the question is if I have a really strong method like DID-Auth, then how many recovery methods do I need in order to get a strong enough verification of the user in order to recover their account? And then how much data do I need to collect about the user in order to do this?

What are the security implications of allowing a recovery method?

Question - what about letting the user upload verifiable credentials?

For us, as an email provider, we're not going to ask the user for a utility bill to recover their email account.

Other issues

Account linking - I already have a Yahoo account and now I want to connect my wallet to it. Is it good or bad? It's an easy technical problem to just add a DID to the account.

Fraud / anti-abuse

It's not hard to generate public/private keypairs. How do I do fraud detection to avoid bot networks registering? What do I do in the registration flow to know whether I should accept this registration.

Our fraud person said no you won't directly create an identity from the claim. Instead you'll present that to the user and have them click it, because that gives us many more signals to detect fraud.

At that point SSI becomes a form fill for the registration page.

It ends up being like SSI is just another social provider. But with social providers, we have the signal that we know an IDP is actively working towards eliminating fraud accounts so we have a higher assurance that a registration from that IDP is good. But with SSI everyone is their own IDP so we are missing that signal.

Data Hygiene

One thing DIDs do provide is the ability to update the user's data since the DID can be queried to find updated info about the user. The RP could use this to update the user's phone number which would be a much better experience than what we currently do which is to ask the user to update their information occasionally.

Relying parties will need to

- support both identity models in parallel
- minimize infrastructure impact
- will need to be involved in the community to know when things are changing
- deal with lack of standardization in the near term

Eve - in order to solve the challenges you identified... do you think that the goals for the current architecture would be compromised by doing this? Even just account linking or account recovery are kind of counter to the goals.

George - I just don't see this right now being practical to have just one DID method for a user account with no recovery plan.

How Do We Move From Good Intention to Gender Parity At Conferences?

Wednesday 10G
Convener: Wendy Hanamura
Notes-taker(s): Wendy Hanamura

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

HOW CAN WE CREATE GREATER VISIBILITY FOR WOMEN/Non-Binary/People of Color WITHIN TECH CONFERENCES?

- Mandate that panels have at least one woman who is not the moderator
- Request that questions alternate between male/non-binary speakers
- Make all emcee roles be diversity enhancing
- Set aside XXX spots for invited guests who represent diversity
- Create structural mechanisms (small groups, working groups) that bring different sectors together
- How do we work with Open Space formats so that women are not intimidated, run over, etc?
- We're seeing a proliferation of Women in XX Niche groups, but no sea change; Women Coding Ruby; Black Women in Blockchain; but no momentum. They need funding, paid work;
- Women who can sometimes less technical don't want to look like idiots? How do we overcome those barriers?
- Discounted tickets or free tickets for women to attend***(Getting companies to attend)
- We know founders—can we request that they nominate a woman to attend and pay for them?
- Swap—same presentation delivered to and by two different groups of people (for/by devs and for/by marketers)
- At the end of the day we are building for general users; how do we get them to relate and communicate to the end user instead of dev to dev?
- 1 session per day: you must go to what you pulled
- In order to attend X—you must come with 2 other people from a different sector
- **Moushimi:** has come for 10 years to IIW; she's on a working group for Hyperledger; been with Oracle for 14 years; used to being the only woman in the group, only woman of color, only person who has to leave at 5 p.m. to relieve the nanny; don't socialize post-work; it's good to meet
- **Do Co-branded events** DWeb Meet Ups + Women in Identity + Hyperledger Ambassadors + Token Women (Blockchain)
- **What type of Event would they want:**
  - New protocols
  - Explainers and demo
- You have to show up to the next event with someone:
  - A different height than you
  - A different gender than you
  - Wearing same color shoes than you
  - Who works in a different sector than you
- You are assigned to rooms—the person gives a presentation you didn't pick
- Coffeebreaks with new people (speed dating)

Creating An Ecosystem Of Trusted Applications (OAuth2 Dynamic Client Registration)

Wednesday 10H
Convener: Alan Viars (VIdentity)
Notes-taker(s): Thomas Berry

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

Use case: Health care applications can register with a lot of different data sources
Some ideas support this:
UDAP Unified Data Access Profiles (Lewis Moss)
Certifications and Endorsements for client applications www.udap.org

Cert authority [endorsing body] signs software statement
Links everything back to an X.509 cert authority

Comment:

- needs to follow trust models like "must encrypt"; must have a validation statement
- need an authoritative source sign the app
- Issuer string is resolving to issuer to validate the signature
- Certificate renewal becomes a problem

Pre-OAuth Entity Trust [POET] (Mark Scrimshire and Alan Viars)
github.com/transparent health/poet/python-poetri
assign a JWT with app signature
Issuer is the issuer of the endorser; what the endorsement means is out of scope

Comments:

- more scalability
- can only register if a (endorser) signed JWT is obtained
- All endorsers must be white listed
- PKI would allow you to trust a root where all endorsers are subordinate (?)
- Health care uses a direct trust/trust bundle of endorsers/issuers
- Application Governance problem

This is a similar use case to user consent for app to access data; endorser consent to app to dynamic registration and provide data

Endorser endorsing that company and its domain exists... but most endorsers don't care. Who is curating of the apps?

Other efforts to establish code of conduct for applications presenting user data.

Companies want to vet the apps; won't dynamically trust the apps

carinalliance.com: Apple, Microsoft, Google, etc. Enabling consumers and their authorized caregivers to access more of their digital health information with less friction.

Overlays (ODCA): What Are They & How Do They Intersect With Self Sovereign Identity?

Wednesday 10 I
Convener: John Hopkins
Notes-taker(s): John Hopkins

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

We discussed the Overlay Data Capture Architecture, which is 'a standardized global solution for data capture and exchange which protects PII data. Here is a link to the info I shared during the session. https://drive.google.com/drive/u/0/folders/1-Q3CBSYXlRNEvTu7XQfGo-6W5H_yyOA3

IEEE Activities in Digital Inclusion and Identity & the 2nd annual InDIITA Event in India

Wednesday 10J
Convener: Moira Patterson
Notes-taker(s): Moira Patterson

Tags for the session - technology discussed/ideas considered:
IEEE, events, India, ethics, bias, standards

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

Moira provided an overview of the IEEE-SA program on Digital Inclusion, Identity, Trust, and Agency (DIITA), which considers causes of exclusion which can be addressed by advancing technology for humanity through standardization and related solutions. More details on the program, and on the workstreams, can be found here: https://standards.ieee.org/industry-connections/digital-inclusion/index.html

Moira introduced the InDIITA 2019 event, to be held 18-19 July in Bengaluru, India.
(Link to the event webpage: https://standards.ieee.org/events/indiita-2019.html)

We also discussed the IEEE's Ethically Aligned Design for Autonomous and Intelligent Systems, which addresses many related topics. The document is intended not only to inform a broader public but also to inspire its audience and readership of academics, engineers, policy makers, and manufacturers of autonomous and intelligent systems (A/IS) to take action. The document can be obtained for free here: https://standards.ieee.org/industry-connections/ec/autonomous-systems.html

Finally, there was open discussion on the workstreams and also suggestions on other topics that should be addressed. Bullying in gaming and other online environments, and online discrimination and bias were proposed as important topics.

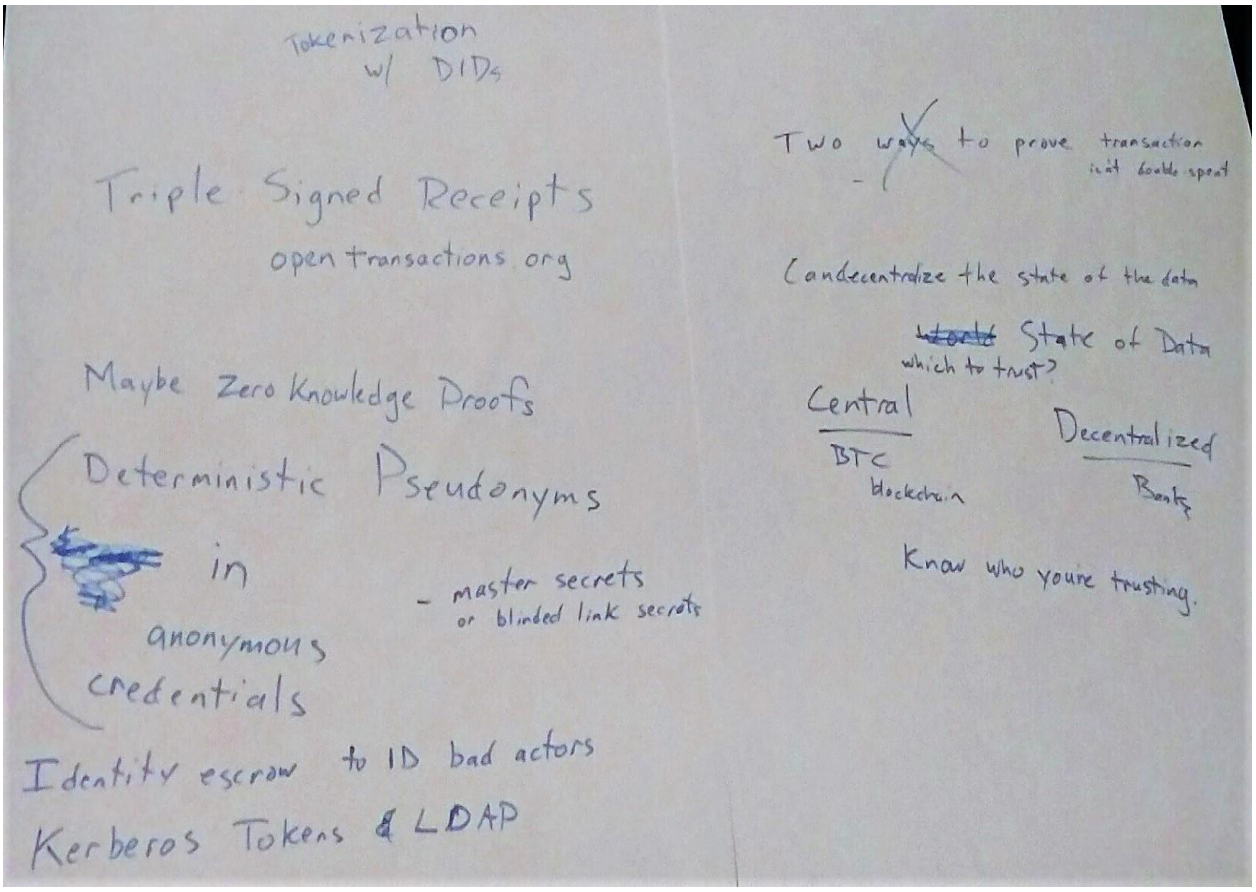
Moira thanked all for their participation in the session, and invited them to learn more about any of the activities and join them, and to help spread the word about he InDIITA event.

Community Claims & Discovery:A Simple Server & Method to Allow Decentralized Support of Rights & Permissions Especially for 3rd World Land Tenure

Wednesday 10L
Convener: Trent Larson
Notes-taker(s): Trent Larson

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

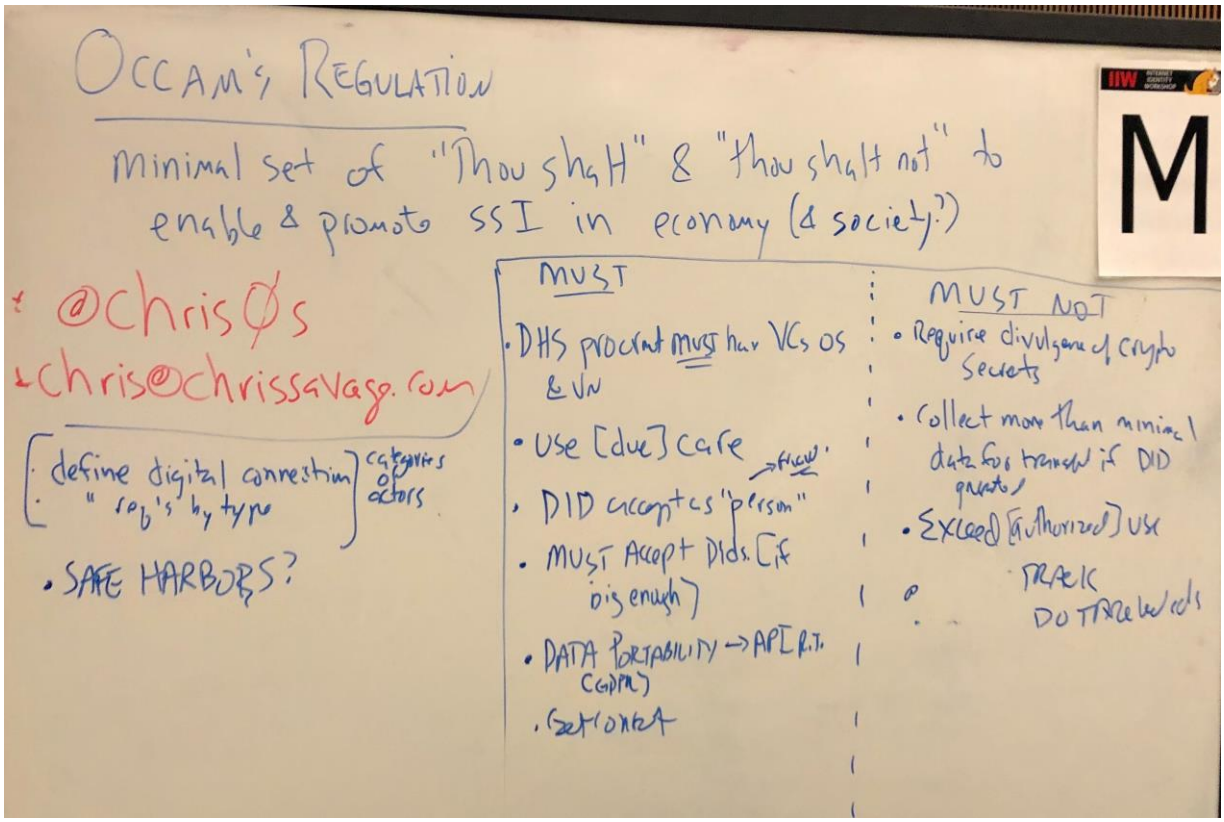
Slides here: http://trentlarson.com/community-claims/community-claims.ppt



There Oughtta Be A Law! OCCAM's regulation, legal engineering, & Policy Entrepreneurship

Wednesday 10M
Convener: Chris Savage
Notes-taker(s): Andrew Hughes

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



Thursday May 2

Fraud w/Credential – Attack Vectors & Remediations

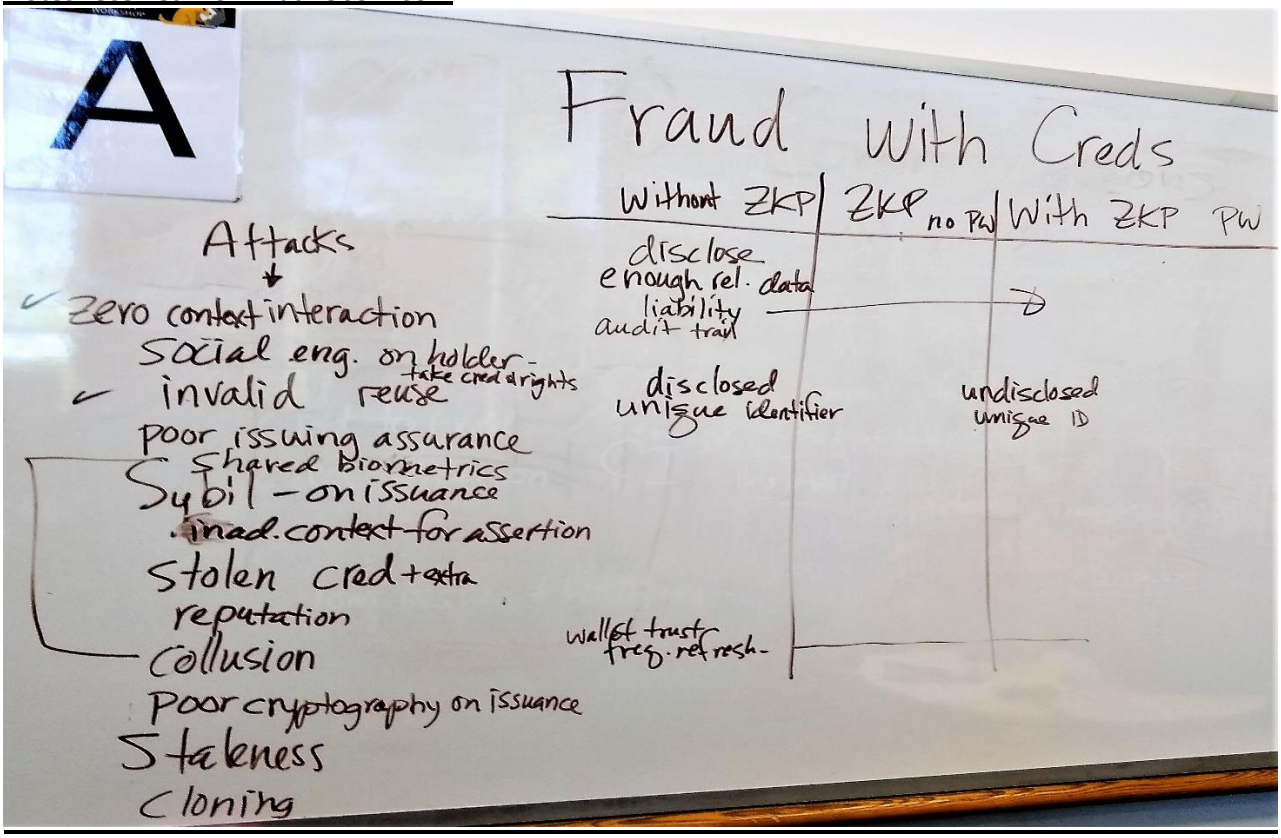
Thursday 11A
Convener: Daniel Hardman
Notes-taker(s): Daniel Hardman & Duane Johnson

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

Notes received from Daniel Hardman:

We discussed what kinds of attacks are possible because of different conditions in issuance or verification with credentials. We grouped the attacks and produced a list of the remediations , and we agreed that we would continue the conversation through a spreadsheet. Click link to said spreadsheet to continue the conversation:
https://docs.google.com/spreadsheets/d/1HALoNgZ7GTogw324squ7LRL4unfLSmPH_8B1ibxCQgE/edit
********** ********** **********

Notes received from Duane Johnson:



Fraud with Creds:

- we need to have a collection of "well known" types of weaknesses under various credential scenarios, e.g. similar to the well-known "man-in-the-middle" attack that helps people think through security scenarios
- ZKP: Zero-Knowledge Proof

Types of Attacks:
- "zero context interaction": you only interact once, party you're talking to is "completely unknown" with regard to their credentials; when you're done interacting, you don't seee them again. Easy to impersonate. You think you have trust with encryption, etc., but you don't really have trust--no long-standing relationship.
  - AAP: Agent Authorization Policy (which device is allowed to do proving--part of the proof includes requirement that you're doing the proof on a device that is authorized)
- "social engineering on credential holder":
- "invalid re-use": you've used the credential once, but then you show up and use it again when you weren't authorized to, or in a context that's different. e.g. "movie ticket"
- "poor issuing assurance": credential shouldn't have been authorized in the first place.
- "inadequate context for assertion": proof that I showed up at Bank of America (credential with my name on it), is not the same as a credential from Bank of America that my name is on the mortgage (but an outsider might be confused by the level of assurance the former provides about my name)
- "sybil attack on issuance": getting someone to issue multiple credentials of the same kind on you when they meant to only do it once
- "stolen cred"
- "cloning": copying private keys from one device to another
- "escalation": one level of credential being used to get permission to do more than was intended
- "invalid revocation": e.g. getting rid of someone's driver's license when it's perfectly valid; someone could use this for social engineering, posing as someone here to help get the credential back
- "reputation":
- "collusion": parties are actively trying to subvert system on an ongoing basis; e.g. selling credentials on the dark web, "the pirate bay" of credentials--selling ZKP proof along with credential. Suppose student is trying to apply to college--you want to prove your SAT scores are really high--someone wants to buy the credential that proves that.
- "poor cryptography on issuance":
- "staleness": e.g. taking advantage of the fact that I know more about current state of a blockchain than you
- "shared biometrics":
- "beer scenario": I'm 18 and I can buy beer for my 17 year old buddies

Mitigations:
- "invalid re-use": sample scenario: simultaneous use of a one-time ticket; sample scenario: voter fraud--you should be able to vote only one time in an election. Mitigation: (without ZKP:) unique identifier; (with ZKP:) link secret allows undisclosed unique identifier. Verifier/Relying Party is using the uniqueness of the identifier to ensure re-use constraints.
- "collusion": if we refresh often, i.e. "frequent re-issuance" can mitigate slow-moving black market. Indy wallets do not have "export private key" API.

