IIWXXIX

INTERNET IDENTITY WORKSHOP 29

Book of Proceedings

www.internetidentityworkshop.com

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

October 1 - 3, 2019
Computer History Museum ~ Mountain View, CA

Notes in this book can also be found online at
https://iiw.idcommons.net/IIW_29_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 Kaliya Young, Heidi Nobantu Saul, Lisa R Horwitch

REGISTER FOR IIWXXX
April 28, 29, 30, 2020
HERE: https://iiw30.eventbrite.com

Contents

Oct 1

#IIW XXIX with many friends and friends to be. Apparently, this is the first IIW to go beyond 300 registrants.

Nat Sakimura @_nat_en

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. IIWXXX (#30) will be April 28 - 30, 2020 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

IIWXXX #30
April 28 - 30, 2020
REGISTER HERE

IIWXXXI #31
October 19 - 21, 2020

@IDWorkshop #IIW

Thank You! Documentation Center/Book of Proceedings Sponsors: People First ~ Jolocom ~ Wireline

PEOPLE FIRST
All Else Follows

@TheBusEquation

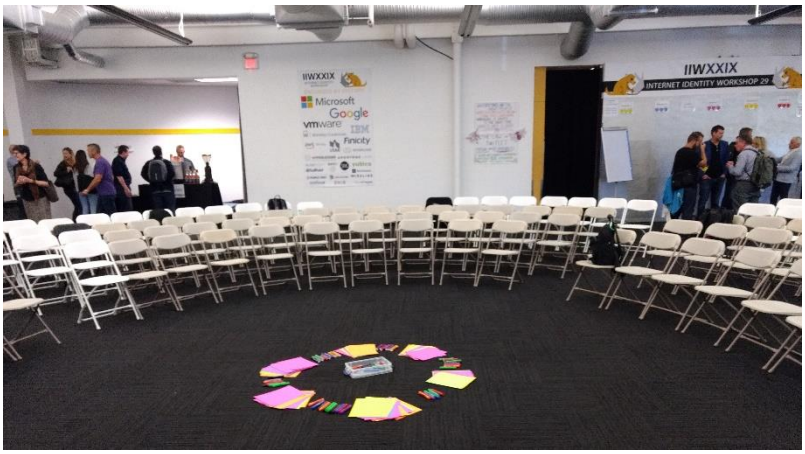
JOLOCOM

@GETJolocom

#WIRELINE

@wirelineio

IIW 29 Session Topics / Agenda Creation



111 distinct sessions were called and held over 3 Days.

We received notes, slide decks and/or white board shots for 97 of these sessions.

Day 1 Tuesday October 1/ Sessions 1 - 5

Session 1
1A/Hyperledger Aries Project Status + Intro
1B/Introduction to OAuth2 (a 101 Session)
1F/Me2B Relationship Management/Tech Archite
1J/DID + Trusted Hardware Agents! (yubico,hsm,enclave)
1L/Link Secret FUD and other VC Fraud Learnings

Session 2
2A/Hyperledger Aries Biometric Service Provider RFC 231
2B/Into to Open ID Connect (a 101 Session)
2C/What Does a Sustainable SSI Business Look Like? The Business of Self-Sovereign ID
2F/The DID SPEC is Perfect! Change my mind.
2G/5G, IOT, DLT, ML, and Other Buzzwords
2H/Machine Identities
2I/Selective Disclosure (w/o ZKP)
2J/Deepfakes: Tools + Rules to Save the Open Internet. What? How? Why?
2L/Open ID Connect 4 Indy Assurance
2M/Signln.Org What is it?

Session 3
3A/Beyond Bearer Tokens
3B/User Manage Access (UMA – a 101 Session
3C/Seed Quest 3D Game Mnemonic Cryptographic Seed Recovery
3D/Identity CoOp
3E/Spirituality, Abundance, Mindset, Personal Identity, Role in Community
3F/Expanding Language… Digital HARMS Dictionary
3G/HYBRID Self – Sovereign Identity
3J/DIDComm Encryption Envelope Discussion
3L/Adam from ID @ Equifax: How can I help? What should I do? AAAAA!
3M/Open ID Connect Federation BoF

Session 4
4A/Calling All Actors! Help is shoot a demo on Guardianship with SSI in a Refugee Camp
4B/Introduction to WebAuthn /FISO 2
4C/A Guide to Hyperledger Aries – Cloud-agent Python architecture and implementation
4D/Cors On OAuth Token Endpoint NOT A BCP
4E/Job Shop
4F/DID Resolution
4H/Well-Known DID-Configuration – Connecting DID's to Domains with an Emerging Standard
4I/Workday Credential Schemas (No LD)
4L/Truth or Dare Verifiable Credential Disclosure Patterns and Commitments

Session 5
5A/KERI: 1 Universal DKMI Root(s) of Trust Decentralized Systems Primitires & DKMI Last Mile of Trust
5B/SSI 101 (Self Sovereign Identity) (a 101 session)
5F/A Protocol for Decentralization – How Many Data Brokers Will We Need
5G/Online Access Refresh Tokens (2.0) & OAuth Browser (BCP)
5H/DIDs For Everyday People
5J/Secure Data Storage (The Hub HVBUB)
5L/Organizational Wallet?
5M/Lean Startup For SSI – How to turn four SSI Idea into a viable biz.

Day 2 Wednesday October 2 / Sessions 6 - 10

Session 6
6A/Verifiable Credential Based Authentication over OpenID Connect
6B/Identity in Sierra Leone – Ask us Anything
6C/Decentralized UX: Designing Around Decentralized Identities
6F/"Trust in Numbers" Ethical (and practical) Approach to Identity – Driven AI/Machine Learning
6H/Identity Standards: The Soap Opera (catch up on previous episodes + review major plot points

Session 7
7A/OAuth Pushed Authorization Requests
7B/Delegated Credentials = Guardians, Controllers, and Delegates with Any W3C Credential Type
7C/Aries Toolbox Demo + Feedback (tools to work with agents)
7F/@Me2B #SSI #VRM #IIW #Identity
7H/Identity for All – Refugees, Human Trafficking, Women, & Marginalized People = Tech Meets Real Life Experience & The Humans that DID + SSI Can Help Most, How & Why
7J/Gender Is Harder Than You Think
7L/What's Going on With DID-Auth? & SSI + SIOP, OIDC DID Auth Demo

Session 8
8A/TXAuth (XYZ,RAR, JAR,JARM…)
8B/Issue A Verifiable Credential in 30min
8C/Problem of Provenance of Digital Content Roadmap to Solution
8F/Consent Receipts for Financial Services and more….
8G/Me2B Intro & Org Finder Wiki
8H/DOMI Digital Rental Passport Architecture & Data Workshop
8I/Freeclaims.org – Let's Encrypt For Basic Verifiable Credentials
8J/DIDComm – Part 2

Session 9
9A/Highlights from 12 Months of Private Sector Research = Election Security, Supply Chain, Legal and IOT
9C/Privacy Chain Update
9F/Customer Commons – VRM MarketPlace FrameWork
9G/Financial-grade API & CIBA (Client Initiated Backchannel Authentication)
9H/Manifold: Identify and Manage All Your Things
9I/Mark of the Beast? Religion's Impact on Identity
9J/Consent is Broken – Privacy Implications for SSI
9L/VC's In The Supply Chain GSI

Session 10
10A/KERI: 2 Universal DKMI Events Witnesses Architecture
10B/Understanding and Implementing peer DID's in 60 min or Less
10C/The Great Hub Hubbub
10D/Finish RWOT 6 Principles for Self-Sovereign Biometrics
10E/AMA w/Sovrin Exec Director
10F/Browser Changes (SameSite, ITP) Affecting Identity on the WEB
10G/A Machine Learning Perspective on Data About Me
10H/High Assurance OAuth/OIDC Profiles for Gov. use Cases
10I/Workshop – Universal URI For Deep Linking in All SSI Mobile APPS
10J/"I Am Spartacus" Privacy via Obfuscation for Vulnerable Populations
10L/The Trust Ove IP Stack – A Path to Global Interoperability for SSI and Verifiable Credentials

Day 3 Thursday October 3 / Sessions 11 - 15

Session 11
11A/Are We Boiled Yet?
11B/Life Scope – Meet Your Digital Twin – Data Hub/DB/Wallet + Identity + Cred + Me2B
11G/Platform Architecture – Building the back ends and systems that support AS services. State? Scale? Price? Persistence?
11H/Aries Protocol Test Site
11J/Pico Agent in a Tab One Click to Identify?

Session 12
12A/Identity for All 2 – how can tech present at IIW help with digital identity for marginalized populations?
12B/XYZ & DID Deep Dive
12C/Seed Quest – Demo & Exploring Use Cases
12D/Verifiable Credentials for Mobile Skills Schemas & UX
12F/Me2B "Me" – side interoperability & integration (part 2)
12G/Retrofitting OpenID to Existing Apps BCP?
12H/DID:GIT: Where is it at?
12I/Life Scope.io Digital Self

Session 13
13A/Censorship Resistance and Permissioned Ledgers: Survivability Analysis
13F/ID4 Africa – Exploring Possibilities for how SSI Communities and Companies show up @ the event & surrounding weekends

13G/DeepFakes Part 3 – What Parts of the Identity Stack & Verifiable Credentials for Digital Provenance?
13H/Generic MFA Token Recovery – The good the bad and the ugly

Session 14
14A/CLAIMS Vis-à-vis Scopes in OAuth & Open ID
14E/Pico Agents for Communication (follow-up)
14F/Tracking for Good Pragmatic Privacy
14H/Product Roundtable – Bridging tech & business, connect and share challenges and resources
14J/Hush-A-Phone
14K/Self-Sovereign Human Rights Parallelism

Session 15
15A/Terminology – the Plan
15B/Cards Against Identity
15F/Expanding Language = Systems / People = Osmosis & Opaqueness
15H/Sidetree did:ion + did:elem Roadmap + dev
15J/Building a Business Around Identity In Education (From a Colombian Perspective)

Notes for Tuesday / Sessions 1 - 5

Aries Project States & Introduction (Hyper Ledger)

Tuesday 1A
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:

Slide deck from Sam Curren:
https://docs.google.com/presentation/d/1zA4AmCGCeJZraSJCGHFvRa2hVYptl80vVJKb5E1J9oY/edit?usp=drivesdk

OAuth2: An Introduction (101 Session)

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

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

Summary:
We introduced the OAuth2 delegation protocol, its history, its structure, and its usages.