Components Necessary for Use of Credentials

Creds	Keys
AAP	Link Secret

* AAP = Agent Authorization Policy

Introduction to Me2B (1/4)

Thursday 11B
Convener: Lisa LeVasseur
Notes-taker(s): Thomas Berry

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

Trustable Technology

- formal vocabulary is still in the works
- Open to feedback if something isn't quite right
- Define, Specify, Certify, Educate public

Vision (A) To restore human dignity in connected products and services
Vision (B) Achieving Digital Dignity: realizing the Social Contract in the 21st century

Comment:

- should emphasize "confidence" and trust

Group prefers A

Recommended Vision: Achieving Digital Dignity in connected products and services

The Problem:
Today's consumer technology marketplace is dominated by business models that are exploiting people.

Ecosystem - Trusted Engagement between individual and business

Usability must be effortless

How to balance the scale: business models got us here; new business models are needed; people need options (choices)

Disruption: Consumer adoption/consumer pull — critical mass of useful apps/services

new category: Me2B

App Developers: Solid, Hub of All Things (HAT), Lifescope, Citizen Me, Digi.me, people.io, whimsical

Make it economically practical for app developers: interoperability (specs defined)
Write once; port with ease

Why a market-making consortium / This has been done before:

CDMA development group

- cut and pasted specs from two competing specs
- Performed certification of devices and network equipment
- Promoted awareness & adoption of CDG to create CDMA market

CDMA-GSM: underlying technology of mobile phones

Comparable standards body: Bluetooth.org

Underdogs Unite!

Mission: Growing the marketplace for trustable technology choices

Technology Stakeholders: technology consumers and technology suppliers
Bring consumer voice into the stakeholder conversation

Value to technology consumers: Education, mitigation, reduced harm, hallmarks: safe, fair, trustable, respectful

Value to technology suppliers: support develop, integrate, market, and brand/certify

There are choice; suppliers can opt-out

Allow for competition: raise all boats

Success of eco system depends on thriving competition

Things that need to be done

- Usability principles [Research]
  - Define what the ethical business models are
  - Code of practice
- Me2B certification
  - Me2B interoperability specification
    - Digital Dignity Lab (vital)
- Consumer outreach
  - Regulatory support (vital)
  - Me2B user panel
- Marketplace of certified devices, platforms, apps
- TLC-IP
- Unified vocabulary

Realization: Multiplicity/proliferation of words for the same thing

Commentary (paraphrased):

- there are a lot of ideas
- feels a lot like the BBB, Trusty mark, Angie's List
- Providers can be forced to do things once they sign
- Missing community and identity (cultural)
  - Could belong in code of practice or user panel
  - suggestion: this be more prominent
- The time is right for this
  - "Anything to put a string through pearl, rock, and gem"
  - Similar to efforts in Linux Foundation
  - Realization that the everyone has to work together
  - There is the beginnings of an incentive right now

- There's a heightened awareness of ethics
- Emphasis: This is intended to be an alliance, not a consortium
- Wants to be an enabler/supporter of standards; this is as "stickish" as this wants to get; this is intended to be more carrot (encouraging)
- Don't be disheartened if there isn't an immediate response; this may be an advanced idea that is ahead of its time.

Progress to date
- 25 people on mailing list
- Organizations committee (4 individuals)
    - Lisa LeVasseur
    - Johannesburg Ernst
    - Andrew Hughes
    - Mark Lizar

Catalyzers
- Academia
- Policy/Regulatory
- Legal
- Standards
- Other NPOs

    - Diverse disciplines: sociology, philosophy, design, legal, technology development

Founder: Arlene Harris, Wrethinking, The Foundation, Family LIfe Management Solutions

2019 Me2B Certificate v1
- Code of practice
- Education
- Organization Structure
- First 20 services certified

2020 growth & Me2B alliance stand-up
- reporting & auditing
- Marketing

2021 Data portability...
2022 international standards

me2b.us
me2balliance.org
- sign-up for Alliance Mailing List
- Join a working group
    - Code of practice
    - Consumer
    - vendor

Survey: Https://tinyurl.com/me2b-survey

Why "Specific & Informed Consent" Is Nonsense (or Not)

Thursday 11E
Convener: Julian Ranger
Notes-taker(s): Julian Ranger & James Pasquale

Tags for the session - technology discussed/ideas considered:
#informedconsent, #consent, PrivateSharing, #trustedsharing

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

Notes received from James Pasquale:

- Resources: meaningfulconent.org
    - No norms exist today
    - Need trust marks by third parties who set minimum levels
    - No real Binding Laws and regulations circumventing the need for consent in general
    - Fairness mechanisms like agents (BOTS) who will fight on individuals behalf to stop crappy uses of data previously shared to high the individual has no access or control over
    - GDPR give individuals the right to have and use a copy of their personal data
        - It also defines a set of rules requesters of data must follow
            - Right to access
            - Right to correction
            - Right to erasers
            - Notice and consent for use.
    - Define what ill happen to data next or post sharing
    - Notice of sharing it's other and or new data processors
    - No selling of an individual's data with out notice and or new consent
    - Scalability of levels of consent from complex uses to innocuous uses
        - Complex will never scale well without AI (resonates assistants working for individuals with set rules of rather road of use.
        - Too long versions of consent will force individual to always just accept with out regard.
        - Trust marks of the kinds of data and use of sharing can over come simple consent.
        - No wordsmithing of consent must be clear and unambiguous for individuals to understand rules an rights AKA what ill happen as a result of sharing. Duration, value exchange for sharing, etc... other rights now and in the future.
    - Companies will always find dark ways to coerce individuals to just consent.
    - Without an individual hold a record of consent legal recourse becomes more difficult. Swaying the balance of power in the legal realm.

    - We need laws to define must do when handling data, and must not do pre and post individuals sharing data, regardless of consent or not.
- By the end of the session the room was split between is consent or is not consent nonsense. With one quarter of the room in agreement consent is required and new laws and regulations around how data is acquired and used need to assist each other protecting individuals from creepy behavior by data requesters

Hub/Agent Cloud Stuff Project/Company Intro's/Explainers (Part 2): Continuation from Day 2 Session 7I (Mapping Working Groups)

Thursday 11F
Convener: Kaliya Young
Notes-taker(s): Kaliya Young

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

Notes received from Kaliya Young: Common amongst all of them are these things

DID Communication
* **Base Encryption (Wallet People Port Civic)**
* **Message Typing**
* **Routing**
* **Alignment w/ crypto key types (secret management)**

Increase compatibility in future w/o hair pulling in the future.

Agents
based on ARIES at Hyperledger
    * Key Management
    * Credentials
    * Protocol Support
https://wiki.hyperledger.org/display/ARIES/Hyperledger+AriesIM

Projects/Companies based on Aries
* IDRamp - https://idramp.com
* Mattr (SparkNZ) - http://www.sparknz.co.nz/
* StreetCred
* connect.me http://www.connect.me
* T-Mobile (Axel)
* Germen Credentials @University
* NL Bank Consortium

* BlockPass - https://blockpass.org
* Some Banks are folding into existing applications
* IBM - https://www.ibm.com/blockchain/solutions/identity
* ATT

British Columbia super Agent in its own category

HUBS

Personal Data Stores
    * Can store encrypted things at Rest
    * Actions -> Meta Protocol
    * Synchronization between Hubs

MSFT and WorkDay

Other Projects

Transmute - Workflows approach - https://www.transmute.industries

digi.me waiting for the - https://digi.me

LifeScope - SOLID - https://lifescope.io - https://solid.inrupt.com

3Box [Ethereum] - https://medium.com/uport/announcing-3box-and-ethereum-profiles-dba9841e0952

Privony - Michael Becker's Company - https://privowny.com

HIEofOne -http://hieofone.org

Wault for Health - https://wault.wymsical.com

Blockstack - https://blockstack.org

* PICO Labs aligned with ARIES - https://picolabs.atlassian.net

WALLETS

*   * narrowly defined around holding credentials*

uPort - https://www.uport.me

Civic - https://www.civic.com

JoloCom - https://jolocom.io

BlockchainCommons key recovery airgap- https://www.blockchaincommons.com

Sphere - https://www.sphereidentity.com

VeresOne Web Profile - https://veres.one

Just Crypto
* *electron*
* *Pillar http://www.pillar.io*

Things in play in decentralized web land include the
Fediverse https://fediverse.party
Activity Streams - https://www.w3.org/TR/activitystreams-core/

Here is a Community Calendar of Calls related to Decentralized Identity & the Market

MONDAY

Identifiers Names and Discovery
Decentralized Identity Foundation 11-12 PST Bi-Weekly Chairs: Markus Sabodello, Jude Nelson

TUESDAY

Sovrin Crypto Meeting Sovrin 7am Pacific Weekly Chairs: Mike Lodder, Nathan George

VCWG - Verifiable Credentials Working Group
W3C Working Group must be W3C Member 8-9 Pacific Weekly Chairs: Dan B

W3C Community Group Open to anyone 9-10 Pacific Weekly Chairs: Kim Hamilton, Christopher Allen, Joe Andrew Credentials Community Group

Semantics Working Group Hyperledger Indy - AREIS? 10-11:15 Bi-Weekly (Next May 14)

WEDNESDAY

URSA Crypto meeting / Hyperledgeer 7am Pacific Bi weekly Chair: Mike Lodder & Dave Huseby

DIF All Members Call Decentralized Identity Foundation 8-9 Pacific Bi-Weekly

Interop Project Decentralized Identity Foundation
8am Pacific Bi-Weekly (opposite weeks of Member call) Chair: Rouven Heck

Me2Be Community Call Werethinking Foundation
8-9 on 2nd Wednesday's Monthly (changing to different day) Chair: Lisa LaVassuer

Consent Management Kantara+ ISO 7AM PT/10:00 AM ET Bi-Weekly
Chairs: Jim from digi.me and Andrew Hughes

ARIES Developer Call
Hyperledger (Formerly Indy Agent) 12-1:30 Pacific Chairs: Sam Curren & Stephan Curran

THURSDAY

Storage and Compute Working Group
Decentralized Identity Foundation 8-9am pacific Bi-Weekly Chairs: Daniel Buchner, Sam Curren

CIS Consent Information Sharing Working Group
Kantara 10:30-11:30 ET (7:30-8:30 PT) Weekly Chairs: Jim Pasquale, John Wunderlich, Andrew Hughes

HyperLedger 8am PT Chairs: Sean Bohan, Nathan George I ARIES Developer Call

Kantara * 6am pacific time/9am Eastern Chair: Eve Maler Twitter: @umawg UserManaged Access

DID Spec and DID Resolution W3C Part of Credentials Community Group 13:00-14:30 PT

Pwn-Back Your ID from Equifax, Experian & TransUnion: "Check it & Protect It"

Thursday 11G
Convener: Thomas OMalley
Notes-taker(s): Thomas OMalley

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

Link to full document w/figures and images included-
https://drive.google.com/file/d/1E2v61i5X4c5AOHwRfy6BjRzwN1EHgdCq/view?usp=sharing

In this session, we discussed how the nation's largest credit reporting agencies (CRA) have "pwned" (pwn-slang term derived from the verb own, meaning to appropriate or to conquer to gain ownership) our "personally identifiable information" (Pii) and long-term credit histories from our existing lenders and other data sources.

As depicted below in Figure 1, the nationwide CRA oligopoly (EXPERIAN, EQUIFAX, TRANSUNION) created a new multi-billion-dollar (projected $18 billion by 2025) revenue stream from its "ID TheX Protection Racket" that the Big-3 CRAs ("the Cranos") control and operate.

The CRAs' current revenue model consists of zero cost-of-goods (COG = $0); specifically, your "personally identifiable information" (Pii) and credit histories provided by your existing lenders, along with other sourced data.

CRAs then aggregate all of your data into "credit reports," which the CRAs then sell to both your existing lenders and creditors AND to new prospective lenders and creditors that want you to buy their loan and credit products. According to the former Equifax CEO who retired aXer its infamous data breach of 148 million people, his CRA's "unique business model" earned CRA Equifax a 90% gross profit margin on its COG sold.

CRAs earn revenue on every credit report the CRAs sell to prospective new lenders, irrespective of whether lenders are dealing with genuine consumers or criminals using stolen identities or "synthetic" (i.e. fictitious) identities created with children's SSNs. Instead of spending money to prevent new account fraud, the CRAs created the "identity theX services protection racket" that DOES NOT PREVENT new account identity fraud, but gives the CRAs a lucrative new revenue stream.

INSERT: Figure 1 - CRAs Pwning Your Pii and Financial Identity

We also discussed how people can "pwn" back and control their financial identity under the Fair Credit Reporting Act (FCRA).

The first step is to download your free annual credit report and check/fix errors in your credit reports maintained by the Big-3 CRAs - Experian, Equifax and TransUnion. ***See Figure 2, draX UX*** re-design of FrozenPii.com.

INSERT: Figure 2 - Free Annual Credit Reports

The second step is to freeze your Experian credit report, Equifax credit report and TransUnion credit report. ***See Figure 3***, draX UX re-design of FrozenPii.com.

INSERT: Figure 3 - Free Credit Report Freezes

The FCRA requires CRAs to implement security credit freezes within one business day following a consumer's on-line or toll-free telephone call request. The FCRA also requires CRAs to "unfreeze" a consumer's credit report within 1 hour of the consumer's online or toll-free telephone request. This allows a consumer to control release of their credit reports only to new lenders chosen by the legitimate consumer, not to lenders dealing with criminals.

The disruptive effect of large-scale consumer credit freezes would be the elimination of the consumer rip-off "ID TheX Protections Services" industry, which markets fear and sells an ineffective "early warning systems" of successful new account identity fraud. ***See Figure 4.*** Only free credit freezes can help PREVENT new account identity fraud.

INSERT: Figure 4- CRA Revenue Disrup9on from Scaled Credit Freezes

For more information about free annual credit reports, free credit freezes and free identity theX victim help services, see FrozenPii.com (new UX web design coming June 2019).

DPoP: Current Draft, Next Steps

Thursday 11H
Convener: Daniel Fett
Notes-taker(s): Mike Engan

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

Dpop status.

The groups walked throught the current DPOP spec and git issue tracker repository
https://github.com/danielfett/draft-dpop

Latest draft is in the github location, not the IETF rfc.

Daniel walked the group through the token request and the new parameters in that request.
And then walked through he resource request call with dpop signatures

Discussion between body or header attributes

Discussion between including or not the “bearer” on the access_token in the authorization header.

Discussion around HTTP request signing methods attempted over the years.
Including cabage signature draft

Discussion around the use of http_uri and it’s other option making it a more generic aud. (or other name).

Discussion on if clients should be more explicitly forced to sign every request.

Discussion if the spec should allow an implementation that a DPOP is re-used.

Suggestion to change exp to iat.

Discussion on enabling key rotation.

Mentioned two different sessions with similar paths. (t-mobiles pop token, and sasha’s client tokens session on day one).

Oh No You DIDn't! Your Identity Is Not Self-Sovereign

Thursday 12A
Convener: Justin Richer
Notes-taker(s): Thomas Berry, Sam Curren & Ben Gregori

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

Notes received from Thomas Berry:

Commentary (C)

JR: The term "self-sovereign" identity is misleading

- Identity should be viewed as a conversation; self-sovereign suggests that it gives the power to the speaker, not the listener
- As technologists, we run into a trap of conflation of aspects to identity
- Instead of Identity as expressed and as received
- The model and discussion is much more nuanced; what does it really mean?

C: Identity doesn't matter

- identifiers and attributes are what is important
- reputation is then a following factor
- I can then assert the important attributes about myself

C: The two views are less in opposition than you might think

JR: The acceptance of the identifier and attributes, etc, are good, but there in lies the central crux of the argument

When the subject is sovereign; the distinction made is self is an individual, a distinctive human being. The other aspects are mechanics. Self-Sovereign is what we feel in the world.

JR: this dicodemy is what I'm trying to raise; ... naming things is hard, no better name for the constructs

C: sovereign refers to some entity that controls a political sphere, but it is not absolute. You don't have to take this to the Nth degree to make it meaningful.

JR: the key pivot is yes, you can be sovereign in expression; you'll never be sovereign in the acceptance

C: sovereign [means] I am in control of the ability to choose the [attributes] that I present

- another really useful ... administrative identifiers are loaned to us; using DLTs you had an opportunity to control those identifiers, you could claim and prove the identifiers [were mine] as a eternally persistent record (blockchain); you aren't relying on an ever present ledger...that exists in the world that people that use it

C: SSI: you have control over your [identity] borders; but, you can't control who accepts your identity

C: sovereignty exists within a domain; outside the domain is not considered a peer. Sovereignty requires others to recognize it or it does not exist. Identity manifest in the observers cognitive capacity. Your can not control the identity that everyone places on you.