Me2B Relationship Management/Tech Architecture

Tuesday 1F
Convener(s): Johannes Ernst & Kim Date
Notes-taker(s): Nick Roy

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

Me to B alliance
Original use cases: I want to change my address once across all web sites / etc.
How would we make this work?
Interop problems
Need to rethink what interoperability is
In the past: This device works with that device, this plug fits into that jack.

Is that what we want as people, around interoperability?

Interoperability means things actually work, people won't start crying because things don't work.

We can get our info from our digital life and have stuff that reasons over it. The data itself is interoperable.

From my perspective, my digital life is totally fragmented - not just usernames and passwords. No unified messaging.

How do we make this happen?

Closest we have ever gotten was the old concept of portals.

Liam is working on a new type of portal related to this.

Adrian claims that the interop layer is an agent. The protocol is something that looks like UMA, the characteristic of that thing is that when you're dealing with one of your apps/service providers, you give them the address of your agent. Instead of giving them your email address, you're giving them the address of a thing that can learn/manage relationships, act on your behalf.

Nat: For a limited set of attributes/claims, don't we already have this?

Kim: We're not talking about identity info, we're talking about all the attributes of your online existence. Slack/email aren't in the same inbox. The services are transient, and as they come and go, you have holes in your life that are ripped out.

Can't accept current architecture where things only live in one place. Needs to survive the failure of one or more parts of the ecosystem.

For data to be portable, the format has to be standardized. We have strong evidence of what this looks like in healthcare.

There is now a rush for data brokers that add value in the healthcare space, acting on this data through ML/etc. As soon as you have this kind of interop, you get people coming out of the woodwork figuring out how to use it for interesting things.

Liam: Built an agent using UMA/GraphQL/Oauth where everyone is their own OP, but it's faulty, want to do a session on this.

Need to know not just where my data is generated, but where it is stored.

Data portability use case- interesting how we create receipts, but we haven't talked about what receipts we create.

Doc: Consent receipt conversation was all about us consenting to terrible terms of other parties. How do you get alignment about consent between people and services, so it's not one-sided? Have any of the password store companies ever been here? Why don't they come? As long as we're stuck in client-server password fail, we can never get out of that? They are in the best position to help us, but they are not interested in helping us.

Mary: Reason to collect consent stuff is not because it really matters to any of us. The consent group was looking for places to drive wedges in the market to put pressure. FTC can go after companies, because the only way to put pressure on companies is to catch them breaking an agreement.

Quintessential FTC issue- only thing they can do is punish bad behavior that has already happened. Need to create a system that creates a counterbalancing force.

Moving back up from the gory details to the high level.

How do we make it so that a user that doesn't know anything about this stuff have a less fragmented digital life?

Original intent of blogging - distributed personal repositories. Then all the decentralized part of that died. So how do I put all my stuff in distributed repos and have it just live "out there"?

Adrian: This is aggregation. Of attributes or of control.

Would be happy if there was at least just a list of all the places that have my address.

Mary: Propose a different word for this, not aggregation, it's indexing.

Kim: Indexing is one way to create an aggregated view. Copying data is another way to create an aggregated view. Should support both / all approaches. Need to be able to survive indexes/stores/etc. going away.

22,000 missing URLs on Kim's blog roll. Trying to fix that problem. All of those 404s were live beautiful things, and it's all gone down the drain.

"Site Deaths" anyweb.org

Doc: Put some easter eggs in old blogs to see if they still show up in indexes, and they don't. Old stuff he wrote is still there, just doesn't show up in indexes. Trying to change DNS has been a PITA as well.

Need to add persistence to the aggregation part of the problem.

Niels: Two questions: What is the incentive for all the services to engage? Because they could lose customers. Second: The API or whatever is always behind what is offered by the services. Interop enables people to do cool new stuff, and thus move off of old services to new innovative services.

Kim: Look at portability work the large corporations have undertaken. Why did they do that? In the past, they all wanted locked walled gardens. GDPR and other things made that impossible or hard. If you have the user at the center of the model, that changes the nature of the game. With SSI, it's possible for the user to be at the center of the model.

Google/Facebook/Microsoft have agreed to the format of data interchange. Goal is to be able to take your email/etc. from one service and put it into another. Wendell says that's export-only, Kim says no it's both export and import. There is a spec on this worth reading. Moving data to the end user is out of scope in that spec.

Incumbent big businesses of all kinds always have reasons not to do stuff. If you look at what happened to the internet, it ripped down all these silos like compuserve, AOL, prodigy. They had no choice. When the individual is able to use standards like TCP/IP, IMAP, SMTP, HTTP, that rips down barriers. While we don't have that for personal data, it's possible for the major players to continue to say 'no'.

I might have that data, but what good does it do me if there's no way to prove that the data is legitimate? Attestation for things like academic credentials.

Don't know what the right architecture is by which we can start to figure out how to interchange and store this stuff.

Lisa: In cellular - feels like disintermediating the carriers - which was a threat because it would just be a 'big dumb pipe', but there is still innovation going on.

Dedra: You have infrastructure providers, and you add standards that make the big dumb pipe be able to serve new needs. In personal data, there is no incumbent. Would users pay to have interop? Guess is not.

Vic: Key is effort: If this stuff works, effort goes away. Effort that I feel to reset my password as an example. People care about the amount of effort it takes. The part of an org that feels this pain is customer service. Every touch point with a customer causes pain. If you're able to eliminate that pain, you win.

Nick: But the monoplists don't have any way for you as an individual to even get help from them.

Jeff: Saving effort *and* building trust. Chrome samesite issue as example of compaines shooting themselves in the foot.

Kevin: Pessimistic about commercial interests solving this problem. They'd take advantage of each other. Could we drive this through government? Example of distribution of data changes through Swedish person number. Estonia, Finland, India all do this.

Johannes: The agent should be OSS. Then the dyanamics of competition goes away.

Niels: Software doesn't run itself, so ultimately there will be another entity who owns the instance of an agent. Unless you solve that on a protocol level, so no one can touch your stuff but you, the sevices will see everything.

Kim: What's amazing is the amount of money going into big companies supporting the idea of decentralization. Big companies by the dozens with 150 people each working on decentralized identity. What are they working on? The wallet. Credential providers. Wallet providers. Free wallets. Likely that the agent layer will be subsidized by companies that want a better relationship with their customers.

Adrian: This experiment has been run by healthcare for 10 years. Health data portability was tried, nothing came of it. None of the SPs trusted each other to input the data. Cheap to send the data out, expensive to bring it in.

Kim: Where the data lives isn't important, what is important is that it provides persistence and portability. Not important where it's stored, it's important how you access it, how it's distributed, how it's permissioned.

What is the incentive for the first services that sign up? No, the service doesn't have to change anything. You have the ability through the APIs and synchronization methods they're opening up, because they have to. You're getting the ability to run software that reasons across those services. If you depend on the services, you fail on day one. Liam's work: Lifescope. Able to amalgamate and build indexes across applications and services. This is feasible without disturbing the other infrastructure. You could build up an SSI infrastructure that can connect up without going through the existing services. Don't know the architecture. Need to think it out.

Jim: Example of the UX of having to contact places when you change credit card number. Terrible UX. Does the agent push out this info? Do SPs ask for it and get permission to access from you?

Adrian: Work on SSI separation of concerns: Non-correlation. Microsoft offers to do this through a tumbler or a VPN that doesn't keep logs. Design the architecture so there are standards around the tumbler. Anti-example: Sign-in with Apple.

Jim: Problem is that the services consider managing your credit card number your problem and not theirs.

By introducing the friction, the agent gets to learn about the data requests. If you give prior consent with our without a consent receipt, for you, they get to learn about the data uses, and you don't. Everyone in the data brokering business is eager to get the benefit of the learning that's going on. We have to own the private agent.

Group thinks this is the right time to have this conversation. Sense that we've been wrong before.

DID + Trusted Hardware Agents! (yubico, hsm, enclave)

Tuesday 1J
Convener(s): Orie Steele, Transmute
Notes-taker(s): Heather Vescent & Karyl Fowler

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

Using a Yubikey to sign something using a DID.
Software extractable key – a key that can come off the yubikey
A verified credential that is issued from hardware

Other trusted hardware scenarios:

Very few people are using PGP and DID togethers.

Why. Are you super interested in trusted hardware agents.
Example
Did.btch.1234….
Did doc contains a PGP key (that has to go into the GPG Suite)

On Mac GPG Suite, keys that are associated with your keyring
(key import of the PGP key from the DID document.
You can then use signatures from JSON-LD

Use case for trusted hardware key management – in journalism space
Using open PGP technology

Have PGP key of recipient
Encrypted payload (message)
Sign some information, plug in device, pin, signature

Operating systems (tails/linux) binary will be signed with GPG keys.
Connect GPG key to DID and use the

Can the camera hardware have a software/chip that does signing of the chip? Short answer – maybe.

Attestation, FIDO, IETF, EAT and RAT (remote attestation)

There have been recent attacks.
We need new key servers.

Who controls the interface where you manipulate/change the key?
Trusted hardware has usability features, they come at the cost of ultimate control by the user.

Trusted execution environment:

Secure enclave on the mobile device, compromise of one area of the app (where credentials are stored), how does that play with the secure enclave and other keys/credentials in the system.
Can you airgap those sections – yes – but can you trust how that works?

Key compromise in the lab – backdoor firmware updates

Two compromises

1. Private key is exported
2. Something goes wrong and escalate privileges

DID method that uses different enclaves
They are all different – they do different things. So it's hard to discuss their security. Nuances are different - cryptographically elements. Varied capabilities. Trust in the hardware itself is the way we want to solve.

Attacks that need physical access vs ones that don't.

Embedded keys linked to DID, can we trust the hardware that is attached.
Any sensor that tracks biometrics.
Or barcode/scanner devices. Confidence around the integrity of the systems.

What does it mean to trust the hardware.
Establish it with several signals.

Photo By Karyl Fowler:

Link Secret FUD & Other VC Fraud Learnings

Tuesday 1L
Convener(s): Daniel Hardman
Notes-taker(s): Daniel Hardman

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

Discussed the need to separate opinion from fact. We're all entitled to opinions, but not to our own facts.

Discussed 2 misconceptions about link secrets:

1. link secrets are not rotatable (false)
2. link secrets are transferrable (false)

Explained why neither of these perceptions is true. Linked to http://j.mp/zkp-vc-safety (a paper from recent RWOT), and also to "Alice Abuses Her Verifiable Credential" (another RWOT paper)

Then spent time exploring a general threat model for VCs, based on this doc: http://j.mp/vc-threat-model.

Hyperledger Aries Biometric Service Provider (BSP) RFC 231

Tuesday 2A
Convener(s): Daniel Hardman & Jack Callahan
Notes-taker(s): Jack Callahan

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

Slides from presentation here:

https://wiki.hyperledger.org/download/attachments/20022661/20190918BiometricServiceProvider.pdf?version=1&modificationDate=1568832910000&api=v2

Introduction to OpenID Connect (101 Session)

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

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

There are PowerPoint and PDF versions of the 101 presentation at the end of http://self-issued.info/?p=2008. The links there are stable.

The Business of Self-Sovereign ID: What Does A Sustainable SSI Business Look Like?

Tuesday 2C
Convener(s): Riley Hughes (StreetCred), Joachim Lohkamp (Jolocom), Ricardo J. Méndez, (Samsung NEXT)
Notes-taker(s): Ricardo Méndez

Tags for the session -technology discussed/ideas considered: trust, business models, sustainability

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

- Timothy Ruff, Evernum
    - It's about the internet stack. Do we have applications?
    - Money is made at the application layer
    - Fat protocols is a failed model
    - Store-of-value does not enable interactions
- Attendee distribution: about 15% are on a SSI provider, 15% on something that expects to consume it.
- Valuable when...
    - Verifying assertions is costly or important
    - Credentials are valuable in other contexts. Example: military IDs being useful for both base access or discounts... but what's the product? Cost reduction?
- Audience check on skepticism vs. belief...
    - Timothy: who's a skeptic of SSI? Who's a believer?
    - Ricardo: I believe on the benefits for individuals, but I'm skeptical on the likelihood for mass adoption.
    - (General audience agrement)
- Audience check...
    - Who would like to be able to manage their identity in a self-sovereign manner? (90% of hands go up)
    - What sort of service would you be willing to pay for? (Crickets, mostly)
- Examples of SSI business models people would pay for
    - Something that pings you when someone tries to use your money
    - Password managers as a tangentially-related business
- "To create or find the value you have to go very deep into existing business models"
- CU Ledger "is priming the pump" by getting credit unions to issue credentials to their customers
- Scott Perry: "It's the trusted identity that businesses are willing to pay for. It doesn't matter if it's self-sovereign or not, it's the trust that matters."
- Most business-focused solutions that the discussion converges to can be summarized as "liability reduction".
- CU Ledger example: who makes money?
    - CU Ledger makes money charging to verify credentials
    - Primitive service providing ledger
    - Middleware provider for the credential management system

The DID Spec is Perfect! Change My Mind.

Tuesday 2F
Convener: Dave Huseby
Notes-taker(s): Drummond Reed

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

David Huseby
Security Maven, Hyperledger
The Linux Foundation
+1-206-234-2392
dhuseby@linuxfoundation.org

Dave is one of the primary proposers of the **did:git** method and one of the primary implementers, together with his team, at the Linux Foundation, where he is Security Maven for Hyperledger.

In implementing the DID spec, he found overall that it allowed too many ways to do things, and it did not have enough guidance about critical points that developers need to know for interoperability. He has published a summary of his feedback here:

https://hackmd.io/@dhuseby/S1APLEDLH

He felt that the spec is overly reliant on JSON-LD as the serialization format, and that DID documents should be specified in a way that can be serialized using JSON-LD but also other formats such as CBOR.

He had a number of major areas of feedback. He broke them into four major suggestions and felt that the DID spec would ideally be broken into four specs to reflect these suggestions:

1. One spec to just define the ABNF for DIDs and DID URLs.
2. One spec to define DID documents.
3. One spec for how to define a service endpoint.
4. One spec for how define a public key or other type of cryptographic material.

With regard to this last point, Dave was particularly emphatic about the importance of being able to describe a key precisely and completely, including:

- Encoding
- Usage restrictions
- Issue date
- Revocation status

He mentioned JSON Web Keys and COZY Keys as examples of complete key description specifications.

In particular he wants to be able to Wants to be able to publish **pre-keys**—the first half of a Diffie-Hellman key exchange.

Justin Richer agreed with Dave that the spec needs to be much more prescriptive in order to drive

true interoperability. Every feature needs to be justified. "The purpose of the spec should be to define the core stuff that everyone does."

Dave said that there was one particularly glaring mistake: the value of a key can currently be be either a JSON string or a JSON object. That is a nightmare. Dave said he wants to be able to use Lint on a DID document.

We discussed the role of registries, e.g., the current DID Method Registry at the W3C Credentials Community Group. We agreed there should be registries for:

- DID Methods
- Service Endpoint
- Key Descriptions

These registries could either be maintained by an established body like IANA or by new registry services at W3C that Drummond said were being proposed at W3C TPAC by David Fisher of Apple.

Wayne had a suggestion he called "Implied DIDs" that could be based on OAuth identifiers such as

did:oath2:login.microsoft.online-john.doe@live.com

He emphasize that no private keys are involved, and this could help with mass adoption.

Drummond promised to take all of this feedback to the new W3C DID Working Group, which Dave and Justin plan to join, and invited all the rest of the attendees to join W3C and the Working Group if they wished to be part of the process of finalizing the spec, which should be at feature freeze in the next 6 months.

Machine Identifiers (DID, VC, Attributes…???)

Tuesday 2H
Convener: Mrinal Wadhwa
Notes-taker(s): Rich Smith

Tags for the session - technology discussed/ideas considered: Secure hardware, DIDs, trust anchors, IoT

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

Goal of topic: [Mrinal] Development of an open source set of tools to help people build secure connected devices, specifically IoT devices that have not had the best security track record

- [Mrinal] Devices often do many things on our behalf often without our direct or real-time involvement. An easy example would be a building's HVAC system
    - How can we help people build secure network connected HVACs

- [Mrinal] Recent developments in the identity and technology space look like they could help make some significant progress on some longstanding problems in the space
- Can we start by defining security?
    - We have been approaching defining security through the use of the STRIDE model (Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, Elevation of privilege) and applying that to the datagrams that are being transferred between systems and not worrying about the transport layers security properties. If we can derive trust in the message from the message itself rather than having to rely on underlying systems and transports then many things get easier. Especially when thinking about IoT devices as there are so many different transports used, each of which come with their own security properties that can be hard to rationalize about.
        1. Would it be fair to say you are applying some 'Zero Trust' like principles to the problem and you are looking to secure the messaging layer and assume the transport provides no security properties?
            - Yes there are some similarities there for sure
- The mantra of 'use TLS' can bite us when working on message level security/encryption as they don't need to rely on TLS for security properties but people cry foul if they don't see devices use TLS and so inevitably double encryption is often done to satisfy peoples misplaced concerns.
    - Outside of the browser/web world this is less of an issue, lots of IoT devices already transmit their data in the clear!
    - Shall we just say 'end to end' encryption even though the 'ends' may not be TLS?
        1. <general agreement that that makes sense>
- 'Identity' should be defined as being 'identifier' + 'attributes'
    - Trust is hard to bootstrap in a device without an identity
        1. There is web of attestations that relate to and provide confidence in a manufacturers chosen identifier for a device
        2. A user pairing with a device essentially adds another attribute to that devices which allows it to act with the authorization/authority of the user
        3. e.g. A lightbulb may have multiple identifiers. One is a manufacturer identifier that enables updates to be delivered, another may be an identifier used by a light switch that allows it to turn the specified bulb on/off. We don't want a manufacturer to know when you turn your light on or off, they don't need that info and lots of potential privacy issues.
            - We need to separate the bootstrapping of trust in a device from the usability requirements of the device.
            - Much more like linking 'roles' not identifiers

- We need to separate physical and network security and think about them differently. Devices that were traditionally not networked and had a good physical security model can fall vulnerable when they are put on the network.
    - As soon as you disconnect a crypto based root of trust from network security then things fall to pieces fast
        1. A crypto key is a 'trust anchor'
        2. The only decentralized root of trust we have is a public/private keypair
        3. For crypto based roots of trust in a device you have to chain all the way back to the manufacturers of the components
        4. We need a mechanism by which we can rationalise about the security of a given device
- Q: How trustworthy is your root of trust?
    - The lightbulb doesn't need to know which light switch turned it on, just that that the request to turn on is authorized
        1. This approach makes it easier to handle 5K devices in a building
    - Requests with verifiable authorization
    - TV's use an OAuth device flow that allows you to easily pair the TV to an account through a short numeric code. This is seen as problematic as once the TV has the OAuth tokens/bearer tokens it can do what it likes with it.
- Q: How important is chained delegation to all of this? (e.g. TV -> Fridge -> Thermostat)
    - Prior to DIDs identifiers in most IoT devices were just MAC addresses.
    - A MAC address attached to a message alone doesn't prove the message came from the device that corresponds to the MAC.
    - So now we need message signing so we need a public/private keypair
    - Which means you now need to maintain a table that maps MAC address to public key.
    - DIDs mean you don't have to do this
    - DIDs enable identifiers to be cryptographically provable
- There is a key agreement phase that proceeds any message exchange
    - mTLS is an example of key agreement
    - NIST has some great key agreement papers – people should look them up and have a read
    - In signal(?) there is a pre-keying approach taken
    - Most HSM's don't support double ratcheting
    - P-256 is the only elliptic curve that works across 'all' hardware in reality when we looked at

real world devices and their capabilities. This is problematic as some cryptographers don't like that curve and think it may have specific weaknesses built in to enable government bypass