JR: my identity is not self-sovereign; I have a different identity that exists out there ... I am not sovereign over that

C: if I have an administrative identifier that is used to talk about me behind my back. [Self-sovereign allows me to provide identity without handing it over]

JR: property boundaries; [your neighbor can look into your property boundary and say that's weird]

C: if it weren't for the internet we wouldn't have this discussion; internet was built without security as an underlying layer. [Self-sovereign identifier establishes the root of trust for the interactions being performed]. Without the root of trust you can not build credible relationship, [it fails]. SSI establishes a root of trust; everything else is noise.

JR: it's only trust if I trust it.

C: [SSI trust secures my identity; my identity is secured and cannot be erased, unlike a DL and other forms of identity. SSI is recoverable]

JR: your existence can be ignored

C: we need to be aware we're talking about more than people

C: SSI means something more than root of trust; you control where your information goes [consent]. Privacy is not secrecy; [its about control]; it's overstating that SSI does those things [privacy, security, security]. Technology is not in everyone's hands for SSI to serve all.

C: [SS relies on it to be built into the right software; trust in the software cannot be controled]
JR: how can you trust that copies of your SS aren't being made unless you wrote the software

C: [there are trends in the population that is focused on identity; SSI should be introduced]

JR: self determination of pronoun reference; your an introduce yourself with whatever name that you want; no one checks on this. Problem of expressivity; human language is squishy; my favorite pronouns are ...; expressing this in a digital space is difficult [to factor into areas of consent].

C: A term becomes useful when there is a strong convergence on its use; we don't have that [with SSI and Identity]; labels are very ambitious and not useful. Let's get back to operational use of things; identifiers and attributes. [There is a core that we can use to describe ourselves]; there is a commonality of attributes to [discuss this]. SSI is not useful outside the tight cliques.

JR: [Gargon is important within the community discussing SSI]

C: [SS was intentionally provocative; this discussion is an indication that it was successful]; the terminology gets conflated all the time.

JR: there is ongoing debate about the decentralization of the terminology

JR: [the trusted credential is the issue at hand; SSI doesn't matter if there is no one to accept it]

JR/C: [is it super scary of convenient when things work together; does this concern the government? the government wants silos of identifiers; data can not be shared.]

JR: nobody cares about what you think about yourself; they care about what they want to know about you

> Dead-naming: common term in trans community; after choosing a new name the "old" family refuses to use it deferring to the previous person's name.

C: where's the tension?

JR: [SSI has an identity as a concept; from the outside world it has the identity—but it doesn't live up to the term]

C: [you always have more sovereignty over a DL instead of a digital wallet; I know how DL works, I don't know how that app/math is working]

********** ********** **********

Notes received from Sam Curren:

SSI is a misleading name.
A better way to look at identity is as a conversation.
SSI is often posited as giving all control to the speaker and none to the listener.
Your Identity is not necessarily tied to the expression of your identity.
Identity as expressed vs Identity as received.
Validity of SSI work is a separate argument.
Nuance of the discussion.
What does the nature of Soverinty of an Identity even mean.

Identity is more simply described as identifiers and attributes.
Reputation is on top of that and is what people think about me.
These labels help the conversation.
Is this a semantic dance?

That description is good, but avoids some of the deeper edge issues.

when Soverign was first given a name, the distinction was between what you felt you were as a human being, as oppposed to the administrative pieces. (This was pre 'self' prefix)

We mostly talk about administrative identities.

in the political sense, soverign refers to the control of some sphere.
A king can be soverign within his borders, but not without.

A soverign identity doesn't have to be perfectly soverign to still qualify for the title.

You can be soverign over the expression of your identity, but not the acceptance of that identity.

Choosing which identifiers and credentials you present is part of the soverrinty.

identifiers that cannot be removed
we can prove our ownership of a self-soverign identity without permission

within your self soverign domain, you don't ask permission, outside of it, you desire to be

soverignty requires that other people recognize it.

an identity is made soverign by the recognition of it.

identity worked consistantly before the internet.
the internet creates new problems to solve.
cryptography is the tool that we are trying to apply.

trust was not added to the internet in the beginning, but that isn't to say that they knew how but just didn't do it. - Dave Crocker

control is often associated with the concept of secrecy.
privicy is context, control, choice, and respect.

ssi techniques.

use of crypto tools requires trust of the developers.

some communities express identity through pronoun exercises.

Names given in person are usually just accepted.
It changes the internet because of the dynamics in play.

A term fails when we don't have widely accepted meanings attached.
Narrowing down on simpler things will help focus conversation.

Jargon exists to be efficient within small groups.
Self-soverign identity is leaking.

The SSI term _has_ promoted conversation about the ideas. Success as a term?

convenience often trumps judgement

'self' as opposed to what others think of us.
there is no platform today for an individual to define their platform.

dead naming is important. There are times
dead naming is used when somebody chooses a new name. Their old name becomes their 'dead name' and may be used by those that refuse to acknowledge their new name.

fancy math feels like no replacement for holding a physical card.
we speak English because we are pretending that we are communicating.

********** ********** **********

Notes Received from Ben Gregori:

Self-sovereign frameworks ignore how people accept you to be. Technologists conflate related but separate aspects of identity:

- Who I internally see myself as (existential)
- Identity that is expressed
- Identity that is received

The model/discussion is more nuanced. What does the nature of sovereignty in identity mean from a tech perspective, personal, or philosophical perspective.

Maybe "identity" doesn't matter – maybe its identifiers an attributes to escape the morass of "what is identity"

- Reputation is layered on top of that (what people think of me)

Those two views may not be in opposition. This second view begins with straightforward constructs we recognize (how to use, create, make new ones – we know properties). But we don't think about issues around that that arise from the first perspective.

- You can't own all identifiers. Some identifiers require an extended conversation and partiers are more equal than in others.
- In some, a party can also mandate identifiers that you can either accept or reject.

So issues the second perspective raises are easier to operationalize.

Note: acceptance of an identifier is a central crux of the argument of the session.

Distinction: self-sovereign (what you think) and administrative identifiers (what people think of you).

- People cannot and should not assign their own administrative identity. You can't *fully own* your own identity…its partly assigned.

What makes it sovereign is not the declaration, but the *acceptance* of that identity. Therefore,

SSI is a technique, not a technology. We need much more than just tech to embody the principles of SSI in the world. Institutions, politics, hardware, etc.

(Dave Crocker)- The squishy nature of identity, on which *no one* can agree, even with the 28th IIW and the existence of SSI for a long time, is proof that we should use operational terminology that is actually useful because we can agree on it and we can act on it. – Humans create jargon to in a tight community, and we STILL cannot agree.

- Joe's Andrieu's hot take: as a catalytic, provocative term , SSI is successful because we're till debating. As an engineer, its incredibly difficult. SSI has ideological/political roles and technical components to achieve that.

SSI is limited, misleading, mismarketed, but its not the perception of the SSI world from the outside. SSI has an identity as a concept, from the outside world, it has an ID that carries certain meanings.

While we may viscerally trust a physical drivers license more, it may be more about reputation. We build reputation for trusting DLs, we could build trust for new tech like DIDs and cryptography.

- There is a degree of trust in a DMV issuing a DL
- This is a difference in logic vs. belief, which are both important and valid. It is certainly exploitable, but we accept there is limited access to doing this, fakes are difficult, and the system that uses DLs hasn't broken down.
    - Fancy math is new, less proven (or less widely understood to be proven)

Me2B – Have YOU Changed Activity Because Unethical Data Company? (1/4) (a/k/a: "It's Not Going To Hurt, Right?)

Thursday 12B
Convener: Andrew Hughes
Notes-taker(s): Heather Vescent & Andrew Hughes

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

Notes received from Heather Vescent: What behavior have you changed due to/stories about ourselves

How our behavior has changed

- Fear of being noticed and targeted
- Apathy
- Self-censor/curate
- Avoid unknown connections
- Use specific throwaway contact accounts. (email)
- More cautious about unexpected
- Use inconvenient apps to change externally viewed profile (e.g. multiple browsers)
- Leave social media. I quit FB 6 weeks ago. I found a lot of benefit, and I connected with people. But it took me a while to get to this point.
    - I watched my behavior of how often/time I would pick up my phone to kill time.
    - I knew it was bad, and they were bad actors. It took the criminal case.
    - I'm not going to do business with a company that is under a criminal investigation.
    - When you leave FB, you have a grace period of 30 days.
    - Recovery clarity results

--

- Do things behind the scenes
    - Anonymous
- Direct choice to not share between apps
- Advising/teaching community about how to determine trustworthiness
    - E.g. mouseover shows target HREF
- Define "known good" actions for others using apps, e.g. insta likes

- Teach community what physical world, protective actions in the online world.
- Dr Michael Ridge – what we are not doing because of technologies.
- An alternative to regulation and laws where people set the new social.
    - Can look at times of history when there were times of lawlessness. We've been in these situations before.
    - Justices of the peace emerged. English common law evolved from this. Local community mores.

--

- Browsers started to enforce HTTPS everywhere
    - Increased security visibility, but confusing to normal
    - I will not use certain browsers because they block those sites, automagically.
    - Different vehicles go different places with different efficacy
    - I install multiple browsers. I have five different browsers that I use.
    - HTTPS killed the archival web
    - (Google has taken the lead to do HTTPS there)
- VPN
    - Certain apps say they can't be accessed/or functionality is removed when using a VPN.
    - "VPN is too weak to engage with."

Stories that we've heard about/from others

- Asked to take down a picture because subject started getting threats
- Women change behavior online (in particular)
- Target of stalker chose to reset real identity and digital identity
    - Self-activated witness protection
- The realization that tribalism becoming embedded. In normal interactions (politics) has caused a schism and self-segregation, e.g. avoid family events because of politics.
- Killed FB account and started a new one.

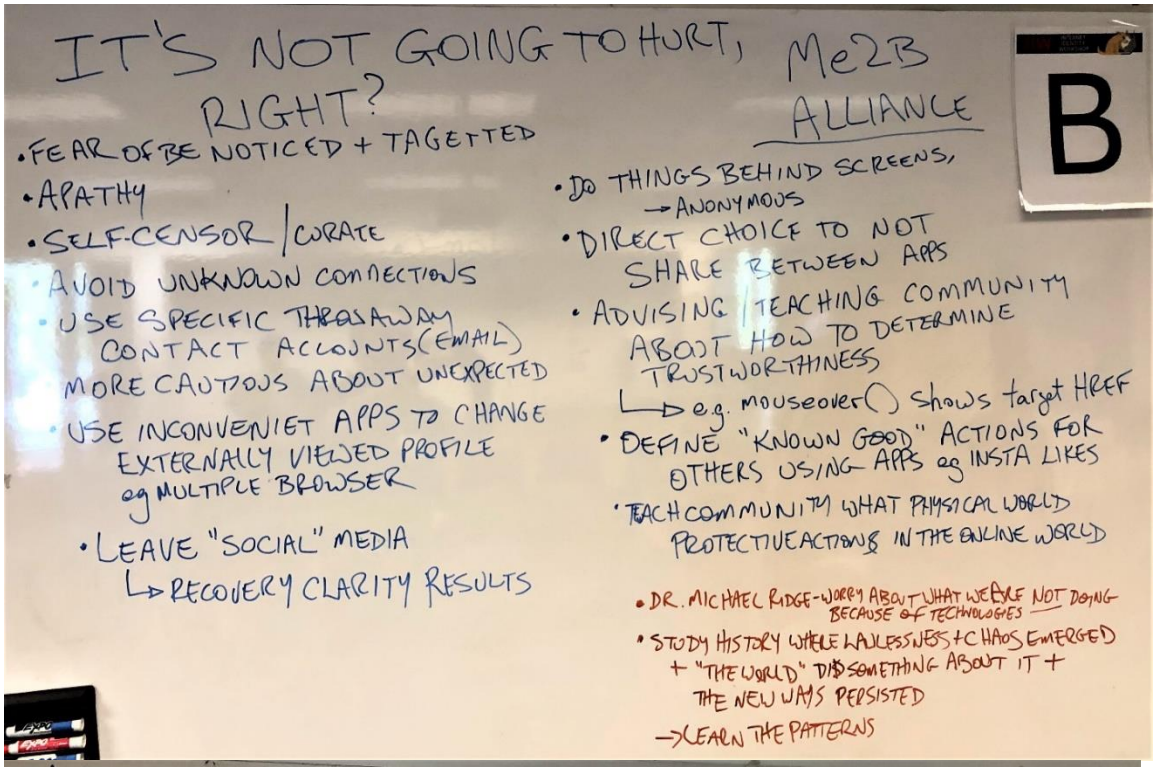
The Medium is the massage. The technology is the rails in which we interact and behave.
Reality and posturing.
I'm in the trust business, I don't trust the internet.
Eventually we will see regulatory discussion to reduce the public harm
The social norms are changing

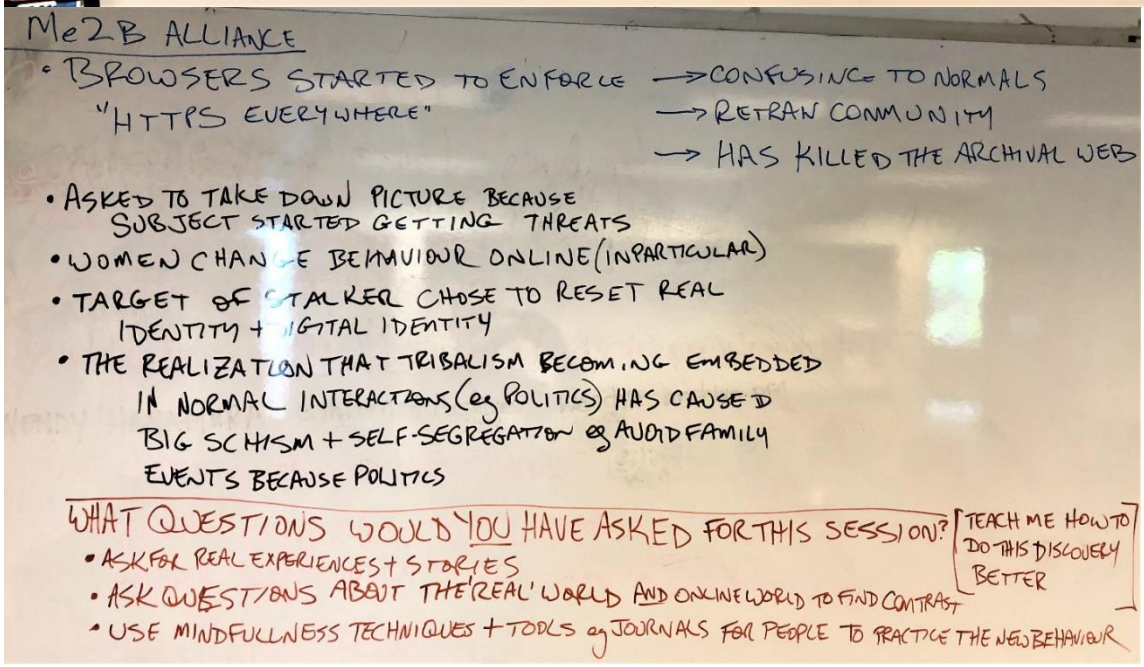
What questions would you have asked for this session?
(Teach me how to do this discovery better?)

- Ask for. Real experiences and stories, "being street smart"
- Ask two different sets of questions for online and offline behavior/world to find contrast – to explore online disinhibition effect
- Use mindfulness techniques and tools e.g. journals for people to practice new behavior/identify + document behavior in the moment.

********** ********** ********** **********

Notes/Photos received from Andrew Hughes:


IT'S NOT GOING TO HURT, RIGHT?
•FEAR OF BE NOTICED + TAGETTED
•APATHY
•SELF-CENSOR/CURATE
•AVOID UNKNOWN CONNECTIONS
•USE SPECIFIC THROWAWAY CONTACT ACCOUNTS(EMAIL)
•MORE CAUTIOUS ABOUT UNEXPECTED
•USE INCONVENIET APPS TO CHANGE EXTERNALLY VIEWED PROFILE eg MULTIPLE BROWSER
•LEAVE "SOCIAL" MEDIA
↳RECOVERY CLARITY RESULTS
Me2B ALLIANCE
•DO THINGS BEHIND SCREENS, →ANONYMOUS
•DIRECT CHOICE TO NOT SHARE BETWEEN APPS
•ADVISING/TEACHING COMMUNITY ABOUT HOW TO DETERMINE TRUSTWORTHINESS
↳e.g. mouseover() shows target HREF
•DEFINE "KNOWN GOOD" ACTIONS FOR OTHERS USING APPS eg INSTA LIKES
•TEACH COMMUNITY WHAT PHYSICAL WORLD PROTECTIVE ACTIONS IN THE ONLINE WORLD
•DR. MICHAEL RIDGE-WORRY ABOUT WHAT WE'RE NOT DOING BECAUSE OF TECHNOLOGIES
•STUDY HISTORY WHERE LAWLESSNESS+CHAOS EMERGED + "THE WORLD" DID SOMETHING ABOUT IT + THE NEW WAYS PERSISTED
→LEARN THE PATTERNS
B


Me2B ALLIANCE
•BROWSERS STARTED TO ENFORCE "HTTPS EVERYWHERE"
→CONFUSING TO NORMALS
→RETRAN COMMUNITY
→HAS KILLED THE ARCHIVAL WEB
•ASKED TO TAKE DOWN PICTURE BECAUSE SUBJECT STARTED GETTING THREATS
•WOMEN CHANGE BEHAVIOUR ONLINE(INPARTICULAR)
•TARGET OF STALKER CHOSE TO RESET REAL IDENTITY + DIGITAL IDENTITY
•THE REALIZATION THAT TRIBALISM BECOMING EMBEDDED IN NORMAL INTERACTIONS(eg POLITICS) HAS CAUSED BIG SCHISM + SELF-SEGREGATION eg AVOID FAMILY EVENTS BECAUSE POLITICS
WHAT QUESTIONS WOULD YOU HAVE ASKED FOR THIS SESSION?
•ASK FOR REAL EXPERIENCES + STORIES
•ASK QUESTIONS ABOUT THE 'REAL' WORLD AND ONLINE WORLD TO FIND CONTRAST
•USE MINDFULLNESS TECHNIQUES + TOOLS eg JOURNALS FOR PEOPLE TO PRACTICE THE NEW BEHAVIOUR
TEACH ME HOW TO DO THIS DISCOVERY BETTER

Get Real ONFIDO ID on Your Connect.Me Digital Wallet

Thursday 12C
Convener: Vladimir Vujovic & Michela Casaldi
Notes-taker(s): Vladimir Vujovic

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

Notes for: Deep dive demo - Connect.Me + Onfido credential
https://docs.google.com/presentation/d/1dEUUSLCnLPO7WBKPhKzU78eFak1_CxQ5_sDBUq6tIcU/edit?usp=sharing

On the session we explained how we have integrated Connect.Me digital wallet app with Onfido Issuer Service, how to get Onfido ID credential, issued by Onfido on the Sovrin MainNet, how that credential can be used to open an account with financial services companies who require ID verification upon account creation. And we demonstrated the whole flow on the session

Wireline P2P O/S

Thursday 12F
Convener: Pete Rowley
Notes-taker(s): Pete Rowley

Tags for the session - technology discussed/ideas considered: P2P, IAM

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

Nodes are self sovereign
Applications run on nodes
Activities produce a Feed
Can be many devices in the self sovereign domain
They read each others feeds
Work on the same resources
Many Participants form a Party
All working on the same resources, using the same apps
They each read and replicate the others feeds (high availability)
Each node merges all Party Feeds into a MegaFeed
MegaFeed resolves into changes to application state
The result is what the participant sees
Everyone guards their own view of the Party state
Cooperating messages form the view
Messages that break the model are ignored
Everyone who is cooperating arrives at the same view
Authority to take actions is defined within the model (Hierarchical, consensus...)
Feeds prove Authorization before taking restricted action
Link to Wireline P2P Slides: http://www.keepandshare.com/doc20/view.php?id=19424&da=y

What Do Activists Need To Know?

Thursday 12G
Convener: Carolyn Tackett
Notes-taker(s): Elizabeth Stephens

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

Access Now introduction

Coalition building process. Working in local contexts in countries where national ID systems have already been put in place or where these systems are being considered. Why is there this sentiment that this type of digital ID system is inevitable? Do we accept that as a premise?

Is it all good governance? Estonia vs. India example. Why is it working in some states and not in others? Does it just come down to good governance?

Even if you have good laws but no accountability or regulation scheme

Having it be decentralized as opposed to one national ID. The China system - they know everything about you and when you jay walk you can't rent a car. The decentralized approach. Our card that's for driving and passport. It can integrate around me it doesn't have to integrate at the governmental level. Technically that's what I think in general. But they love these experiments — Adhaar. 1.2 billion people experiment. There were only 4 data points and then the government got involved and added so many more. Work with ID2020 and Omidyar Network and the question is, is how the small countries…they want to be one of the big boys. Our country's smaller and they want to copy the work of the bigger companies, buying off the shelf eIDs that they can just deploy. They can't build a decentralized thing and these things are chaotic and right now we are both too early and too late at the same time.

Consolidated ID for Canada across Canada. You want a government to be efficient. They collect taxes and enforce laws. Services should be insanely efficient. It's more important to have a non police state than for things to be efficient. You want to promote anonymity if you don't trust the gov, if you do…

You can trust a government in that current moment but there needs to be accountability under any circumstances. If we think they won't exploit it now, then why not build a decentralized system that can't be exploited.

I can be different "identities" for different purposes. Those bits of information don't need to talk to one another. Why do we want a single unified thing? So it can keep track of you.

We don't want everything to be efficient. And if everything is too convenient and the speed…we can't get both.

Separate identities for separate interactions. Person 1,2,3 is entitled to vote. If that could be done really cheaply and efficiently. There are coordination costs. The illusion of economies of scale.

If you weren't a bad actor before, you might become a bad actor. How do we explain to them that the costs will be better, that people will be happier. They're looking for the UN to say these are the ones that are

good to use and

All of these international players are part of the problem. They're selling the idea that these centralized models are useful. Conversations in UNCHR.

We're missing the refugee gang (those working in eID in development settings) We have a working group called ID for all working on decentralized ID use cases how to make eID more accessible — refugees, old ladies who can't use phones — across the world. We have to start our identity somewhere. We have to start decentralized.

All these little technologies are deployable. Something will run on a 5 dollar PC that has a scanner and a cryptographic thing in it that issues tokens with a QR code, then all I have to show is my little QR code that's cryptographically sign. Even if it's a biometric click at the end and a cheap little system to run it, you could give them away.

Very anti UN being the golden standard setter. Highly controlled (government funding)

Like the idea of these cheap hardware device. Anything else you have interoperability issues.

Here's the 25 buck phone and it does need to connect. Facebook decides to make it free and then FB is suddenly the internet. Where do you go with these ideas? You start in the places without laws so you don't have to tear down any infrastructure. Why Jeff Airies wants to work only in places where this infrastructure doesn't exist.

Democracy.earth - it's about identity. I don't necessarily approve of the approach you prove your identity via video. I think that ideas like this are out there. Aragon is another one. It's about governance and organization

Digital Life collective is another one talking about governance. Working with a leader making an interactive map for this community so that any community can map themselves. Connecting tool builders and apps together. Tech we Trust. Spent 2 months in India. Interested in sharing.

Working with governance Medici Land Gov where governments aren't that strong and people want to assert their rights especially when there are mining cos coming in. We want to find ways - videos, pictures - where we can start recording them now so that they can say 10 years from now that they were here and this is their land.

History of the Alaska Native Land Claims. When land was taken from Americans Russians, the natives had remarkable informal systems of land ownership. Here is the evidence that every fall I went fishing here. US government had them arbitrate. This is about establishing after the fact those claims.

If you read the Mystery of Capitalism, chapter 5 talks about how the US started this way.

Serving communities that already aren't integrated into a broader system. They don't necessarily want to be part of the formal system, but maintain theirs. T

One of the things I'd like to see is this community getting some pilots done — any institution can issue an identity to anyone. Communities that have identities within themselves can issue credentials within themselves. Ethiopia has an in tact local registry system that's all on paper. All you have to do is digitize it

using decentralized registry but the World Bank is pushing them to create a centralized digital ID. The World Bank is funding over a billion dollars in loans to implement Aadhaar systems in 10 African countries. We have to move faster, and we can with the help of the big companies Microsoft, etc. We have to get the consultancies involved. Deloitte is working with one of the companies in this community. Centralized systems cannot scale for the complexities of the whole society.

SSI is one of the options. Not the option, is what these consultancies' papers are saying. Subsidiarity is that decisions should be made on the lowest possible level. The higher level the decision making is done the more unrest is trickling down. There's more business for everybody if everybody has to duplicate various processes. To me this concept of subsidiarity really works as a philosophical conclusion about how decentralization in the technology could work for humanity. People designing things get the idea that they should just design the whole thing, but the interfaces are so important.

I think to have the option is best. Liquid Democracy.

James Scott's work is really important. Seeing Like a State. How land tenure and identity registration systems. The Art of Not Being Governed. People who left the plains. Who got out of where you could be governed and got out and went to the hills so they could be ungoverned (self governed). I have a real problem with the concept that 1.1 billion people without identity is a problem. For people in cities yes, it can be a problem.

What is the issuing of that "identity" credential for?

We're at the beginning stages, access now. Here are the reasons why this is important to present to decision makers.

How do we know we're the good guys and how do we differentiate ourselves from them? How do you educate and build consent?

Need to involve the local populations, raising issues, not imposing solutions.

Human centered design focused? Yes.

Start to develop resources for civil society people so that they can accurately assess when government wants to impose systems of any kind.

Who owns the future by Jaron Lanier Universal Basic Income project

Sidetree On Ethereum "Element"

Thursday 12H
Convener: Karyl Fowler (CEO, Transmute) & Orie Steele (CTO, Transmute)
Notes-taker(s): Margo Johnson

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

Technology Discussed: Scalable Decentralized Identity & Attestations
Creating DID using Element -- DID:ELEM

Demo of Sidetree Ethereum: https://www.youtube.com/watch?v=KY_dt2tKQxw
Go to element-did.com to try the demo
Contribute! https://github.com/decentralized-identity/element

Went through in the video:

1. Creating and importing an encrypted wallet
2. Creating DID document using both light node and full node methods
3. Batching and creating more than one DID at a time
4. DIDs are created, resolvable in light and full node
5. Updating a DID document in full node, new operation to add service node
6. Multiple service endpoints on DID document
7. Currently supports Create and Update
8. See tests in element implementation for Recover and Delete (will be added to UI later)

Q&A

Is Transmute currently hosting a node?
Yes, Transmute is running a node -- using Infura to host.

Gihhub repo, where is the solidity code?
It should be in the Element lib package in Github repo.

Differences from previous anchoring?
Element is initially being tested for scalable attestations
IoT device, Ad-tech platform… lots of attestations need some form of batching operation.
Currently use Element for anchoring attestation, mixed with ETHR as DID identity method. For example -- a ETHR-DID can issue ELEM-DIDs.

Public attestations?
Default behavior for element is to use IPFS as storage layer, so operations are public
But Element has a pluggable storage mechanism and can select different contracts.
Anchoring to a different contract is an option, could be to a private database
Operations only visible to permissioned users

Clarification about anchoring attestations...
Sidetree method used for anchoring DIDs — not just identities but also attestations

Service section of DID document
Service endpoint says there is anchored credential, if you have right privileges can access and verify information.

What about the sidetone protocol is useful for attestations? Why better than centralized database?
Centralized database can be better in cases - JSON LD signed and registered to DIDs
Sidetree as DID method has build-in CRUD support — can use same set of code for both use cases
Combination of infrastructure
Using mechanics of DID for credentials

Closing notes
Still testing with combination of ETHR-DID and ELEM-DID
Actively using in Transmute ID transmute.industries/transmute-id
Thinking through inter-operability from one method to another
Long run use whichever is most cost-effective, safest for anchoring

Ontology & Taxonomy: Crafting Chaordic Organizations In An Ontonomic World

Thursday 12J
Convener: Nicholas Racz
Notes-taker(s): Nicholas Racz

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

I discussed what Ontologies and Taxonomies define, and how taxonomic definitions serve as the foundation of Ontological derivation. I enumerated on how Ontologies stack, and how higher order Onotologies operate on lower.

Nathan took the baton of explaining how Ontological development in context of Sovrin. We had an active discussion on how Ontologies are socially decided on.

TL;wasn't there: Ontologies by nature are fuzzy, and need to be built from taxonomic foundation blocks toward a teleos.

Linked is the PPT file.
https://drive.google.com/file/d/1Egnj_uySX74mEnZF4sWRMZp4MiF_jZ0k/view?usp=sharing

(We stumbled upon a Ontologic framework that by accident works one to one to Sovrin's inherent ontology.)

Hub/Agent Action Meta Protocol

Thursday 13A
Convener: Sam Curren
Notes-taker(s): Thomas Berry & Sam Curren

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

Notes received from Thomas Berry:

Action interface and its merits:

- things you do has flows
    - Example of the hub flow model
        - Collections endpoint (is CRUD with semantic)
            - Objects embedded: Gs1.com, products
        - It has things like storage for states
        - The interfaces are setup to be able to talk to common components
    - for actions [inherited], the way that tasking works...
        - Image a numeric map, unique
        - [C: This is Threads]
    - states can keep accruing; the addition of new state objects
        - In the application it shows as a chunk of data
        - An object string that evolves over time
    - the schema is model-less; it is inherited
    - Offer: bid/ask
    -
    - C: [the hub is not only thing involved in the flow]
    - [The interacting agent is in on the task]
    - The task is only relevant to the aspect of relationship between two agents
    - The hub doesn't necessarily hold the actions of all agents; but, it can when the task depends on it.

Use case

- Buyer/seller interactions tasks are only involved in the actions from each perspective (not unified)
- Bidder/Auction interaction tasks are collected as a whole; all actions across all agents are consolidated

What we're trying to do is charted (not centralized, decentralized, or distributed) state-management between parties; when there is a central server (hub) involved, each party holds the transactions between the parties.

State is what you want state to be.

Two agents are developed independently; the agents what to have they're attributes and states.

But, there are generics that pertain to all parties; everything is an action (schema.org/actions)

What common properties must every interaction have? schema.org/actions

Attributes (required in bold)

- Status
- Agent (driver of the action: john wrote a book)
- End time
- Error
- Instrument
- Location
- Object (of the action: john's book)
- Participant (co-agent or co-author or role)
- Result
- Start time
- Target (for an action)

Whoa! This hasn't been built yet.

Not everything being done is a "task"

Are the objects being passed around? Only if the action is relevant to the interaction between the two parties Invite->RSVP... don't pass the invite back if RSVP is being conveyed.

C: schema.org/actions attributes doesn't apply; if you use schema/actions you have to use it is documented in schema/actions

[Trying to find a way for business actions to operate]

Message family

```
@type trustping/1.0/ping
@id ~

@type trustping/1.0/ping_response
@id
~thread { ... }
```

Actions

Alice's Phone app
POST to HUB
@type Action
payload: { action object for ping }

HUB inserts it into an array

Bob's phone app
GET from HUB
@type

The model for protocols interjects agent-to-agent comm to storage ...
You can never operate outside the paradigm

- Hubs are intended to replace wire messages with routing
- Something is posted to the hub and synchronized around to the intended destination
- The Hub is nothing but a data store that agents interact

The wire protocol would allow the Hub to arbitrarily act on an action
The action is intended to have a dumb HUB which takes no action on a message

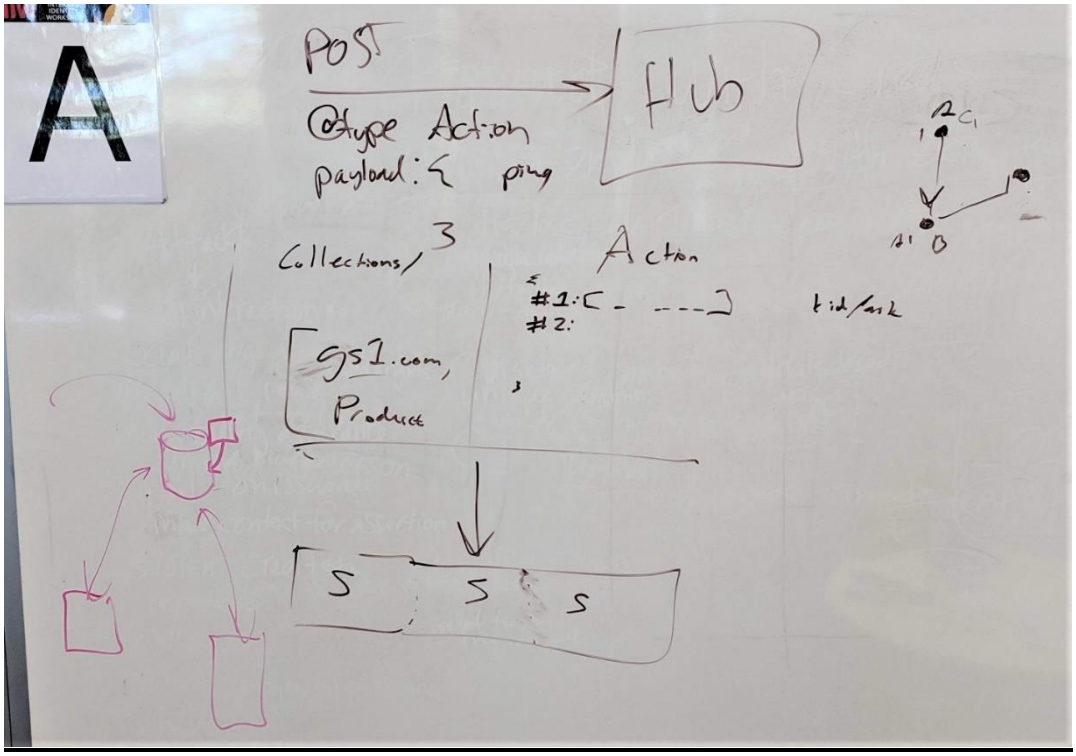
********** ********** **********

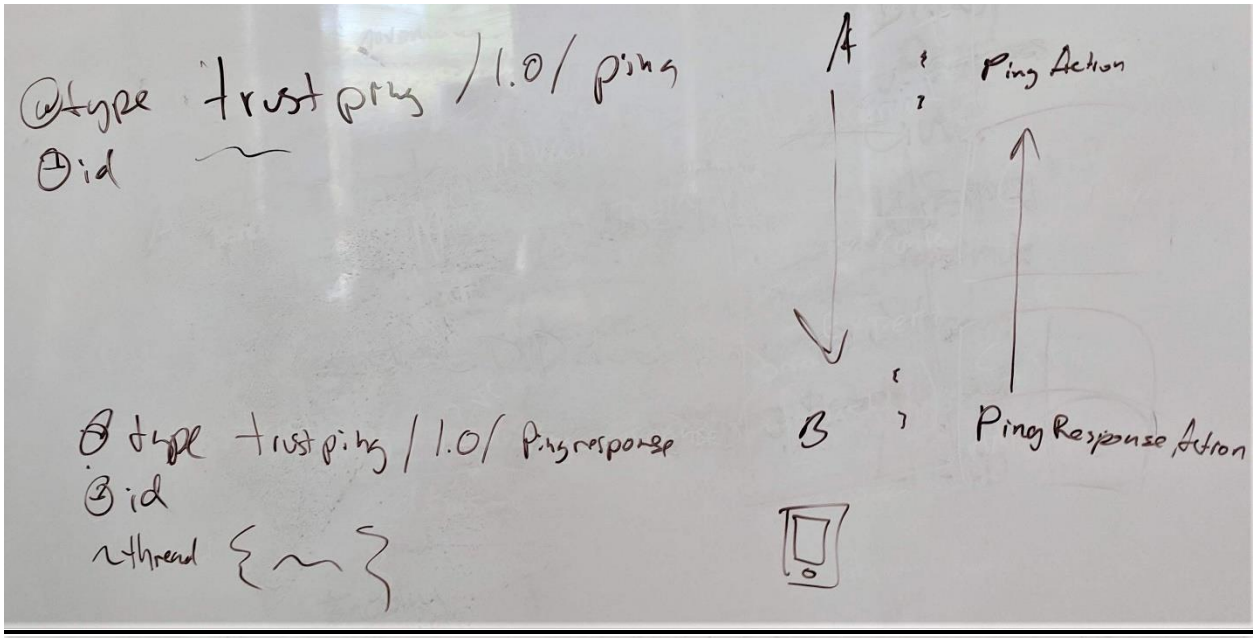
Notes & Photos received from Sam Curren:

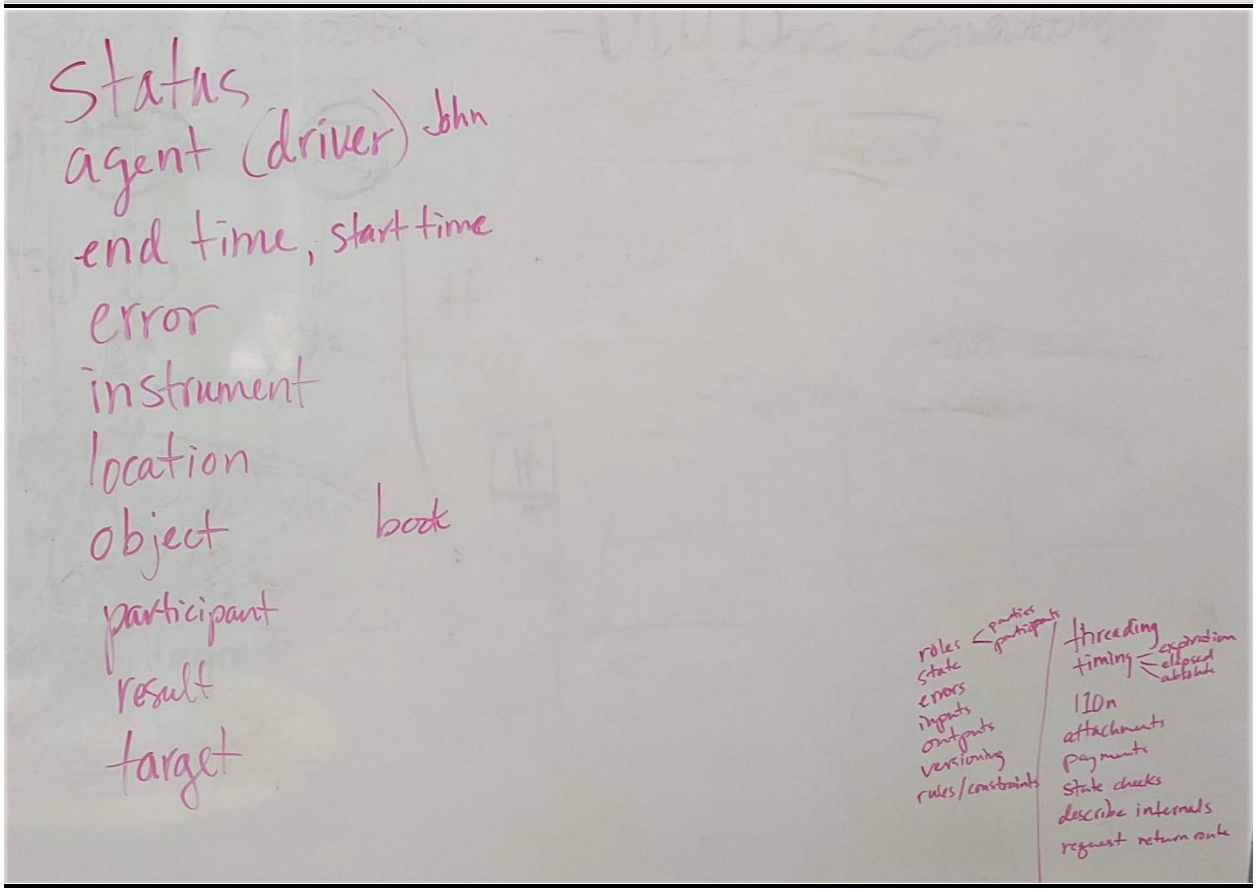
We discussed the approaches that DIF Hubs use for Protocols called the Action Interface. We compared that to IIW Protocols as message families.

Outcomes: We will further compare the approaches using existing examples from the Indy community in more detail to draw out important elements of each approach.

That work will happen in DIF Storage and Compute WG calls and in Hyperledger Aires Community calls (if necessary for openness).




@type trustping /1.0/ ping
@id
A
Ping Action
@type trustping /1.0/ Pingresponse
@id
~thread {~}
B
Ping Response Action


status
agent (driver) John
end time, start time
error
instrument
location
object book
participant
result
target
roles
state
errors
inputs
outputs
versioning
rules/constraints
parties participants
threading
timing
expiration
elapsed
absolute
IDn
attachments
payments
state checks
describe internals
request return route

Social Contract: Universal Guiding Principles

Thursday 13B
Convener: Lisa LeVasseur & Richard Whitt
Notes-taker(s): Lisa LeVasseur & Andrew Hughes

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

Notes received from Lisa LeVasseur:

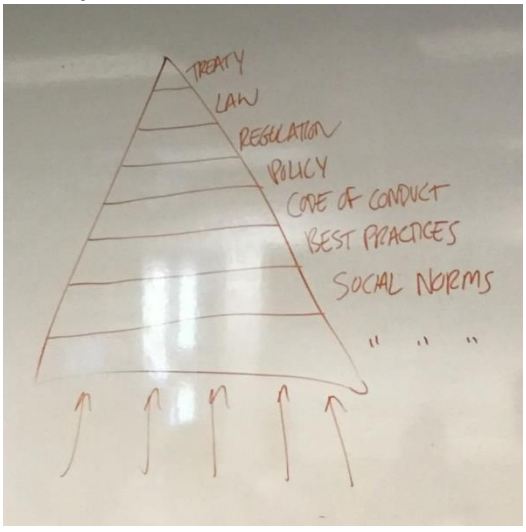
- John Locke quote: from The Two Treatises of Civil Government
- This is a moment in history when a lot of thought went into government – what it is, to take over what a monarch/despot used to do.
- We are in a new place here. We were in a new place when print came along.
- The social contract we have – that needs to apply online. It doesn't.
- Other side of this spectrum is Thomas Hobbes.
- John Locke is the idealized nature of what it should be.
- The global view, has no shared understanding.
- Looking for a list of universal principles.
- Defend against approaching discussion from a single cultural viewpoint.
- Is there/should there be a set of universal principles
- Analyze the good in the world and model on that
    - If it exists in the world, it can become a law (Elinor Ostrom)
    - Focus on the positive reinforcement
- Do the 8 laws of ethically-designed AI.
- Universality is a western concept. There are other ways of seeing human identity. E.g. African view of I am, because you are.
    - One of the key IEEE EAD1e feedback, was this was very western. And there was an effort to get and incorporate this feedback.
    - The principles are very high level, you can still have disagreements on the details.
- We are in a battle about what the dominant narratives are for the future.
- China social contract – that was the birth of the Chinese nation.
    - 400 BC reforms of sheng yang led to foundation of China 222BC
    - Everyone is in a group of 5 able bodied men. If someone did something bad, you all got punished, if someone did good they all got credit and benefit.
    - Defend the smallest social unit of responsibility + ingrained in. Feeling of safety in group rather than the individual.
    - Mai Lin, shared the Chinese model, it's an accountability model. It's completely non-tech.
- Is this technology itself the. Problem?
    - Need a slow food movement for tech
    - What are the embedded moral foundations that are at the root of the "bad"
        - E.g. productization, monetization
    - Tech is simply our current framing. This is not simply tech.
- Has the tech caused a disconnect between the action and the harm?

- **What is the right kind of accountability that needs to reemerge?**
- The nature of the digital world is fundamentally different from the natural world. Suddenly nature is changing at this (fashion) speed. We are in a completely different field.
- Agile is cultivation of sloppiness.
- What I see missing, different incentives. The incentive became a burden, and in that story it is about protecting the other 4. Can we find commonalities about aligning incentives?
- You could plug in, pick your favorite religion for the stating point of the discussion – we use social contract.
- In real life there is deternance, but we don't have that online, and that's a problem.
- What if you have a bot, that is programmed to do things, and it's programmed to break the norms and it does some harm?
- Dan Ariely – Skin in the game book – when you have skin in the game it changes your behavior in the system.
- More foundations theory, feels male and legal… this bias might be due to my presenting of them (I'm male, western, legal).

Example Models / **Ethically Aligned Design Principles: IEEE EAD1e**

1. Human Rights
2. Wellbeing
3. Data Agency
4. Effectiveness
5. Transparency
6. Accountability
7. Awareness of Misuse
8. Competence

Social/Institutional Constraints on behavior



- It looks like there is a filter at each level?
- Is that filter thing true?
- Is there one principle that guides us in the selection of this filter?
- There is interaction between the layers
- These are layers of abstraction

Moral Foundation Theory

These are the dimensions we care about. Good/Bad. What does it mean to do these things online?

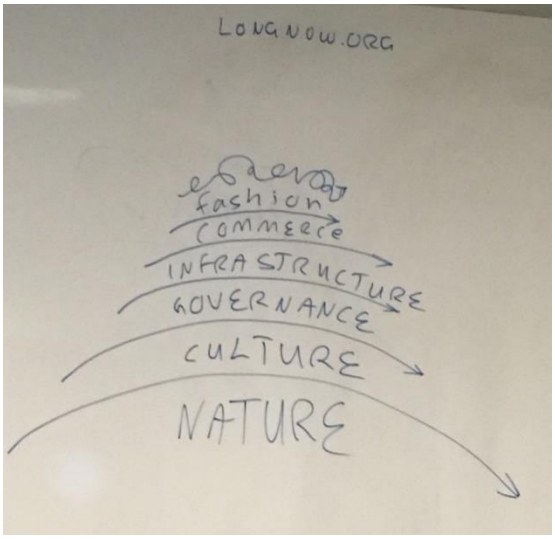
- Care/Harm
- Fairness/Cheating
- Loyalty/Betrayal
    - You expect the website you are trusting will not screw you
- Authority/Subversion (Golden Rule)
    - Don't hack, don't spread malware
- Sanctity/Degradation
    - There will be religions (open source, android), there are things that are sacred.
    - Translate this into respect
- + Liberty/Oppression
    - Open source vs non-open source

Go and read the actual theory.

Bring your own perspective to the discussion.

What we're missing here, is

- We're all talking about technology
- We want them to succeed
- Technology itself is a problem, and needs to be stuffed back in the box, by slowing it down.



<u>Photos received from Andrew Hughes:</u>

OBSERVATIONS

HTTPS://ME2B.US

SUBSCRIBE TO THE EMAIL LIST!! ①
LISA@WRETHINKING.ORG

- DEFEND AGAINST APPROACHING DISCUSSION FROM A SINGLE CULTURAL VIEW POINT
- IS THERE/SHOULD THERE BE A SET OF UNIVERSAL PRINCIPLES (NOTE THAT 'UNIVERSALITY' IS A WESTERN PHILOSOPHY)
- ANALYSE THE "GOOD" IN THE WORLD + MODEL ON THAT
  - → IF IT EXISTS IN THE WORLD IT CAN BECOME A "LAW"
  - → FOCUS ON THE POSITIVE REINFORCEMENT
- DO THE 8 PRINCIPLES OF ETICALLY-ALIGNED DESIGN
- "SOCIAL NORMS COME FROM NARRATIVES"
  - WHAT NARRATIVES DO WE WANT INORDER TO SHAPE THE NEXT NORMS
- "I AM BECAUSE WE ARE"
- HOW SHOULD THE FEAR OF REPERCUSSIONS BE RESTORED?
- STARTING POINTS MATTER "S RESPONSIBLE FOR THE ACTIONS OF I" ie if I does bad, all are responsible
  - → CRF. 400 B.C. Reforms of Shang Yang 'cult to formation of China' → DEFINED THE SMALLEST SOCIAL UNIT OF RESPONSIBILITY + INGRAINED IN FEELING OF SAFETY IN GROUP RATHER THAN THE INDIVIDUAL
- IS (THIS) TECHNOLOGY ITSELF THE PROBLEM? (A: TECH IS SIMPLY OUR CURRENT FRAMING. THIS IS NOT SIMPLY TECH)
  - → NEED "SLOW FOOD" MOVEMENT FOR TECH
  - WHAT ARE THE EMBEDDED MORAL FOUNDATIONS THAT ARE AT THE ROOT OF THE "BAD" eg PRODUCTIZATION, MONETIZATION
- HAS THE TECH CAUSED A DISCONNECT BETWEEN THE ACTION + THE HARM?
  - → WHAT IS THE RIGHT KIND OF ACCOUNTABILITY THAT NEEDS TO REEMERGE?

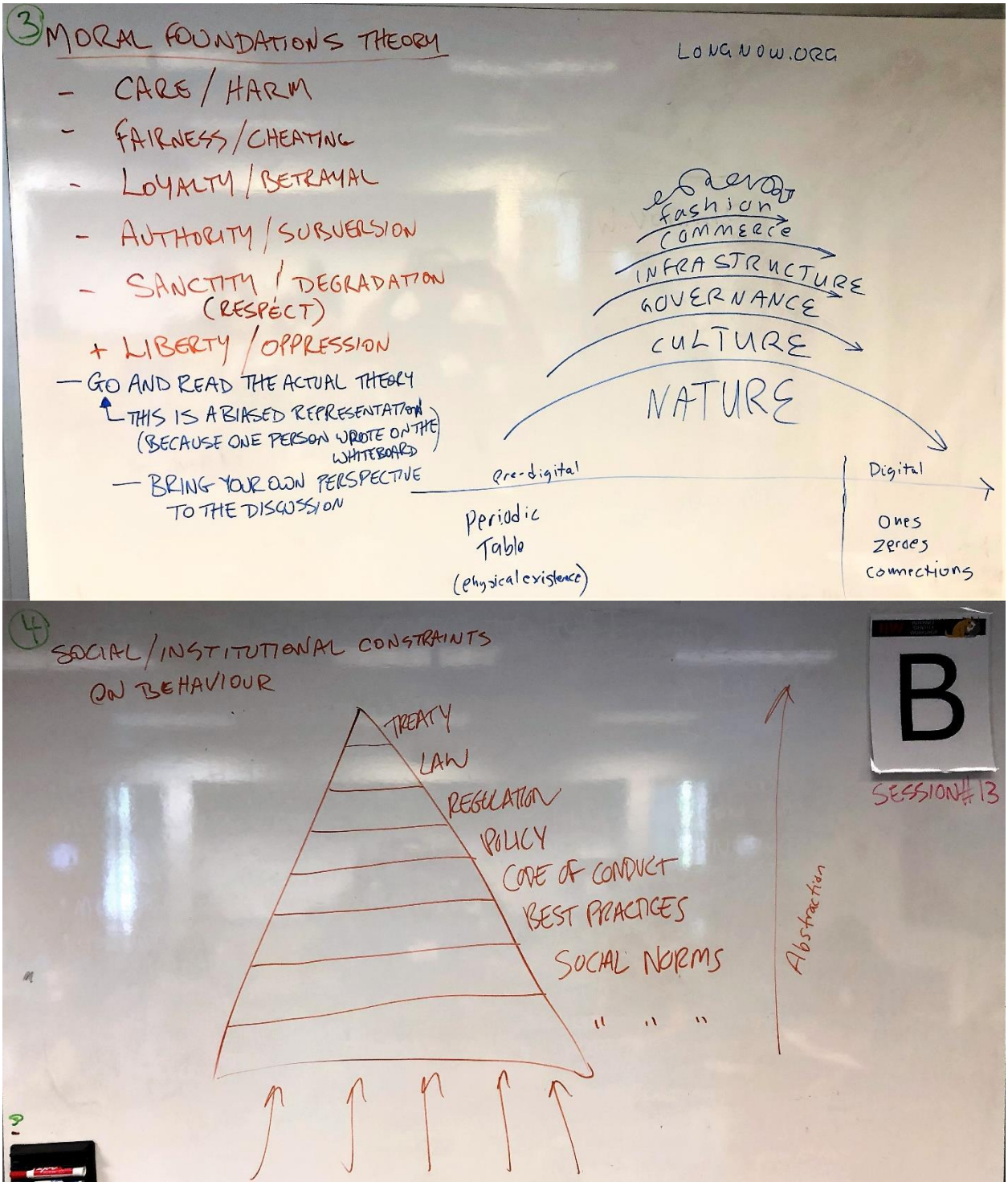
Golden Rule

TALEB
BOOK: "SKIN IN THE GAME"
- WHEN YOU HAVE SKIN IN THE GAME IT CHANGES YOUR BEHAVIOUR

Ethically Aligned Design ②

1 Human Rights
2 Wellbeing
3 Data Agency
4 Effectiveness
5 Transparency
6 Accountability
7 Awareness of Misuse
8 Competence

[IEEE EAD1e]

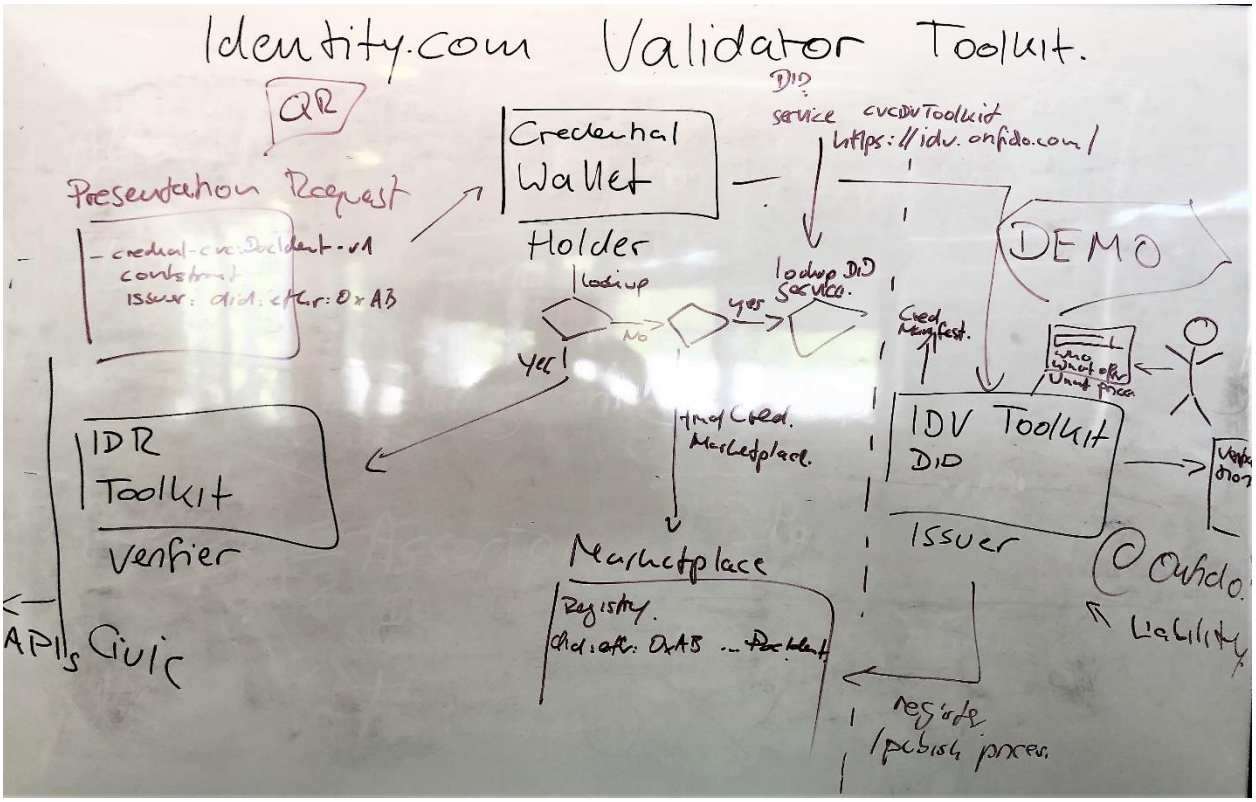

3
MORAL FOUNDATIONS THEORY
- CARE / HARM
- FAIRNESS / CHEATING
- LOYALTY / BETRAYAL
- AUTHORITY / SUBVERSION
- SANCTITY / DEGRADATION (RESPECT)
+ LIBERTY / OPPRESSION
— GO AND READ THE ACTUAL THEORY
↳ THIS IS A BIASED REPRESENTATION (BECAUSE ONE PERSON WROTE ON THE WHITEBOARD)
— BRING YOUR OWN PERSPECTIVE TO THE DISCUSSION
LONGNOW.ORG
fashion
commerce
INFRASTRUCTURE
GOVERNANCE
CULTURE
NATURE
Pre-digital
Periodic Table
(physical existence)
Digital
Ones
Zeroes
Connections
4
SOCIAL/INSTITUTIONAL CONSTRAINTS ON BEHAVIOUR
TREATY
LAW
REGULATION
POLICY
CODE OF CONDUCT
BEST PRACTICES
SOCIAL NORMS
" " "
Abstraction
B
SESSION# 13

The Identity.com Validator Toolkit: Demo with Onifido & Zoom Integration

Thursday 13C
Convener: Martin Riedel
Notes-taker(s): Martin Riedel

Tags for the session - technology discussed/ideas considered:

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



- Introduction to Identity.com Principles of ID Requester, ID Validator and Credential Wallet Toolkit
- Introduction to Marketplace to offer and discover Issuers of Verifiable Credentials
- Demonstration of a Presentation Request Flow and how Missing Credentials can be discovered on the Marketplace
- Technical Demo about the Verification Process with an Issuer
- Demonstration by collecting
— Document Scan via Onfido
— Selfie Capture with Liveness via ZoOm
- Verification and Capture of OCR'd data
- API Documentation and Demonstration
- Mobile Demonstration

How SSI Can Disrupt Platforms: Uber, AirBnB, FB, PayPal, Ebay, etc.