        - That said P-256 based crypto is better than no crypto at all or keys being kept in the filing system so it's always a trade off
        - Don't let *perfec*t get in the way of *progress*
    - Sign then encrypt - The signing of encrypted messages carries some benefits in terms of resilience against attacks against an encryption algorithm as if the encryption is broken the signature won't match
        - In some jurisdictions the signing of encrypted messages carries consequences legally (or is not enforceable) as the signatory cannot see what it is they are signing, they are instead signing an opaque representation that does not hold up in court
        - Q: Why would you not just sign the hash of the encrypted message?
        - <discussion on merits and drawbacks on sign after encrypt and other schemes that went too fast for good notes to be captured>
- Q: What are the attributes that describe the exposure level of a device?
    - For any hardware the reality is there will be many attributes and signals form multiple parties who created the hardware/components – all the way back to manufacture
    - Q: Can this *web of attributes* be used to better trust messages originating from that device?
    - Q: What is the ability to compromise the software in such devices?
        - <references made back to the earlier discussions on physical and network security being different>
        - Secure/trusted/measured boot can all help and bind some measure of current state against a known good
        - There would be a real benefit if public keys were replaced by DIDs in such IoT devices as it would help if keys were compromised
- Q: Does anyone have a good answer for post-quantum crypto for IoT devices?
    - Nope!
    - In general the closer you can put IoT devices 'controllers' to them (e.g. local 'hub' device vs cloud service) the better as the attack targets are more distributed and need to be targeting individually. Additionally the capabilities of that hub are more under your control to adjust and add compensating controls to as the threat landscape continues to evolve (whether than be quantum computing or anything else)

- Cost of IoT devices and controllers is something that needs to be kept in mind, many of the constraints in the capabilities of IoT devices (and the subsequent security properties) come as a direct result of needing a device to sell for $50 rather than $500. We could achieve many of the discussed properties already with current technology but it is cost prohibitive and therefore not done
    - Yes, but isn't the goal to make the technology to improve the situation widely available and thus drive down costs?
    - You can do much of this on a raspberry pi and they are low cost
        - But they you have the problems of trusting and securing a general purpose computing device and whole software stack from multiple different vendors/projects – doesn't this just kick the can on the problems that have been discussed?
    - A good way to balance the costs is to have cheap devices and more intelligence / cost in the controllers / hubs <see prior discussion on post-quantum>
    - Providing ways for IoT devices to interoperate across vendors / transports is a way to lower costs for all

Selective Disclosure (w/o ZKP)

Tuesday 2I
Convener: Joe Genereux
Notes-taker(s): Joe Genereux

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

Claims Proofs; W3C Credentials Working Group Proposal 1.0

- Authors:
    - Joe Genereux joe.genereux@workday.com
    - Rory Martin rory.martin@workday.com
    - Bjorn Hamel bjorn.hamel@workday.com
    - Gabe Cohen gabe.cohen@workday.com

- Last Updated: September 28, 2019

Status

- Status: PROPOSAL
- Status Date: 2019-08-28
- Status Note: Request for Comments (RFC), draft 1

Abstract
The [W3C Verifiable Credentials Data Model](https://w3c.github.io/vc-data-model/#the-principle-of-data-minimization) suggests the principle of **data minimization** to reduce the cost of privacy violations in the exchange of verifiable claims. This document outlines the **claimProof** mechanism proposed by Workday as a solution to achieve data minimization in Linked Data Signatures, and is a natural and backwards compatible extension to the W3C-Spec. The following proposal is intended for migration into the W3C specification as a future addition.

Contents

Proposal

1 Introduction
In [section 7.8](https://w3c.github.io/vc-data-model/#the-principle-of-data-minimization) of the Verifiable Credentials Data Model (here-after **W3C-spec**) we learn that privacy violations occur when `information divulged in one context leaks into another`. It is widely accepted that for individuals and organizations large and small, privacy is becoming a central focus and feature in the exchange of information. Principles such as **data minimization** help reduce the risk of such violations. Hereafter we define data minimization as limiting the information requested, and received, to the absolute minimum necessary.

Verifiable credentials help reduce the risks of privacy violations by allowing the holder to share limited information with a verifier. This is in contrast to the traditional credential verification model where a

verifier talks directly to an issuer. However, verifiable credentials are also susceptible to privacy violations when the credential contains more information than the verifier requires. To address this susceptibility, the W3C-Spec recommends `for issuers [... to limit] the content of a verifiable credential to the minimum required by potential verifiers for expected use.` And correspondingly, `For verifiers, [... to limit] the scope of the information requested or required for accessing services`.

For systems that are using [Linked Data Signatures](https://w3c-dvcg.github.io/ld-signatures) for claims exchange, this specification proposes a mechanism called a **claim proof** that facilitates selective disclosure of individual claims. We recognize that [zero-knowledge proofs](https://w3c.github.io/vc-data-model/#zero-knowledge-proofs) and derived credentials is another technique to achieve data minimization in claims exchange. This document focuses only on systems using Linked Data Signatures.

1.1 Selective Claim Disclosure

The W3C-spec uses a term called *selective disclosure* to refer to the holder's `ability to make fine-grained decisions about what information to share.` When using Linked Data Signatures, the granularity is limited to the full credential. As stated above, this relies on the issuer making a predetermination about `the minimum required by potential verifiers for expected use.` We submit that this will always lead to some level of privacy violation given that the issuer cannot know a priori the minimum set required by every verifier. We believe that the appropriate level of granularity should be on a per claim basis.

We formalize on the concept of **selective claim disclosure**, which we define as the process of only revealing the values and signatures of a subset of claims and withholding all others on the credential. Whether or not that subset of claims satisfies the data requested by the verifying party depends on the credential exchange protocol implementation.. An example is given in the spec: `[...] a driver's license containing a driver's ID number, height, weight, birthday, and home address is a credential containing more information than is necessary to establish that the person is above a certain age.`

There are many reasons why a holder of a credential or a verifier may want to hide the non-requested information. The most obvious case that comes to mind relates that the holder simply does not want a verifier to know any extra information than what is needed to satisfy the proof. Conversely, the verifier, concerned about privacy violations, may not want to be liable for requesting and holding any information that isn't required to fulfill the request. Another reason is simply the less information revealed in a presentation results in less sensitive information being transferred from the holder to verifier where someone might be able to intercept the data in the middle.

2 Claim Proofs

The following section outlines the Claim Proof protocol and its implementation details.

2.1 Embedded Proofs

In a typical verifiable credential (as defined by the W3C-spec), we create an **embedded proof** using a linked data signature. This signature is issued over the whole credential in order to detect tampering and verify authorship of a credential or presentation.

Embedded Proof Example

<pre>

{

<pre>
 "version": "1.0.0",
 "id": "did:work:<cred_def_did>#uuid",
 "type": ["VerifiableCredential", "UniversityDegreeCredential"],
 "issuer": "did:work:abc123",
 "issuanceDate": "2018-01-01T00:00:00+00:00",
 "targetHolder": "did:work:def345",
 "credentialSchema": {
  "id": "did:work:abcdefghijklmnop;spec:uuid",
  "type": "JsonSchemaValidator2018"
 },
 "credentialSubject": {
  "degree": {
   "type": "BachelorDegree",
   "name": "Bachelor of Science in Mechanical Engineering"
  },
  "institution": "UC Berkeley"
 },
 "proof": {
  "type": "RsaSignature2018",
  "created": "2018-01-01T00:00:00+00:00",
  "verificationMethod": "https://example.com/jdoe/keys/1",
  "signatureValue": "BavEll0/I1zpYw8XNi1bgVg/sCneO4Jugez8RwDg/+
   MCRVpjOboDoe4SxxKjkCOvKiCHGDvc4krqi6Z1n0UfqzxGfmatCuFibcC1wps
   PRdW+gGsutPTLzvueMWmFhwYmfIFpbBu95t501+rSLHIEuujM/+PXr9Cky6Ed
   +W3JT24="
 }
}
</pre>

In the example above we have a verifiable credential for a university degree. The embedded proof was created over the entire credential. During verification a holder is able to prove cryptographically she has a credential with the fields *degree* and *institution*; however, because the signature was issued over the entire credential, the holder is not able to selectively reveal only one of those attributes. This can be a very common issue in claims presentations as the holder may need to prove she studied at university but not what degree she attained, or conversely, reveal what she studied but not where.

2.2 Claim Proofs

Hypothetically, the issuer could instead choose to issue individual credentials per claim. In theory, this would allow the holder to selectively disclose information at the granularity of a claim. However, the claims are not truly independent of each other, and part of the semantic meaning of the credential is lost when they are separated. Therefore, we seek to provide a mechanism that extends the current use of Linked Data Signatures to also include proofs per claim.

In contrast to the example above, we would like to extend the use of a Linked Data Signatures from being over the entire credential to also include a signature per claim. This shift in protocol will allow us to achieve *selective claim disclosure* of individual claims.

We outline the following requirements of such an extension:
* It is backwards compatible with systems that do not support per claim signatures
* It still allows the verifier to request the entire credential
* It allows the holder to select any subset of claims that she chooses to disclose

We propose a new property to the W3C-spec, **claimProof**. In this model a signature is generated over *each* attribute in the credentialSubject field followed by a signature over the entire credential using the standard embedded proof model in the section above. Effectively this creates a separate verifiable credential for each attribute, packaged together by the linked data signature over the entire credential. A key difference between using the claimProof and issuing a set of credentials is that the credential metadata is exactly the same and included in the signatures of all of the claims. This binds all of the claims together semantically, but allows for individual disclosure. With this mechanism we are now able to achieve selective claim disclosure of individual properties in a verifiable credential.