Thursday 13D
Convener: Timothy Ruff
Notes-taker(s): Ben Gregori

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

Because SSI enables you to own your identity in relationship with others, it opens the door for vendors to respect personal borders and ask for access in exchange for providing a service.

- It will become easier/more economically valuable
- Rich/wealthy people will want to use it
- Once it becomes possible, it will become inevitable.

Protocols kill platforms – platforms are the walled garden that make it easy for people to use. But they're limited, and eventually will not be able to offer all of the services that people demand. Limitations of the platform create incentives for new entrants.

Disintermediating the users from a platform needs a common language (protocol), and it opens the relationship

- Like email before SMTP: dependent on the email interface. Not with SMTP. So you can host a server and be independent in your email, but if you use Gmail then you're identity is tied to google regardless of SMTP

OTT vs. SMS – SMS is a protocol, over the top (internet) is owned by platforms now, and requires them as intermediaries.

Sam Smith – open reputation (decentralized reputation)

- At first, most won't trust it, but it will enable new entrants that provide more economic value than the incumbents.
- People will not want info held hostage…they will rather want something EASIER that enables portability and protocols enable that.
    - Master place where credit card is held instead of reregistering
    - Address
    - Phone number (I can take it across carriers)

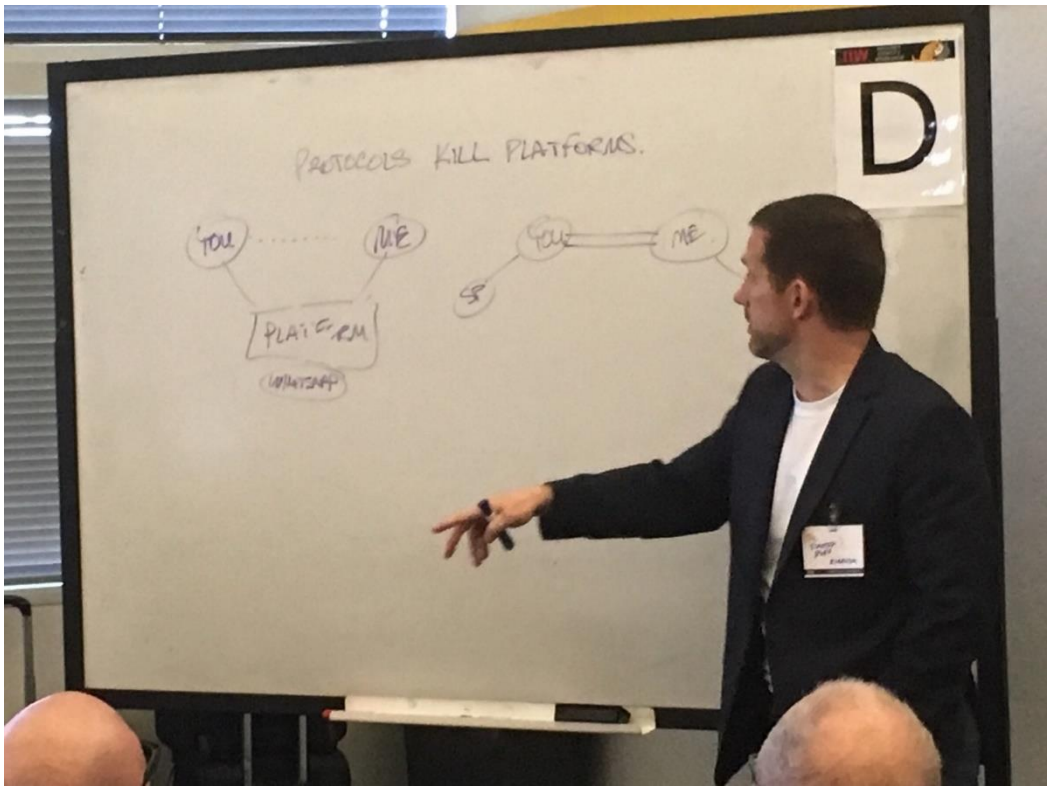
Example:
In this model, when you need a ride, you can broadcast that signal via protocol and ANYONE can answer because it's a protocol (lyft, uber, new entrants, etc). I can limit who can see my info automatically due to certain characteristics like reputation.

Example:
I need a mortgage, I broadcast that with three pieces of info: value of home (I have a home) attested by nondescript title company, credit score, some reputation of follow-through on transaction. Without revealing any PII, you can flip the switch and get mortgage providers to come to you (rather than having to market by a data aggregator like Facebook or Google).

- Same can be used for very specific parts (like obscure part for some foreign home appliance)

- Protocols don't have to be the perfect version, and they don't have to be the best. They will win due to adoption, and then updates can happen even after adoption has happened.

Clayton Christanson (Innovators Dilemma)
- Disruptive Innovation
- Sustaining Innovation



Off Chain (PKI) Key Management: 1 of N Proof Revocation Rotation, Didery Micro-Service, Lightweight Identity, Data Streaming/IoT, Self-Governing PKI

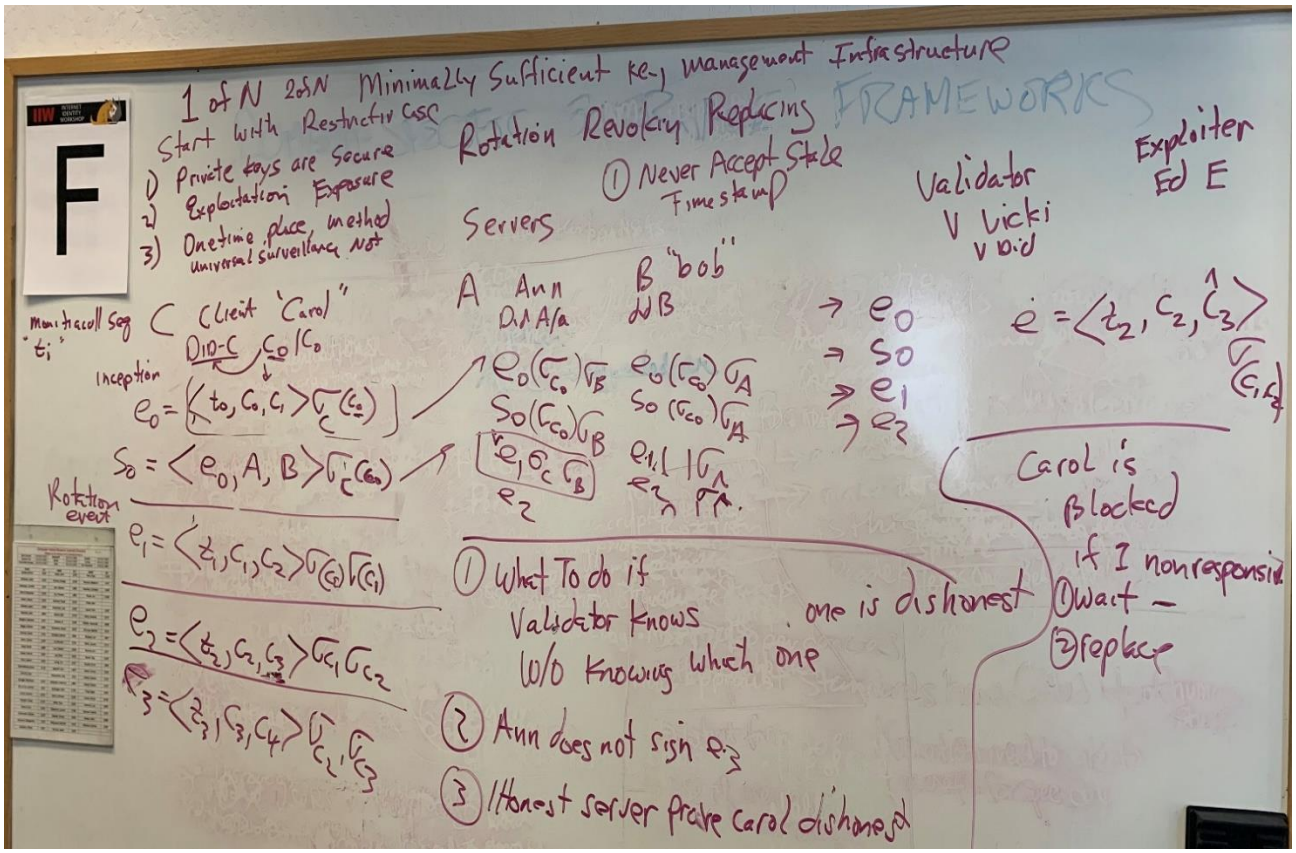
Thursday 13F
Convener: Sam Smith
Notes-taker(s): Sam Smith

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

Lightweight identity. Proof that may perform reliable secure key rotation without a distributed ledger but merely 1 honest out of N servers.

This was established with some caveats and maybe need 2 out of N. This enables more scalable architectures with data streaming or IoT for key management.

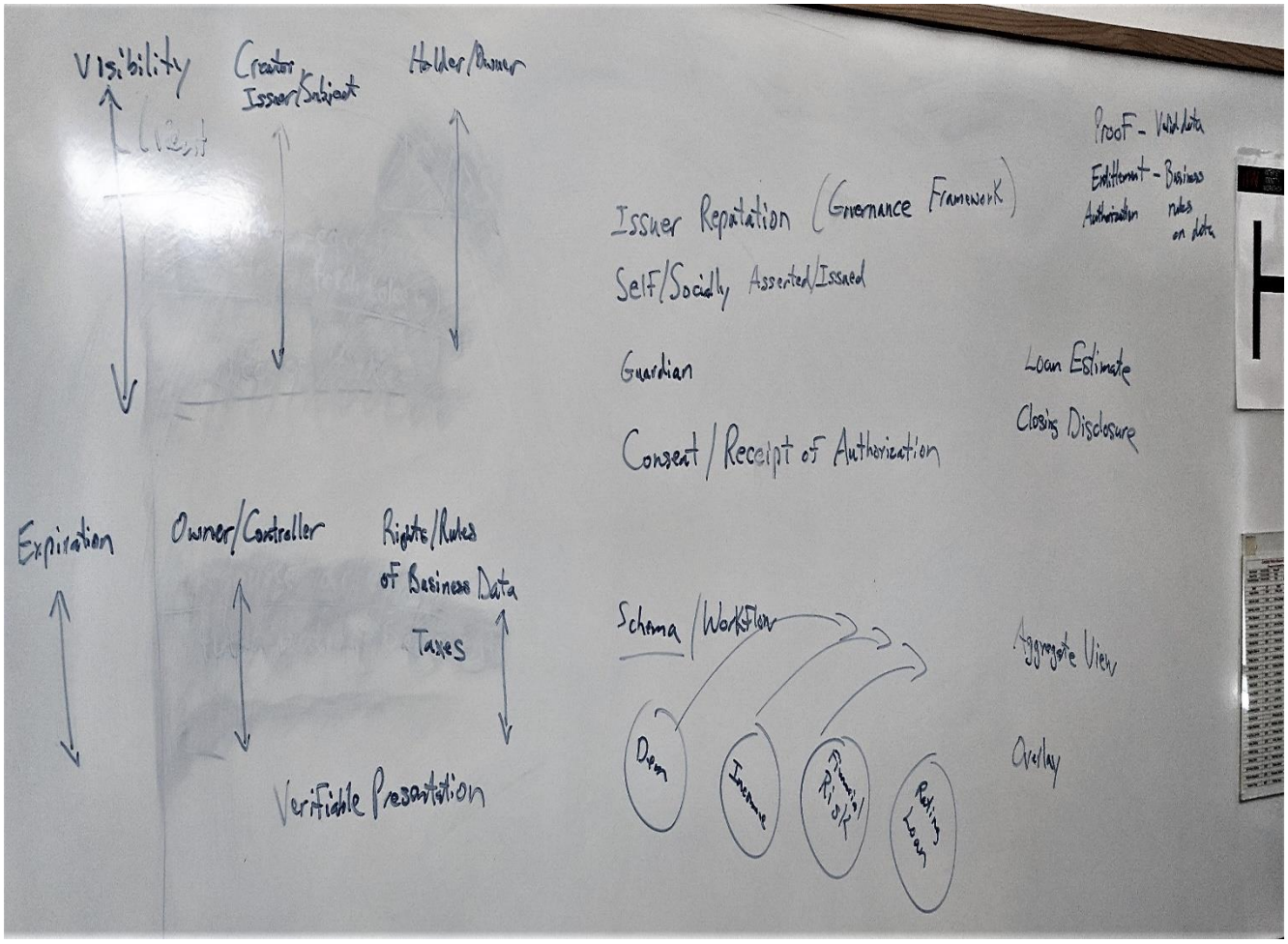
Established framework some additional work required.



Workflow/Forms & SSI Credentials

Thursday 13H
Convener: Matthew Hailstone
Notes-taker(s): Matthew Hailstone

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

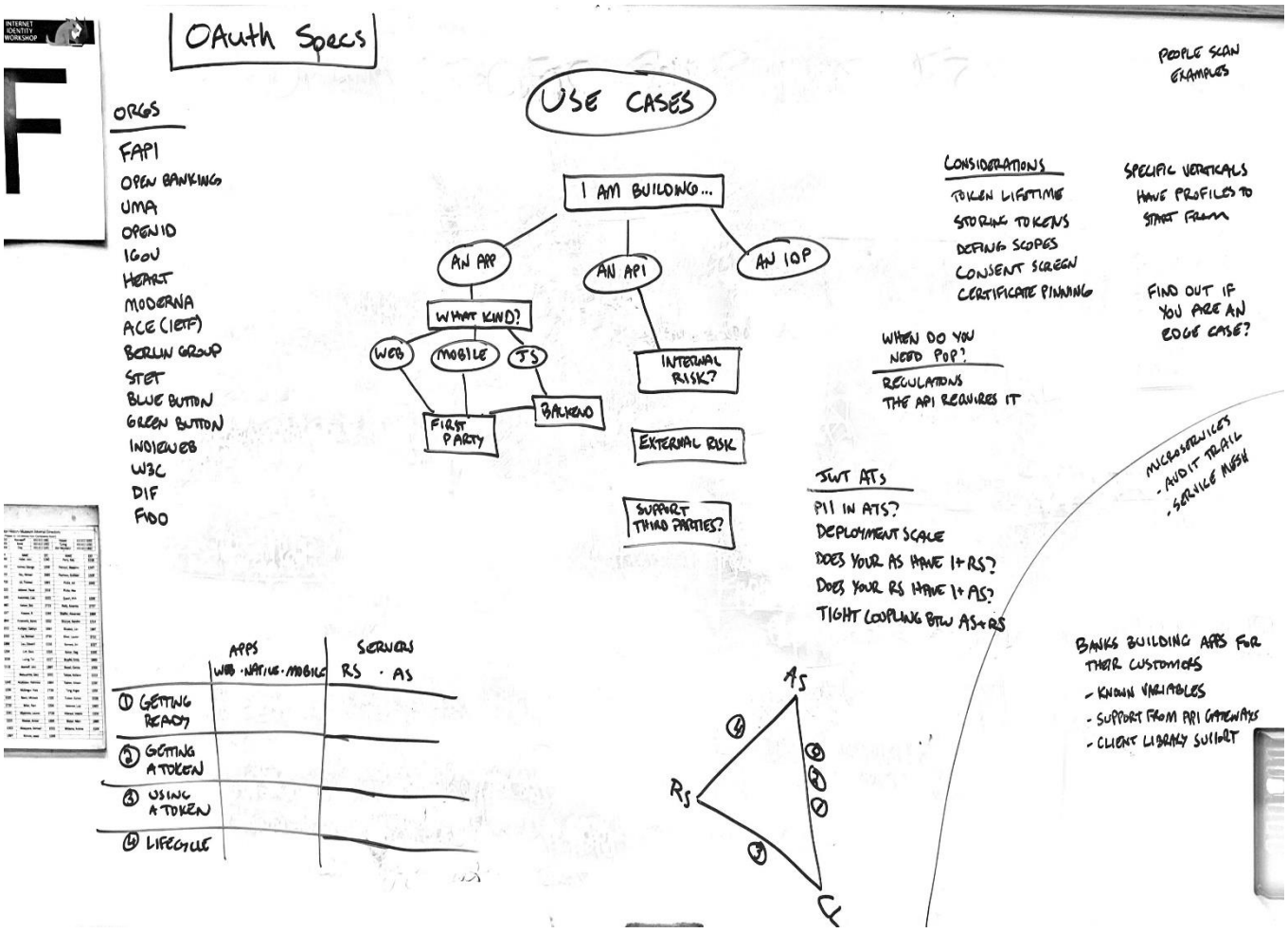


Let's Make A Map! Of OAuth Specs

Thursday 14F
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:

We brainstormed a few different ways of categorizing and presenting all of the OAuth specs. We discussed a few different possible visual presentations of the data to show related specs based on use cases, such as asking the viewer a series of questions about what they are trying to do in order to present them with the relevant specs. We also listed out all the different organizations we knew about that have built specs on top of the OAuth framework.



What I Learned In India About Their National ID System (Aadhaar)

Thursday 14G
Convener: Kaliya Young
Notes-taker(s): Kaliya Young

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

I was in India for two months between January and March to study their National ID system as part of the New America India-US Public Interest Technology Fellowship.
My research paper for this is focused on comparing the US Social Security Number system with the Aadhaar system. It will be released in June on their site.

The high level take away is that the India system is a vast and sprawling system. Each week I was in India I learned about a new piece of it or feature that I didn't know about.

The UIDAI was founded in 2010 and was a quasi-legal entity created by executive order with its head joining the cabinet even though they were not elected to parliament.

They devised a system to collect the biometrics of citizens along with demographic information and based on that issue to citizens a number via a card sent to them in the mail.

They managed to enroll all of the residents of India because they got other agencies to help and to pay them per enrollment. These included state level governments, the post office and banks. These then outsourced enrollment to enrollment agencies and individual operators who bought equipment to do enrollment.

The UIDAI to get states to participate worked with them to support collecting additional information at the state level beyond the core demographics that they were collecting. This was called KYR+ (Know Your Resident - Plus) Information into State Resident Data Hubs. They required that the state level government use software that they created.

Then at the state level they started with the consultancies doing most of this work to merge together all the databases of various programs together using the Aadhaar as linking key as it were. Except the mostly didn't get citizens to tell various programs what their Aadhaar number (known as organic seeding) they would do algorithmic matching and connect the data without the individual's awareness or consent. This was known as Inorganic seeding.

Today there is a set of Authentication Service Agents and Authentication User Agents all hooked up to the CIDR to do authentication in the field.

They also have a set of services that do what is called eKYC the querying of a the national level database to have it send the demographic information (name, address, date of birth and gender) in the form of an "electronic document" that can meet the FATF requirements for KYC. That is for the banking system. India also has KYC requirements for the phone system so phone providers wanted this.

When talking with over seas Indians who were in my session afterward the session they described their experiences with registering for banks and phone companies and wondered where the consent for the KYC happened. They didn't realize that they actually pulled information from the CIDR.

When enrolling people they also ask for a phone number. They use this to remote authenctation that is people who want to do authentication can ask for an OTP this is used for Authentcation. The trouble with this is that not everyone has a phone many people in remote places gave the UIDAI the phone number of the local head man.

India also created a Universal Payments Interface system and created an Aadhaar look up service that lets people send money by just knowing the Aadhaar number of people. One challenge that is happening in the field with this system is that people are encouraged by various financial service providers to open a new bank account - they do a eKYC process for this and then this over-writes the record in the look up service at the center and they are then are having their benefits going to this new bank and not the one they had originally set in the system.

There is the ability for employers to hook up their daily attendance system up to the CIDR. I met people in India who had to do this. I opens up the question is it an appropriate use of a National ID system to be monitoring people's daily attendance at work?

There is the DigiLocker where you can pull all sorts of different documents in digital form from various agencies.

They have a mobile application for Aadhaar number holders.
You can sign documents using Aadhaar.

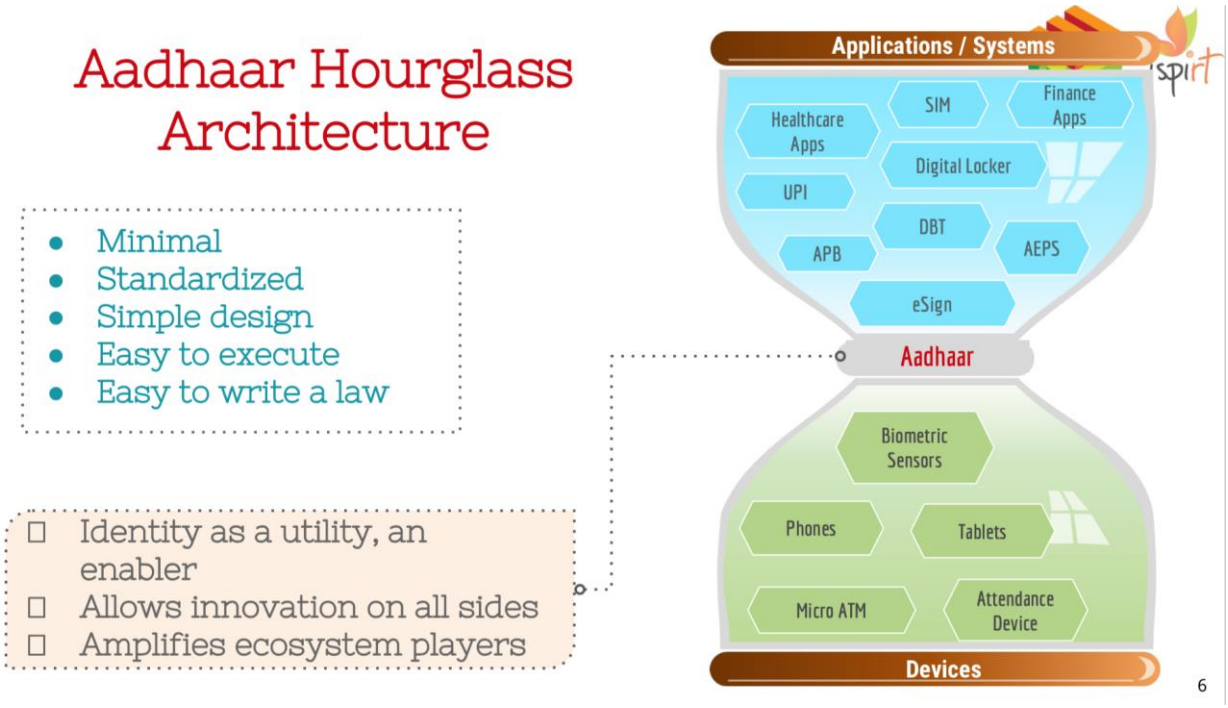
We didn't get into it but they also have a new type of ID called a Virtual ID that can be created as a one-time ID to both KYC and Authentication.

The system is sprawling and seems to be growing with new attack surfaces created. The over seas Indian's present thought I did a great job explaining the system and

The ISPRIT a trade association of Indian software makers has a model for how Aadhaar should work putting it at the center of a bottle neck of Indian's us of applications in what they call the India stack.

Books I would recommend in this order.

- The Aadhaar Effect: Why they World's Largest India Project Matters by N.S. Ramnath and Charles Assisi
- Decent on Aadhaar: Big Data Meets Big Brother edited by Retina Khera
- A Biometric History of India's 12-Digit Revolution
- In Pursuit of Proof: A History of Identification Documents in India by Tarangini Sriraman
- Rebooting India: Realizing a Billion Aspirations by Nandan Nilekani and Viral Shah



Formal Security Analysis Of Web Protocols

Thursday 15A
Convener: Daniel Fett
Notes-taker(s): Daniel Fett

Tags for the session - technology discussed/ideas considered:
#formalmethods, #oauth, #oidc, #attacks, #proofs, #security

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

Presentation slides: https://danielfett.de/download/thesis-defense.pdf

The work this presentation is based on, including the formal models and case studies: https://elib.uni-stuttgart.de/bitstream/11682/10214/1/%27An%20Expressive%20Formal%20Model%20of%20the%20Web%20Infrastructure.pdf

The formal analysis efforts resulted in improvements to the security of OAuth that are described in the new OAuth Security BCP RFC draft: https://tools.ietf.org/html/draft-ietf-oauth-security-topics-11

Summary of the new security recommendations: https://danielfett.de/download/locomocosec-2019-how-not-to-use-oauth.pdf

Me2B Alliance Code of Practice – Harms Worksheet

Thursday 15B
Convener: Lisa LeVasseur, Richard Whitt, Andrew Hughes
Notes-taker(s): Lisa LeVasseur & Andrew Hughes

Tags for the session - technology discussed/ideas considered: #Me2B Alliance

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

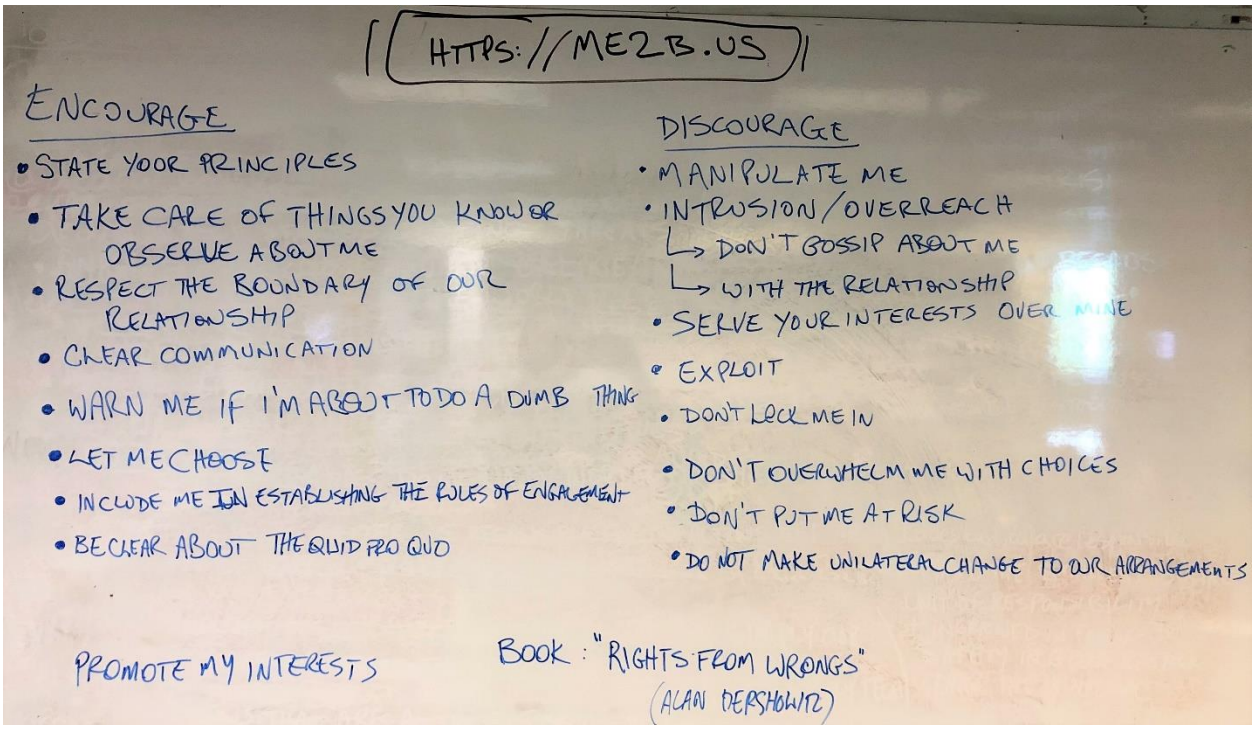
Notes received from Lisa LeVasseur:

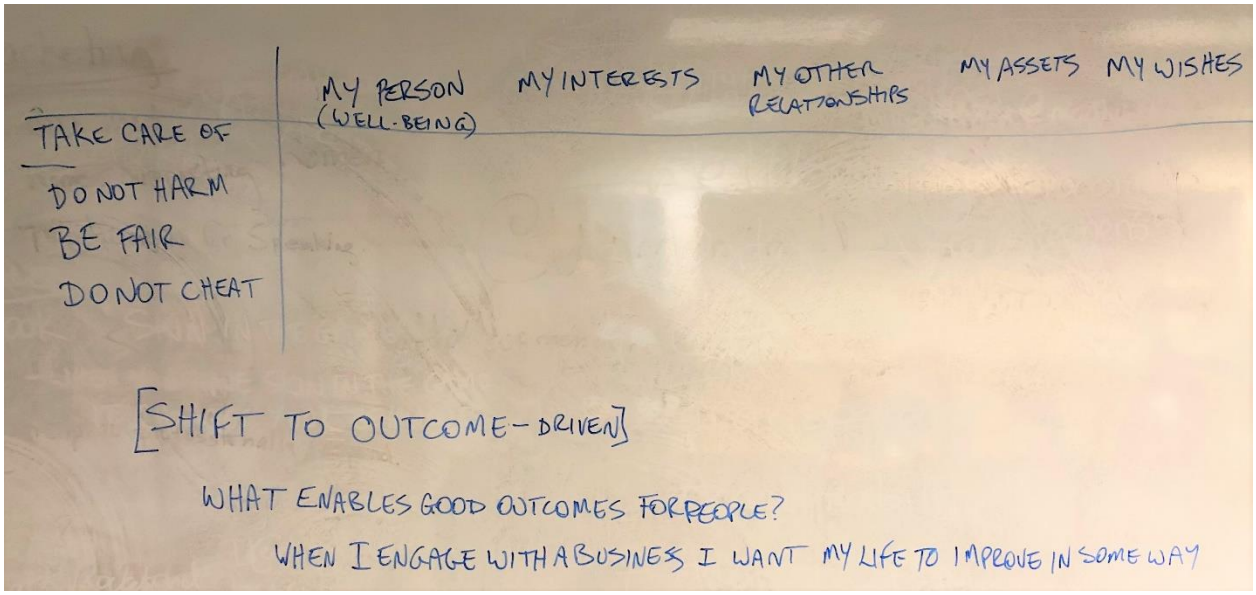
Created a baseline list of positive behaviors to *encourage* and negative behaviors to *discourage* based on personal experiences from the participants in the session.

Mei Lin suggested that it may be more fruitful to focus more on desired outcomes than a list of specifics.

Joe Andrieu proposed that the overarching guidance was: "When I engage with a business, I want my life to improve [in ways that are meaningful to me]."

Notes received from Andrew Hughes:





Selling The Business Value of DIDs: How Do We Convey (And Quantify) The Commercial Value of: Portability(Mobility), Selective Disclosure/NKPs?

Thursday 15F
Convener: Karyl Fowler, CEO at Transmute
Notes-taker(s): Margo Johnson

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

Transmute: Starting with business process optimization
3 question framework

1. Is selective disclosure or privacy a priority?
2. Is there is high coordination burden?
    1. Defined as Large amount of friction between players of a network
3. Is traceability or audibility important?

Focusing on cost and revenue centers of the company

Core features:

1. Portability of DID
    1. Inter-operability: vendor proprietary lock-in is seen as a problem (Government)
    2. The word portability seems to resonate in some cases… attach to person or thing
        1. Relationship to mobile phone number portability
            1. Vendor: it is configurable (portability can be a bad word!)
            2. Consumer thinks of as ubiquitous acceptance - “freedom”

What types of language work for clarification of the business proposition of DIDs? (group brainstorm)

Unlock potential of better work flow… further integration into the market value network that provides customer experiences
More APIs more integration of services
Identity layer unlocks potential for deeper service integrations
Get out of your silo
Parallel to microservice architecture value proposition

Telcom example
New company… if you don't like my service you can always go back… and I can ingeststst
"Insurgents" like idea of portability
Bigger companies don't like ideas of portability

Future-proof, fear-based sales don't work as well
Regulation in the mid-term
Defense logistics totally different

EU Governments
GDPR — privacy is a big selling point
Opportunity to leapfrog from paper to not a central silo… not having to be the sole carrier of risk
"Distributed responsibility"
Everyone can use the same SSI method… you can't tell that I am using social benefits services
"Seamless"

High failure costs … "cryptographically verified" to save time and money
Don't trust, verify

Avoiding correlation
"Protecting proprietary information"
"Protecting business secrets"

Who you are at work, at home, etc. Protecting personal privacy… own identity

Decentralized reputation

Open your network to opportunity, not risk

Carrier can take their reputation, not your IP

Using the word "blockchain" is the innovation sell

Compliance and ease of integration

Provability

Healthcare context - the "P" in HIPAA … portability is required

Governance: anti-surveillance is compelling

Ease of use

Federal government clearance process
Same with physician credentialing

Standardized way of doing this

Recognition between a company and customer
Stop treating you customer like strangers

What are you gaining from SSI?

What are you losing from not adopting it?

Legal challenge: How to port reputation without giving things away
Selective disclosure about prior confidential matters without over-disclosing

Congressional testimony: say the things you want to say without saying the things you don't want to say

At same time, building community of belief of self-sovereign identity
Putting the customer in charge

What is the most compelling functionality of DIDs?
-Wallet in order to manage identity
-Mutual consent receipts
-Terms and conditions consent provably bilateral
-Open Source
-Password-less options

Next steps
Need for a business gathering?
Temporary working group for the DIF
Business glossary?
Common language

SSI Agents For The IoT Using Picos

Thursday 15G
Convener: Phil Windley
Notes-taker(s): Sam Smith & Phil Windley

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

Notes received from Sam Smith:

Demonstrated picolabs.io implementation of indy agent protocols for DID decentralized identity running on Picos devices that uses event driven messaging architecture for digital twinning.

Link received from Phil Windley:

Link to presentation – *Picos, Agents and the Internet of Things*:
https://www.dropbox.com/s/jc7099f4x7zj3i3/Picos%20as%20Agent.pdf?dl=0

The 4 Layer Digital Trust Infrastructure Stack

Thursday 15I
Convener: Drummond Reed & Scott Perry
Notes-taker(s): Drummond Reed & Ben Gregori

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

Notes received from Drummond Reed:

This session was given by Sovrin Governance Framework Working Group chair Drummond Reed and SGFWG member and Sovrin Trust Assurance Framework author Scott Perry.

The framework for the session was this diagram, which is based on Appendix D of the Sovrin Glossary (see link for image to Appendix D)

The first part of the session was focused on explaining the four layers in this diagram, and how they depend on the one below. For detailed explanation see Appendix D of the Sovrin Glossary.

The discussion then moved to the fourth layer, the layer where trust in verifiable credentials is established when those credentials need to be relied upon by verifiers that do not necessarily have any direct business relationship with the issuer. We talked about the five distinct roles at this layer (all explained in depth in Appendix H of the Sovrin Glossary).