If the `claimProof` property is present:
- The property **MUST** be a JSON map with keys corresponding to the keys of the credentialSubject field.
- Signature values **MUST** be generated with *all* credential metadata for verification.

claimProof
<dd>
The value of the claimProof MUST be a JSON map with keys corresponding to the individual keys of claims in the credentialSubject field. Each claimProof field has an independent proof block for verification purposes that is signed over the metadata. If there are multiple credentialSubjects (an array) then claimProof fields may be structured in a corresponding array.
</n>
</dd>

ClaimProof Example
<pre>{
 {
 "modelVersion": "1.0",
 "@context": "https://",
 "id": "did:example:#uuid",
 "type": ["VerifiableCredential", "UniversityDegreeCredential"],
 "issuer": "did:work:abc123",
 "issuanceDate": "2018-01-01T00:00:00+00:00",
 "credentialSchema": {
  "id": "did:work:abcdefghijklmnop;spec:uuid",
  "type": "JsonSchemaValidator2018"
 },
 "credentialSubject": {

<pre>
  "degree": {
   "type": "BachelorDegree",
   "name": "Bachelor of Science in Mechanical Engineering"
  },
  "institution": "UC Berkeley"
 },
 "claimProofs": {
  "degree": {
   "type": "RsaSignature2018",
   "created": "2018-01-01T00:00:00+00:00",
   "verificationMethod": "https://example.com/jdoe/keys/1",
   "nonce": "123456",
   "signatureValue": "..."
  },
  "institution": {
   "type": "RsaSignature2018",
   "created": "2018-01-01T00:00:00+00:00",
   "verificationMethod": "https://example.com/jdoe/keys/1",
   "nonce": "123456",
   "signatureValue": "..."
  }
 },
 "proof": {
  "type": "RsaSignature2018",
  "created": "2018-01-01T00:00:00+00:00",
  "verificationMethod": "https://example.com/jdoe/keys/1",
  "nonce": "1234",
  "signatureValue": "BavEll0/I1zpYw8XNi1bgVg/sCneO4Jugez8RwDg/+
   MCRVpjOboDoe4SxxKjkCOvKiCHGDvc4krqi6Z1n0UfqzxGfmatCuFibcC1wps
   PRdW+gGsutPTLzvueMWmFhwYmfIFpbBu95t501+rSLHIEuujM/+PXr9Cky6Ed
   +W3JT24="
 }
}
</pre>

In the example above we have reissued the same education credential, but this time we want to give the holder the freedom of selective claim disclosure over her individual claims. She now has the option to prove where she studied but not what degree she earned, as well as what she earned but not from where. Because she also still has the embedded proof over the entire document, she still also has the ability to present the entire credential should both fields be required in a presentation or if the verifier *does not support the claimProof property* which we establish as a backwards compatible requirement for the spec.

Validation

The following JSONschema can be applied to validate against a credential containing a claimProofs block.

<details>
<summary>Show/Hide JSON Schema</summary>

```
{
  "$schema": "http://json-schema.org/draft-07/schema#",
  "description": "W3C Verifiable Credential using JSON interchange format",
  "type": "object",
  "properties": {
    "modelVersion": {
      "type": "string",
      "pattern": "^\\d+\\.\\d+$"
    },
    "@context": {
      "type": "string"
    },
    "id": {
      "type": "string"
    },
    "type": {
      "type": "array",
      "contains": {
        "const": "VerifiableCredential"
      }
    },
    "issuer": {
      "type": "string"
    },
    "issuanceDate": {
      "type": "string",
      "format": "date-time"
    },
    "credentialSchema": {
      "type": "object",
      "properties": {
        "id": {
          "type": ["null", "string"]
        },
        "type": {
          "type": "string",
          "enum": [
            "JsonSchemaValidator2018"
```

```
      ]
     }
    },
    "required": [
     "id",
     "type"
    ],
    "additionalProperties": false
   },
   "credentialSubject": {
    "type": "object",
    "minProperties": 1
   },
   "claimProofs": {
    "type": ["null", "object"],
    "patternProperties": {
     "^.*$": {
      "type": "object",
      "properties": {
       "type": {
      "type": "string"
     },
     "created": {
      "type": "string",
      "format": "date-time"
     },
     "verificationMethod": {
      "type": "string"
     },
     "nonce": {
      "type": "string"
     },
     "signatureValue": {
      "type": "string"
     }
      },
      "required": [
       "type",
       "created",
       "verificationMethod",
       "nonce",
       "signatureValue"
      ],
```

```
      "additionalProperties": false
     }
    }
   },
   "proof": {
    "type": "object",
    "properties": {
     "type": {
      "type": "string"
     },
     "created": {
      "type": "string",
      "format": "date-time"
     },
     "verificationMethod": {
      "type": "string"
     },
     "nonce": {
      "type": "string"
     },
     "signatureValue": {
      "type": "string"
     }
    },
    "required": [
     "type",
     "created",
     "verificationMethod",
     "nonce",
     "signatureValue"
    ],
    "additionalProperties": false
   }
  },
  "required": [
   "modelVersion",
   "@context",
   "id",
   "type",
   "issuer",
   "issuanceDate",
   "credentialSchema",
   "credentialSubject",
```

```
    "claimProofs",
    "proof"
  ],
  "additionalProperties": false
}
```

</details>
Interoperability
In order to be more compliant with the existing W3C-Spec we recognize that breaking out the per-claim proofs into a new property fits more appropriately in the extensibility model. Effectively the claimProof property could be ignored and the overall proof and credential would still be valid.

Signatures Note

From the W3C-spec: `Because the method used for a mathematical proof varies by representation language and the technology used, the set of name-value pairs that is expected as the value of the proof property will vary accordingly. For example, if digital signatures are used for the proof mechanism, the proof property is expected to have name-value pairs that include a signature, a reference to the signing entity, and a representation of the signing date.` This holds true for claimProofs as well and it is RECOMMENDED that all proofs use the same format in the verifiable credential.

Example RSA claimProof structure:
* `key of credentialSubject claim`:
  * `type` type of signature
  * `created`: Signing date
  * `verificationMethod`: method of signature verification
  * `claimSignatureValue`: signature of the credential with the single claim present.

2.4 Proof Request/Response
A separate proposal to update the W3C-spec to support proof requests/responses for individually signed attributes on a credential will also be submitted.

Drawbacks/Limitations
- The **claimProof** field is optional and relies on the issuer to include it when issuing credentials and the verifier to support a credential exchange protocol that uses it.

Alternatives
The following are a list of known alternatives to achieve selective disclosure over verifiable claims:
- Issuing a separate credential for each field in a schema
- Derived Credentials with Zero-Knowledge-Proofs
- Signatures included as part of the credential subject field. (this was also explored, but that forces direct incompatibility with the W3C-Spec so it is less desirable).

The authors of this specification would like to remain very clear that while we are able to achieve selective disclosure without the use of ZKP's in verifiable claims presentations, we are **NOT** dismissing the unique and desirable properties that are provided using ZKP schemes and believe that *both* models each serve unique purposes in claim presentations. We therefore recommend that organizations evaluate both models and make a decision that fits their business use case and needs. We anticipate that future platform implementations will allow for *both* zero-knowledge proof and attribute level signatures as part of their supported feature set. The use of such hybrid platform schemes are also being explored and we recommend that the community further explore how to interoperate at the protocol layer to support both schemes.

Privacy Considerations

- As with any disclosed presentation with verifiable credentials, this proposal for claim proofs over individually signed attributes does not obscure the revealed attributes. This is in contrast to a Zero-Knowledge Proof based system (such as CL-Signatures used in Indy) which has the ability to to attest a claim in zero-knowledge if it is sufficient for the verifier's request (if not done in zero knowledge the properties are still revealed and thus suffer from the same vulnerability). All credential verification and issuance should be treated with care by implementers regardless of the solution.

- It is the opinion of the authors that no matter what techniques are taken to minimize the risk of privacy violations (including zero-knowledge proofs), that privacy violations can *still* occur. We would like to reiterate and emphasize on [this](https://w3c.github.io/vc-data-model/#the-principle-of-data-minimization) point made by the w3c-spec authors about privacy: `While it is possible to practice the principle of [selective] disclosure, it might be impossible to avoid the strong identification of an individual for specific use cases during a single session or over multiple sessions. The authors of this document cannot stress how difficult it is to meet this principle in real-world scenarios.`

References

- W3C Verifiable Credentials Specification: https://www.w3.org/TR/vc-data-model

Deepfakes: Tools & Rules To Save The Open Internet: What? How? Why?

Tuesday 2J
Convener: Kathryn Harrison, founder, DeepTrust Alliance
Notes-taker(s): Scott Mace

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

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

Was part of the IBM blockchain team

My first IIW, diving right in

https://www.DeepTrustAlliance.com

Definition of deepfake: Technique for human image synthesis based on AI. Created through the combination and superimposition of existing images and video using a ML technique called generative adversarial network (GAN)

This summer there was the cheapfake of Nancy Pelosi. Not a new problem. Fraudulent content has existed since before the printing press.

Tools are rapidly accelerated. Cheaper and faster to build this.

Motivated enemies.

In this country hard to have an honest discussion on it.

Will impact every industry that does business on the internet. How do I know if this is real.

Today you have a few options. Look at the web site. Look for caption or source. Or use your eyes.

Social engineering

Market manipulation. Casino Royale movie. Could publish a CEO saying whatever, market might correct itself quickly, make a ton of money in short term.

Extortion and harassment. Rana Idowa, fake porn created in India.

Banking and financial services. Already seeing fake audio theft of hundreds of thousands of dollars, CEO's voices impersonated.

Social media fakes

Democracy

Just the tip of the fakes iceberg.

2.1 billion fake FB accounts diabled in Q1 2019.

Fake followers, fake views.

Why now?

Will take tech and human solutions to solve it.

This market is incredibly fractured. FB solve for FB, Google for Google, NYTimes for NYTimes.

But content ricochets across the net like a pinball.

Need persistent verification of content via an open standard.

If anything is going to get to scale, it has to be done in an open way.

We are dealing with potentially nefarious actors, and this is an arms race.

We need to pull together all the different parties impacted by this. Think about how this is going to impact their business. A lot of fear. Executives' plans, we haven't seen anything major right now. Not sure. That has to change. So much work needs to happen.

This is what I am driving toward. There needs to be a way to go from the digital edge, the real world, so you can know the source of the content. Plug into existing identity solutions. Already lots of metadata standards, but all that gets stripped out in FB, etc.

A checkmark could say we know the source of this content. A standard.

An opportunity to go from the device. Apple 10S phone onward, why couldn't it generate a key where it was taken.

Q: Similar to email spam problem. How can we trust who signed the message?

Scott Mace: Content that's guaranteed anonymous?

Q: Goal of masquaroca is to change your view of reality to what your adversary wants you to believe is real to change your decision process. Our brains are attack surfaces to change our view of reality. People trust crackpots.

Q: We don't have a society any longer with sources that people trust. Trust is a way bigger problem than the technology.

Has to be both technical and societal. We don't have a clear lexicon for defining these things. Every company decides what is real or not. Reddit pulled all the deepfake channels. FB keeps deepfakes. Doesn't flag them, just doesn't put them up in the newsfeed. There's a whole spectrum to misinformation. Info is wrong but you don't mean for it to be used in the wrong way. Needs to be set of rules and best practices so

companies aren't necessarily trying to make decisions on their own. In August, journalists put Cloudflare in spotlight, for hosting 8chan manifestos. There was no line in the sand, this is as an industry how we think about these things. Given it's a network problem, dozens of state actors and others navigating through these policies, we need to create these best practices to have this line in the sand. It is a question of how far back do you go to answer the question what is real. Measuring intent is extremely difficult. One way is to warn them they may be looking at false information. Checkmark or confidence score.

Q: Warning on pack of cigarettes. Let's say we are successful in identifying deepfakes. What's to keep it from here is my official version.

Scott: Right to be forgotten abuse.

Trying to run forensics with traditional statistical analysis is getting difficult.

Q: Regarding warnings falling on deaf ears, the cigarette risk is a static variable. But if you say in this community there is a likely possibility you will be pickpocketed today, it's different on the human psyche.

What are the seat belts or air bags as you get into dangerous situations. Automated safety features.

Q: It's a spiritual problem.

Scott: How will this intersect with / conflict with publishers' notion to get more compensation for content they product today but is ultimately monetized by others?

The first product we're working on is a digital watermark for images.

A few standards could give you a ledger that provides a standard for the provanance of content.

Scott: recent selfies people have taken that end up being used in a Trump ad. Need technology to detect that, without the whole world having to detect it.

Does consent become part of this?

Virginia cracking down on deepfake porn and lack of consent.

Scott: How do we protect Edward Snowden's physical address from being disclosed.

And yet verify it's Snowden.

Deepfakes can be hilarious. But at least you know where it came from.

Q: I believe people are starving for trust. Teaching media literacy in school.

Q: Are our cars safe?

Scott: Pedestrian injuries & deaths are way up.

We will launch officially in November. I have a mailing list.

OpenID Connect for Identity Assurance

Tuesday 2L
Convener(s): Torsten Lodderstedt (yes.com)
Notes-taker(s): Neil Thomson (QueryVision) & Torsten Lodderstedt

Tags for the session - technology discussed/ideas considered:

OpenID Connect, Proofing, Identity, Assurance, Validation, Verified Claims

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

Link to Torsten Slidedeck:
https://www.slideshare.net/TorstenLodderstedt/openid-connect-for-identity-assurance-178535795

Notes from Neil Thomson:

Torsten (w slide deck) presented the core concepts behind the Use Cases driving the need for Identity Validation/Certification/Assurance as being driven by German standards/compliance (e.g. Anti-Money Laundering Laws, Telecommunication Acts, Anti-Terror Laws, and regulations on trust services, such as eIDAS) governing Health services use cases for users accessing their own health system data.

The proposed standard defines the presentation of verified vs non verified claims via the JSON package provided by the IdP to the RP, plus the ability of the RP to query for both claims and verification metadata about those claims in the RP/IdP communication protocol.

The key requirement is the need for the RP to be able to retrieve validation metadata about user claims (from the IdP) to ensure that requests don't proceed if the user does not meet the validation criteria.

The proposal for OIDC identity assurance is focused on the unchangeable "natural" data about a person in the health system. For example, this includes unchangeable information about the physical person (birth family name, country… and birth records), but not email or current address, which can change over time.

The proposal adds a number of claims to enhance the current OIDC claims for the "natural person". This may not be complete.

Torsten emphasized that the intent of the proposal was a "MVP" (minimal viable product)/pragmatic approach, based on dealing with the minimal complexity based on concrete use cases and standards which have been proven in initial application - as a starting point which could move forward immediately, with updates based on a new proposed Working Group.

The proposal is based on actual working solutions based on customized OpenID Connect solutions, which are in the process of being upgraded to use the new Identity Assurance specification – so the proposal is based on working, German regulatory compliant solutions, including online/electronic signatures.

He also emphasized that this specification must – by design – accommodate evolution of the metadata and techniques used for validation.

The discussion quickly changed to questions, observations and additional requirements (in support) of the proposal.

The presentation is about the solution to the standards/requirements driving a pragmatic solution to those factors

What are the use cases driving Identity Assurance?

This should be documented and expanded by proposed Work Group (WG) contribution

The proposal doesn't currently allow for claims to be individually be validated by different Trusted Providers.

The dividing line between the "biological person" vs. the "data person" is difficult to determine. Perhaps this needs to be determined by convention/input from the proposed WG

A key point is the accommodation for verification determined by multiple Trust Frameworks, with each claim being validated by traceability to one or more Trust Frameworks.

Requesting individual claims vs using scopes - feedback

This is potentially a privacy issue for RPs requesting claims they should not be allowed to ask for (phishing for personal data). Suggest some standard "Scopes" which are pre-defined for "unchangeable person" metadata to avoid this problem.

Request for having the Trust Framework (TrstFrmWk) identified for each claim (e.g. if the "natural person" claims are provided by multiple TrstFrmWks

RPs filtering – the concept of the RP can request which claims to return and which must be verified plus how they are verified

The proposal was well received – allowing the RP to request only the data it requires.

This should be extended to allow the RP to specify which Trust Framework(s) must be included in the validated claims request.

The standard should include the ability to extend what metadata is required (as this evolves) by the specification supporting extension

Observation (from several) – Trusted Frameworks may be common in principle, but in practice are Country specific (e.g. EU standard, but Italy has their own variation) – so determining a common set of claims is complicated (observation: almost random selection and mapping from one country to another in EU).

Perhaps an abstracted model of claims will mapping to individual Country (or other jurisdictions) claims organization or naming is required to have sufficient commonality to avoid an explosion of claims (and complexity for RPs). There was consensus that a mechanism to stop an explosion in complexity is required.

How does the IdP know which Trust Frameworks can be trusted? Are they subject to a tiered level of trust (from weak to strong)?

On the subject of explosion of size of URLs that include claims parameter requests:

Use JPATH?

Incompatible with OpenID Connect

Torsten proposed new “Push Authorization Request” – proposal to be tabled soon to avoid “piping” large volume of data via URL requests.

Question – how to conduct verification based on consent from the user on the individual claims?

It was proposed to determine how to integrate consent (by the user) into the validation process

The current proposal leaves the user consent at the discretion of the OP

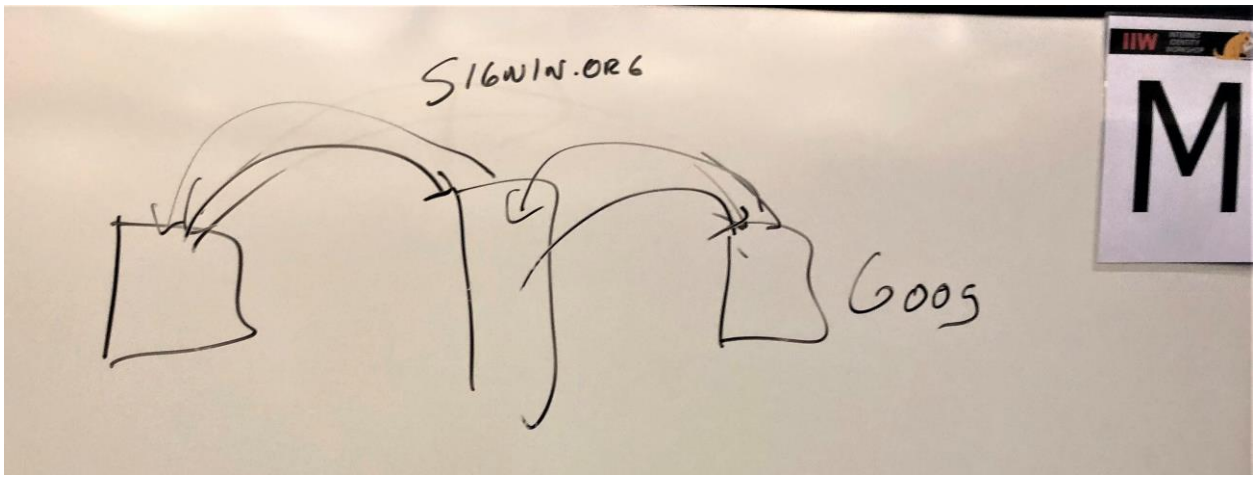
SignIn.org What Is It?

Tuesday 2M
Convener(s): Dick Hardt
Notes-taker(s): Dick Hardt

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

SignIn.Org allows users to use the provider of their choice to get the convenience and security of a provider, without the provider or the developer knowing who each other is.

Image of how SignIn.Org works.



Beyond Bearer Tokens?

Tuesday 3A
Convener(s): Annabelle Backman
Notes-taker(s): Darin McAdams

Tags for the session - technology discussed/ideas considered:

OAuth, Sender Constrained Tokens, Token Binding, DPoP

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

Requirements

- Sender Constrained tokens
- Authenticity/Integrity of the message, binding the request to the proof for greater assurance on the request contents sent by legit party.
- Scalability/Distributability, needs to work across highly distributed fleets, both clients, RS, AS.
- Performance, in some case single digit millisecond latency goals
- Headers or QS
- Browser Clients, Single Page Apps (SPA)
- Streaming, or traffic with large request bodies

Current Solutions

- TLS Token Binding (RIP)
- Mutual TLS
- DPoP
- HTTP Request Signing, couple draft specs
    - One based off experience with OAuth 1.0
    - Another variant based on OAuth XYX, only signing a detached document signature, not all HTTP request contents.
    - Another one presented by Cavage, but only a presentation. Not picked up yet. Started as a way to sign headers. Can also sign a message digest, but mostly header signing.