At that point we moved to interactive discussion of many topics related to governance frameworks and these five roles. Some of the questions asked and answered were:

- Q: How do we promote good behavior and privacy practices at layer 3? A: By specifying the rules for issuers, holders, and verifiers in governance frameworks and promoting their use.
- Q: How many governance frameworks are expected at layer 4? A: While it might look like just a few (e.g., credit card networks), we believe there will be thousands or tens of thousands over time, because they will be of any size and complexity for any trust community that needs one.
- Q: Are all the roles at layer 4 needed? A: No, different governance frameworks will need different roles.
- Q: What will typically be covered in a domain-specific governance framework? A: The "BLT sandwich": business, legal, and technical policies covering: a) what credentials and claims are covered, b) who can issue them under what policies, c) who can hold them under what policies, d) what policies apply to verifiers, e) legal policies and requirements, and f) technical specifications.
- Q: What are early examples of domain-specific governance frameworks? A: CULedger is developing one for MyCUID, a global digital credential of credit union membership which will probably be the first KYC-backed digital credential. DignifID is developing the DignifID Animal Guardianship Framework to establish best practices for SSI for pets. Truu is developing a governance framework for doctors credentials in the UK.
- Q: What is required to create a domain-specific governance framework? A: The Sovrin Governance Framework Working Group has just formed a DSGF Task Force to build templates and provide assistance. You can contact us via the Sovrin website.

Drummond and Scott finished by inviting all attendees (and all IIW note readers) to join the Sovrin Governance Framework Working Group if you are interested. It is open to anyone interested in business, legal, and technical policy or governance frameworks.

********** ********** ********** **********

Notes received from Ben Gregori:

Largely: this model is analogous to SSL (URL at base, connection between browser and server, SSL, and the certificate authority

1. Why do we think that Public Ledger Layer, Agent-to-Agent Layer, and Credential Layer technologically distinct?
2. Why do we think that layer 4 (Governance Framework) is less developed? What exists in this layer, and what is the role of trust issuance (the classic function of auditors will fulfull in this infrastructure)
    - Trust Anchor
    - Credential Registry
    - Governance Authority
    - Auditor
    - Auditor Accreditor
3. We can't deliver value to the market until the Governance layer is understood
    - In a particular application of SSI, Credit Unions are the issuer and can only issue credential if it is KYC'd. Now, even though that is valuable for the credit union, the assertion of KYC approved will be useful to many other organizations, and they want to charge verifiers for the ability to use their credential for other business uses. Moreover, that organization shouldn't have to interact in any way with the issuing credit union. So it needs a credentialing template for that domain specific governance frameworks.

- Trust communities of any size will interoperate (cities, churches, etc) based on the governance framework – standardize the roles so that any trust community can crop up and fill the roles of trust anchor, credential registry, governance authority, etc). Perhaps not *all* of these will be used based on the scale and application (British Columbia doesn't have all of these), but these are all possibilities.

The reason why the layers are separated:

- DID layer: anything that refers to a persmissionless or permsissioned blockchain that comprise of a DID network (many different DID networks that issuers can root within). DID networks are roots of trust, but the term "trust anchor" is at the top. Need for clarification of terminology. But there will be different networks at a base level (foreign government, foundations) – it acts as the plumbing and does not discriminate (it like the transport layer?), and will not seek to interpret human trust. Its like URLs

Why wouldn't consortiums bifurcate and trifurcate? Network effect. Is it therefore in the best interest of these mobile wallets (who are all devising SSI systems) to collaborate and build a governance framework and become a network of credentialing authorities that become the trusted network? Maybe. Applicable in higher education, banking networks, etc. You could even create a DID for the governance framework *in the credential* to verify that a certain credential complied with a preapproved governance framework that had the support of an audited industry.

To avoid an Aadhaar system, how do you specify which credentials are appropriate for verifiers to use? We use a governance framework and enforce it (regulation, legal, normative, institutional – it can also be rules *within a domain*), whereby more specific use cases will develop their own rules that are domain specific).

Governance is also important as tech/frameworks evolve. GDPR and creating permanent DIDs fly in the face of GDPR rules even though SSI aligns strongly with spirit of GDPR. Sovrin is going to the EU Commission specifically to see how they can accommodate the governance.

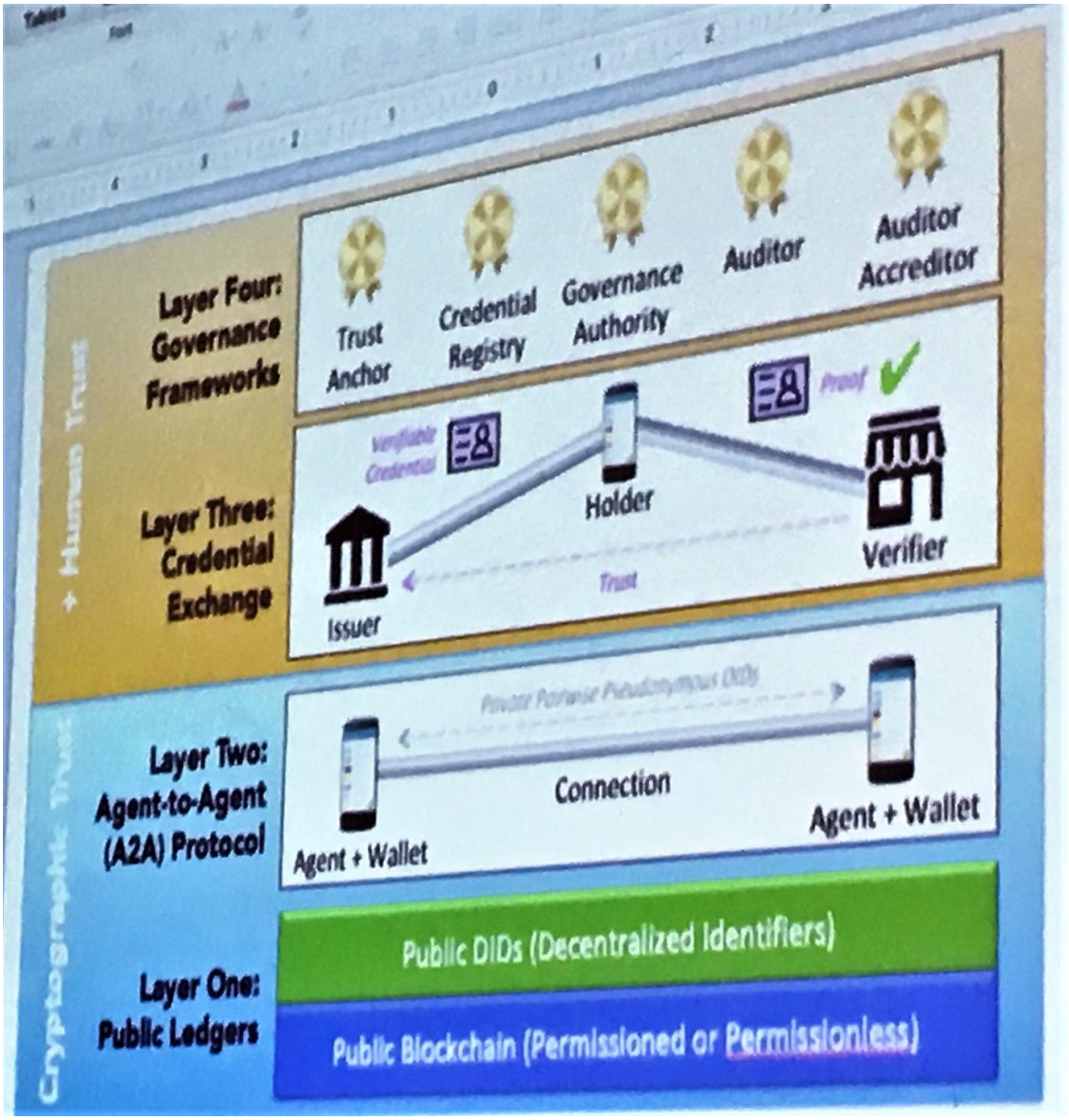
Ex. Visa is a governance stack (private) – requires all participants play by the rules, and to do that tthey bring in credited auditors to ensure that participants are playing at the same level, or fulfilling their obligations and roles.

-start up in Seattles that automate policy decisions by translating policies to data governance implementation. "Salesforce for Compliance" and Dignify.

Scenario:

4. Assuming some new mobile wallet comes out, just the process of taking a physical credential into a digital credential in which a specific COMPANY is the issuer, it has earned millions of funding. This is *before* looking at the human trust level.

https://sovrin.org/library/sovrin-governance-framework/


Layer Four:
Governance
Frameworks
Trust
Anchor
Credential
Registry
Governance
Authority
Auditor
Auditor
Accreditor
Layer Three:
Credential
Exchange
Verifiable
Credential
Holder
Proof
Issuer
Trust
Verifier
Layer Two:
Agent-to-Agent
(A2A) Protocol
Private Pairwise Pseudonymous DIDs
Connection
Agent + Wallet
Agent + Wallet
Layer One:
Public Ledgers
Public DIDs (Decentralized Identifiers)
Public Blockchain (Permissioned or Permissionless)
+ Human Trust
Cryptographic Trust

Demo Hour

IIWXXVIII #28 Community Sharing / DEMO LIST
Wednesday May 1, 2019 1:30 – 2:30
http://iiw.idcommons.net/IIW_28_Demo_Hour

Thanks to our Demo Hour Sponsor HYPERLEDGER

1. **WSO2 IAM - Keep Calm and Authenticate: Why adaptive is the way to go:** Ayesha Dissanayaka, Maduranga Siriwardena **URL: https://wso2.com/identity-and-access-management/** Adaptive authentication is an evolved form of Multi-factor Authentication (MFA) where authentication steps can be configured and deployed based on user profile and behavior. WSO2 IAM enables an organization to apply extra security only when needed while increasing usability.
2. **Jolocom SmartWallet:** Ellie Stephens, Eugeniu Rusu, Joachim Lohkamp **URL: Jolocom.io -** or go directly to the demo at **bit.ly/Smartwalletalpha** Who controls your digital identity? Jolocom's self-sovereign identity solution empowers any person, organization or IoT device to collect, carry and share the information that defines them. Test out your self-sovereign identity with Jolocom by downloading the user-facing SmartWallet, adding your credentials, and sharing those to access services.
3. **digi.me / Current PC/Mac, iOS/Android version application:** Jim Pasquale **URL:** https://digi.me/partners digi.me enables the new personal data economy allowing individuals to share more data, for greater value w/complete privacy, security and consent. Private Sharing is the quickest, most secure way to build apps https://developers.digi.me/ that respect user privacy and security by design.
4. **NextLabs Inc., CloudAz: Data Centric Security & Attribute Based Access Control in the Cloud**
   Jason Hammond, Principal Sales Engineer **URL: https://www.cloudaz.com/home**
   NextLabs CloudAz is a Cloud Authorization Service providing Attribute-Based Access Control (ABAC) for custom and COTS apps. CloudAz helps secure your applications, speeds time to market, simplifies policy management, and reduces security and compliance costs.
5. **Trustee - A Standards-based Self-Sovereign Agent: Adrian Gropper**
   URL: https://trustee.ai/ Trustee by HIE of One uses UMA, uPort, and OIDC to show how Verifiable Credentials and DIDs go beyond federated identity to create a patient-owned self-sovereign health record that self-sovereign licensed practitioners can sign into and be held accountable without intermediaries.
6. **JLINC Labs - User push CRM updates:** John Wunderlich
   URL:https://www.jlinc.com The JLINC protocol enables customers to control their own information and preferences with live permissions. The ability for customers to provide permissions in real-time means that notice and consent are moot. By actually empowering the individual companies can build trust with their customers, get better information, and reduce regulatory risk.

7. **IDENTOS - Federated Privacy Exchange (FPX) :** Alec Laws
   URL: https://identos.com/ https://identos.com/products-federated-privacy-exchange-fpe/
   FPX was built to put people in control of their privacy and reduce silos for a connected online experience; FPX is next generation IAM technology, providing digital authentication, authorization & governance to enable trusted ecosystems & complex integrations across a jurisdiction.

8. **IIWBook: Trusted Peer-to-Peer Messaging using DIDs, Verifiable Connections and Agents:** John Jordan, Stephen Curran, The Government of British Columbia
   URL: https://iiwbook.vonx.io Learn about the SSI-tech behind IIWBook—a demo of DID comm. interoperability. Use your phone to receive verifiable credentials (e.g. emails, attendance @ IIW), find peers, connect to, authenticate and send end-to-end encrypted messages. Keep the conversation going after IIW!

9. **IdRamp "Authority" - Enterprise ready decentralized identity: Mike Vesey**
   URL: idramp.com/ledger **-** Learn how practical Interoperability with enterprise infrastructure enables adoption of decentralized identity.

10. **Danube Tech - Universal DID Infrastructure:** Nader Helmy
    URL: uniresolver.io, uniregistrar.io Now that we have basic functionality for resolving a DID, we will demonstrate a more complete toolset for DIDs which will practically enable developers to build blockchain-agnostic applications.

11. **Sphere Identity - A brand new way to sign up:** Asya Ivanova
    URL: sphereidentity.com A simplified customer sign-up experience that hands the control back to users, an alternative to forms, passwords and even typing. It reduces sign-up abandonment rates and allows flexibility around user data. The original implementation of a 3-party consent receipt.

12. **Botlabs, KILT Protocol:** Matthias Moeller, Marton Csernai
    URL: kilt.io KILT is a blockchain protocol that incentivizes claim standardization and facilitates the management of trust relationships on the internet. The KILT Trust Market enables new business models for anyone who owns trust or wants to build up both simple and complex trust solutions.

13. **Frozen Pii, LLC:** Tom O'Malley (Founder)
    URL: http://www.FrozenPii.com - Self-Sovereign Identity (SSI) cannot be achieved without people first controlling their "financial identity" collected and sold by the credit reporting agency oligopoly - Experian, Equifax and TransUnion. Frozen Pii provides people with information and trusted links to secure and control their "financial identity." A consumer-controlled PiiCloud will be demonstrated.

14. **Yubikey - FIDO has Browsers:** John Fontana
    URL: https://www.yubico.com/products/yubikey-hardware Get a glimpse of FIDO2, W3C Web Authn standards working on the Microsoft platform and in browsers, along with other FIDO (and YubiKey) options for strong authentication. The next version of FIDO/Web Authn was blessed as a standard on March 4 and is ready to deploy. But don't forget Yubico also supports open standards such as PIV, OATH, and OpenPGP.

15. **PDPR - Personal Data Protection Regimen- Technical Associates Group, LLC:** Jeff Orgel
    The concept of a *Personal Data Protection Regimen* is designed to illustrate how HumanOS practices (aka decisions) influence user IT relationships. These decisions shape systems and algorithms that will impact the user's online identity and presence.

16. **Endorser Search/ Using uPort as a Server - enable discovery ~ preserve privacy:** Trent Larson
    URL: https://github.com/trentlarson/endorser-ch We want to make it ridiculously easy to make arbitrary claims, and then search for claims by people who are within your close network (ie. those who have supported your own claims and/or confirmations).
17. **ConSensys - SeedQuest / A 3D Mnemonic Game for Key Recovery:** Michael Mendoza
    URL: https://github.com/reputage/seedQuest SeedQuest is a 3D mnemonic game for key recovery. It is designed to be simple and fun. Instead of memorizing your key, you memorize actions in the game to recover your key. After learning the actions, simply play the game to recover your private key. That's it.
18. **Transmute - Transmute ID and Sidetree Element: Margo Johnson**
    URL: https://www.transmute.industries/transmute-id Transmute ID brings decentralized identities and verifiable credentials into traceable multi-party business transactions. The app is an identity security layer integrated with major cloud storage and identity access management tools. Scalable DIDs are possible with Element – the Sidetree protocol on top of Ethereum and IPFS.
19. **UBOSbox: Johannes Ernst, Indie Computing Corp**
    URL: https://indiecomputing.com/products/ UBOSbox is a pre-configured home server that enables users to take their personal data home from on-line services such as Dropbox onto hardware they control. Now shipping. Looking for more apps to ship, e.g. self-sovereign digital identity, IoT, VRM and others!
20. **Mattr: Tobias Looker and Josh Hill**
    URL: https://www.mattr.global SSI products built upon Hyperledger Indy and AgentFramework (https://github.com/streetcred-id/agent-framework) demoing a range of SSI use-cases.
21. **Wireline D-Suite demo:** Pete Rowley, Chris Waclawek
    URL: https://www.wireline.io/ DSuite is a proof of concept decentralized alternative to Google Apps. Build as a demo application of Wireline stack enabling p2p, censorship resistance, self sovereign identity, data ownership.
22. **Blockchain Commons - AirGap Wallet Demo & Standards:** Christopher Allen @ChristopherA
    URL: https://www.BlockchainCommons.com See how we can use airgapped QR codes to more securely support multi-persona wallets for both identity & digital assets. Included also simple social key recovery.

The IIWXXVIII Demo List can also be found here
http://iiw.idcommons.net/IIW_28_Demo_Hour

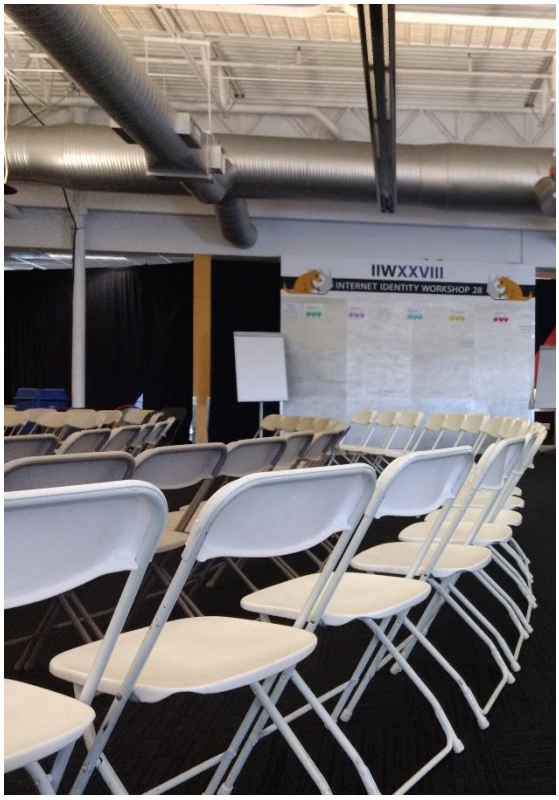
IIWXXVII #28 Photo Albums by Doc Searls

Check out Doc's FABULOUS photos of IIW 28 @dsearls

Day 1:
https://www.flickr.com/photos/infrastructure/albums/72157708808124568

Day 2:
https://www.flickr.com/photos/infrastructure/albums/72157708829091557

Day 3:
https://www.flickr.com/photos/infrastructure/albums/72157708832085467



See you
October 1 - 3, 2019

for
IIWXXIX

The 29th
Internet Identity Workshop

REGISTER HERE
https://iiw29.eventbrite.com

www.InternetIdentityWorkshop.com