Discussion

- Token Binding is dead.
- MutualTLS:
    - Fails the browser use case.
    - OK when hosting your own webserver, but difficult when outsourcing your edge to a cloud provider. Lots of layers between, say, an AWS Lambda function and the caller. TLS information not always available when service is fronted by edge services.
    - Add another requirement: works with TLS offloading.
    - Should we try to fix that problem? There was a draft spec, but went nowhere. Would need to be adopted by all the reverse proxies and edge providers.
    - May come back to this…

- Okta: tried a proof-of-concept with DPoP + Request Signing. Multiple RSA signings resulted in a performance hit. Must be mindful of the amount of signing.
- Question – do we have a viable solution for achieving authenticity and integrity at scale?
- To people in the room: what OAuth scenarios do you have which are currently unsolved by bearer tokens or mTLS?
- We have a long history of working with Smart Cards, looking for signing where keys are coming from a secure element, external element plugged in. Moving from Windows to Linux, that model changes. We want a web application, with a consistent user experience, where the browser could talk to device. That use case is being done in the WebAuthn space, but want to extend into the request.
- Humans in a browser - Increasing barriers to get access to a bearer token, but still many scenarios. Would like more protections here.
- Duo – we have our own signing approach we had to invent.
- If we have anomaly detection for bearer tokens, is that enough? All these mechanisms are complementary means to address the risks of token theft and message replay.
- Should we revive TLS Token Binding? There is a fork in the road coming: do we want a world where TLS is end-to-end encrypted all the way, or do we want to keep man-in-the-middling ourselves.
- May see both scenarios continue playing out. Don't need a panacea answer. May see different technologies for different scenarios.
- Don't know it's meaningful anymore to ask what TLS is trying to solve anymore. So much virtualization is happening in the networking stack to create a modern, identity-aware firewall, service meshes, routing across VPCs dynamically… do not assume architecture is always client through TLS to webserver. If you want to use that approach, go for it. If you don't, we need more options.
- Increasingly, there are more hops in the chain. E.g. end-user to point to point to point. Desire to know the originating end-user and all the hops in between. That's becoming more important than just presuming a single channel.
- Agreement that we'd like a stronger alternative to bearer tokens in places where mTLS isn't the answer. Don't know what that answer is, yet.

User Managed Access (101 Session)

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

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

Link to slide-deck for this 101 session:
https://kantarainitiative.org/confluence/download/attachments/17760302/2019-10-01%20IIW%20UMA%20101.pdf?api=v2

SeedQuest 3-D Game Mnemonic Cryptographic Seed Recovery

Tuesday 3C
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:

Link to slides presented:
https://github.com/SmithSamuelM/Papers/blob/master/presentations/SeedQuest_Didery_IIW20181023.pdf

Identity Coop (OpenID Connect, ID Assurance)

Tuesday 3D
Convener(s): Alan Viars
Notes-taker(s): Alan Viars

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

We discussed the concept of an "Identity CoOp" where member organizations would trust the identity assurance verification performed by agents/employees of other member organizations.

This would form "Circle of Trust" between Organizations.

The benefit of such a setup in a health care scenario, from a consumers point of view, would to allow a user to authorize access to data from different data sources without having to login to each provider individually (with separate usernames and passwords).

We discussed the potential issues with such a setup. These include:

- Introducing a new Identity Provider would be a heavy lift for data resource providers. In addition these organizations already have existing authentication mechanism and may be apprehensive to trust a 3rd party.

Key Takeaways

- Instead of trying to create a monolithic Identity provider, instead it might make more sense to profile OIDC and encourage organizations to comply with the profile.
- The core component of the profile would be verified person claims pertaining to identity assurance.
- A governance model would be needed to certify IDPs that met the specification and agreed to be part of the CoOp.
- If large IDPs, such as Microsoft, Apple, and Google participated, it could have a wide reach and provide a smoother user experience. This would not exclude a hospital or other data holder to have their own IDP that met the profile and CoOp membership requirements.
- It was unclear how such a model would work from a consumer's perspective. Whould the login be a very long list of potential places to sign on?
- We discussed the "Interac" model in Canada and Identity brokers.
- Pointers were given to an open source OpenId Connect provider that supported verified person claims. https://github.com/TransparentHealth/vmi

Spirituality, Abundance Mindset, Personal Identity, Role in Community

Tuesday 3E
Convener: Brent Shambaugh
Notes-taker(s): Brent Shambaugh

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

facebook manipulation for it own goals....what you think and what you want....

aspirational goals....

build goals for yourself....

black box of data

goals interests, aspirations, getting in better shape....

capture digitally, what your version you think you....

the best data

ai is a reducing value....

identity is a fine thing....

crisp boundaries.... we know what an individual.... microbes outnumber ten times....

these identities .... relative to something else....

identity is defined by contrast....biology and ecosystems, and what life is in general....

organism... liver has its own shape, everything is a continuum, individuality.

self is a noun. it is not a verb. technology,it is very rigid. one of the foundations is empowering users with the insights with an inaccessible black box.

how do you prevent ai from abusing your identity. there is not an ability to interact. you can tell them whether you want ads or not.

the algorithms of where my minds are, they reflect our own mental patterns.

you always gain something, but it is still your own mental patterns, you make progress. There is a huge value in doing your own inner work.

what if your digital identity, what if you conspire with the technology to be reflecting on yourself. there is no meaningful way with the ai to interact (to get it to go where you want).

the incentive structure is to make a buck on advertising, but to optimize on human growth and human flourishing...

the whole structure is based on profit...the whole system is set up... I know as a marketer that a hot lead is a good thing.

profit needs to be made, and something....I need to live in a gift economy... optimizing a system for efficiency

the ai will maximize.

Is that what you want to talk about? Brent is dealing with an existential crisis.

we have a massive intractable problem.

how do you define boundaries.

what is identity when you get a brain transplant...

what is self? what is biology? Mark says that self is consciousness. Marius ...

what is consciousness.... what tunes into the same thing.... far out speculation. ...

for a sane and just society...the work begins on our-self.

when an artist in in the zone. that is the space of larger self. all creators. I did not really create this. it just came to me.

there is a conference coming up. science and non-duality. that and wisdom 2.0.

this looks like a bunch of rambling. Mark: I think that it what it is.

evolve....making space...identity is one of the big ones. the state of playfulness gets you closer. your whole thing shifts. Normally we are anxiety driven, but deep creation comes from there.

the universe does not always agree with what you want...

when you operate on the universe...

the right action in the world is to be here now. we are transparent to allow that force to go through you.

if you are present....with very good intentions very bad things can happen....

technology is evolving us...

Expanding Language…Digital Harms Dictionary (Me2B Alliance)

Tuesday 3(F)
Convener: Jeff Orgel & Lisa LeVasseur
Notes-taker(s): Jeff Orgel

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

We reviewed the issues related to surfacing and crafting language regarding various categories of harms people may experience in their relationship with brands and their products and services.

Examples of reputational, financial, informational and physical harms are review for impacts and implications for those involved, correlated documented examples, legal bases of redress, suggestions.

Please submit any suggestions for edit to jeffo@whatisyourrealit.com rather than editig the workspace directly.
https://workdrive.zohopublic.com/sheet/open/dv1v1d27c51171bf045928d475d3b9a84d7a5/sheets/Version%201/ranges/A1

Identity Bot for SSI (HBO)

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

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

Slides presented are here: https://docs.google.com/presentation/d/1-9Q7Cga1Dw5HiTJEOhzbKG0ANc35ZfUC7xHgvmJRviE/edit?usp=sharing

The aim of the session was to collect wisdom from the attendees including problems, insights and questions about the approach.

Attendees contributed problems, insights and questions to be considered:

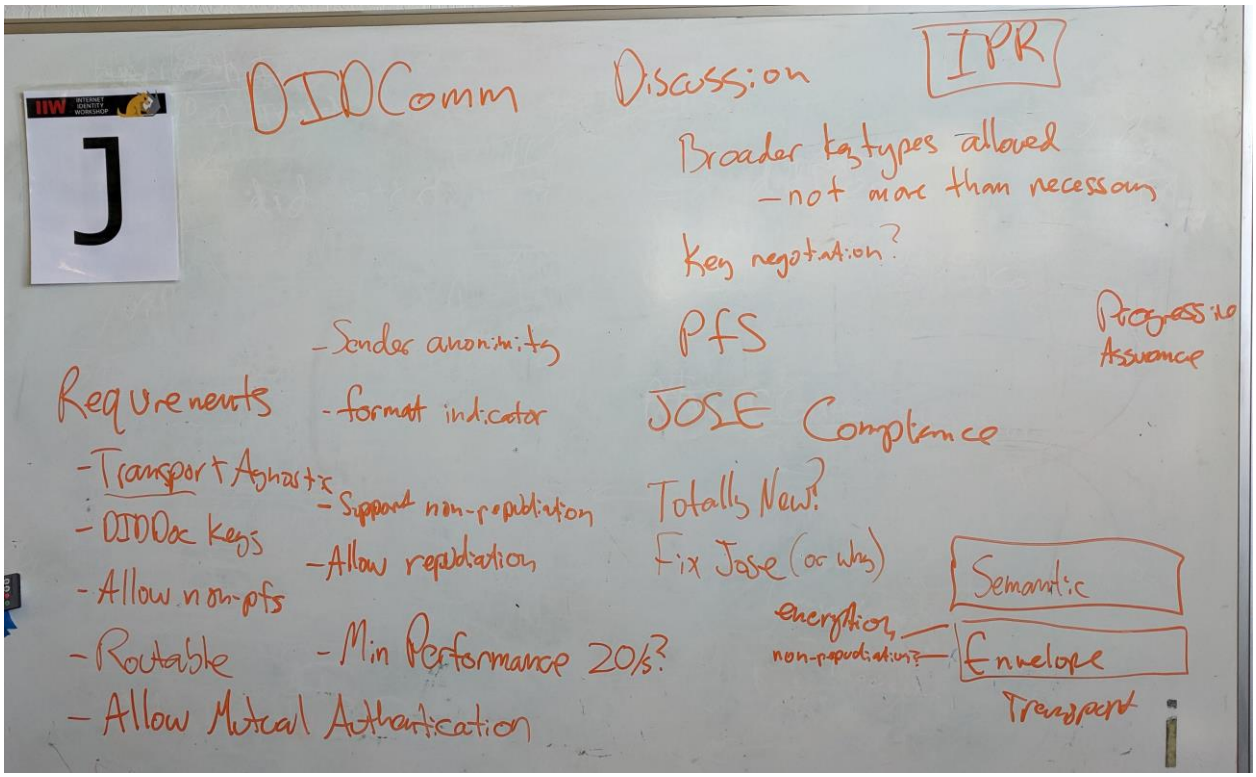
1. Cost of hosting
2. Trust of the hosting provider
3. Connecting DID and DNS (cf another session today)
4. Dealing with flow dependency failures
5. Migration issues for relying parties
6. Use of work such as OpenID Connect CIBA
7. Concurrent implementation issues

There was a discussion about these, and we hope to continue collaborating with participants as we develop this approach

DID Comm Encryption Envelope Discussion

Tuesday 3J
Convener(s): Sam Curren
Notes-taker(s): Sam Curren

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



I'm Adam, Now Leading Digital ID @Equifax.How Can I Help? What Should I Do?

Tuesday 3L
Convener: Adam Gunther, Vice President, Digital Identity at Equifax
Notes-taker(s): Scott Mace

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

Replies are Adams and do not represent the thoughts and opinions of Equifax:

My fourth IIW.
Prior, led decentralized identity at IBM.

One thing that frustrated me on decentralized identity was the slow pace.
BC demo is great, how do we get 20 governments to do this.

When the opportunity came to be at a data provider, now I can DO this.

In charge of digital identity at the company.

We do a lot more than credit reports. We have a few different business units. One is on workforce solutions. Onboarding employees. That's an Equifax product. A lot we do around fraud not just consumer credit but B to B.

We see our role as helping people and businesses to do business and transact more by powering decisions with insights and analytics.

Consent is a great thing. We now have an opportunity to infuse consent and user control into the center of the process.

There is value in us issuing that data to you, cryptographically signed data. To help you do business. Self-asserted credentials will not work for business. We should not confuse self-sovereign with self-asserted.

The business model, I'm still figuring it out. In general, businesses are willing to pay for trusted data. Consumers will pay for some things as well. Today when I go to apply for a mortgage, I don't view them doing a credit check on me as something I pay for. I'm telling the bank go talk to these credit agencies. I would much rather go to the credit agency and say this is the stuff I need.

There is a lot of energy and excitement within Equifax around the role of decentralized identity.

Blockchain: Certainly a part of everything we're doing in decentralized identity. May be part of what we do tomorrow. Get off things like SSNs. Trusted digital commerce. If blockchain helps us, great.

Q: Instead of uploading data to Equifax, give results of local computation back to Equifax, to calculate my credit score.

Holding on to big honeypots of data, we've seen the downside of that. I'm excited as well when I'm presenting that data in real time, it helps me tell that's you.

Q: what part of honeypot is still a requirement for you and your industry?

Nothing jumps to mind. The key thing is to vouch for and provide trust. What is the minimum we need to stand behind that. I've come in because Equifax sees a huge opportunity. The secure key network in Canada, now live, Equifax is the first data provider in that network. This is cool. Now where do we go with it?

Q: What is the most needed thing?

Production network for blockchain, the whole ecosystem.

Q: So how do you deal with the problem that if you're successful, people will ask for all the information? It becomes the only way you can sign in for something completely trivial. Prevent race to the bottom for privacy.

Pan-Canadian Trust Framework. Won't be Equifax's role to legislate that stuff. Not something one company can control. Equifax started with Secure Key Canada. SecureKey has a governance framework.
For example, people who sell alcohol are allowed to ask for zero-knowledge proof to prove you're of age to drink. They cannot ask for your address. It's far from solved but that's the space to attack those types of problems.

Adrian: What's the difference between a good-guy data broker and a bad guy. Anyone who is a hidden data broker – bad. Certain principles – strong privacy laws. Things like that. Good guy data broker uses standards.

In this new world, there's a way that with the right privacy constraints, zero-knowledge proof, a company can do analytics without knowing more about you. A way we can help without leaving us susceptible to the kind of problem you're talking about. There are regulatory evolutions that need to happen.

Q: Don't give up on the data broker thing. Most of us aren't crypto-anarchists. I don't want to hold all my data and all my keys. How about a model, give me the opportunity, I can lock and unlock my credit, give me some keys, in return will you sign this. You're still the data aggregator.

That's a value we can add. I don't like the word "broker/aggregator." Preserves more of the privacy than you have today. We need a new term for the new world.

Q: You're doing it now but I'm out of the loop.
That's a good first step. Thanks for the feedback.

Adrian: Say zero-knowledge proofs and regulations break your way, how do you deal with the ML benefits of being able to be in the middle of all these transactions?

Speaking for myself, not Equifax, followed MIT work on open algorithms. That and transparency help people understand what's happening there. That's a space that can help.

Adrian: Why not use the MIT model and do federated learning, not centralized learning?

This is something to explore.

Q: We have enough robust tech to do experiments. Breakthrough will be when people who have different business models try this. Make sure I have an internal budget for proof of concept. Educate the different aspects of the company, what the value of self-sovereign identity could be. Understand the biggest costs. Run some brainstorming sessions to build internal buy-in. Kick up executive chain budget approval for some small pilots. Would try to share aspects of this info externally to show Equifax is a thought leader.

Adrian: A comment. To some of us, the problem is not having enough friction in the system. Praying to the god of adding value or reducing cost of certain transactions looks like something we might not want to do to begin with. Lawyers introduce friction. Doctors over selling of drugs OTC on purpose. As a society when we get into things where the regulations are difficult, we introduce very expensive friction, in order to allow the institutions and society to evolve the norms that we need. Competing on the efficiency of this is worrisome at that level. We're not prepared to regulate.

Q: I want to go back to the beginning. Your company has a trust issue. They hired you, an expert in the field, to fix something. I don't know what the value proposition of your company wants to be. I'm not going to be successful until I know where you want me to go. In interviews, they asserted something to do. Find a clear road. You're in a sticky situation.

We have to be clearly articulating that value prop back. Show of hands – Equifax can help, not sure, Equifax shouldn't exist. (results of poll stayed in the room)

Q: Who watches the watcher? You have to bring in other bodies to check your own power.

Scott: Some people say if the credit bureaus went away, companies like Acxiom would be just as bad or worse.

Q: We're still seeing the reaction of the way they're handling it. In five years, is anything going to come of this?

The fact is, once I get that SSN, the crook can impersonate you. We have an opportunity to make sure that cannot be used by anyone else. When that happens, let me revoke and reissue your keys.

Q: SSI requires high-value issuer. Replace SSNs with move accounts over to privacy-enhanced identifiers. Architecture allowing newer protocols to become real in the market.

Everything being driven by DIF is the way to go, is my opinion. SecureKey joined DIF. We have to participate in the same open standards as anyone else.

Q: Still a gap in negative history. I don't have an incentive to share about my car accident, my bankruptcy. It's a beautiful role for some third party that has negative, toxic information. Someone's got to do it, where the bad stuff can accrue where someone gets the whole picture.

Today you don't have a choice on who that third party is. Still need regulation and control.

OpenID Connect Federation BoF

Tuesday 3M
Convener(s): Roland Hedberg, Mike Jones
Notes-taker(s): Nick Roy

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

Interpreting the policy language has to be 100% deterministic and water-tight, or you will have big problems.

If you evaluate the chain of policies, can you have places where you throw an error, or will you always return a result?

Sometimes throwing an exception allows you to detect problems, not always best to ignore conflicting statements. Some times they meant something else, and if you don't throw an exception, they'll never know. This is where the "MAY" comes in about informing you what's going on. An exception should never carr meaning, it should purely be for debugging.

Major change that was made recently: .well-known URLs are supposed to point to configuration, not API endpoints. Depends on your definition of API endpoints, but OK. OIDC uses this to get the config, and from that a number of endpoints. The change that was made made the profile more aligned with how OIDC core does this.

If you are interrogating an entity for its view of itself, you use .well-known. If you want to know someone else's opinion of an entity, you use the federation API. Went from a one-step, to a two-step. Eventually you will cache the results.

With the change in place, what is the data structure that you retrieve at the .well-known URL? A signed entity statement. Doing this split into two allows you to have different endpoints. Lets you put the federation API on a different domain/etc.

A number of other changes, one change was authority hints. A pointer to a superior, but coupled to that, info about where you would end up if you talked to that superior and kept climbing up the list. Comment: How would the leaf know anything about what's above it? The reason authority works in X.509 is that we don't play around with self-signed, use whatever the CA gives us. In this case, we are using our self-signed statement, and we are using the CA as an added feature. There's no way to feed the CA path back into the self-signed construct.

Trying to put information in a data structure that's not reliable is not reliable.

Apart from that things that have come up lately are constraints- trust anchor constraints, for example: "You can only have 2 intermediates, or zero intermediates." Another: Naming constraints - entityID. Might not be used that much by the trust anchor, but by would be used by intermediates. Path depth restriction helps you as an FO restrict behavior that you're not vouching to by, say, allowing zero intermediates.

Key duration and rollover: I require my subordinates to issue statements with validity no greater than t timespan (say, one day).

Idea is that the validity window of any subordinate statement has to be less than the parent.

Without a flexible enough policy language in the implementation profile, you can't support it in practice using a deployment profile intended to inform how to build a real federation.

Key rollover for FOs is already suported by just creating a new trust path with the new key and keeping the old one around for some period of time.

The thing you are issuing can't be valid longer than the thing you're signing it with.

Mike is going to review the current draft and make suggestions. What of the rest of the stuff is checked in? Max path and naming constraints are checked in. Max validity is not, but could be easy to check in if it's needed. That is non-breaking if you ignore stuff you don't understand as an implementation.

What do you do when a subordinate tries to set a value that has already been set by a superior? Easiest one is you always go with what's been set by the superior. Have to think about that.

Is the policy language expressive enough? The more expressive you make the policy language, the less possible it is to implement correctly.

Leif suggests that we do a gap analysis with PKIX, make sure that the policy language covers what's in PKIX. The fact that the web PKI is flat isn't a good argument for why we shouldn't put stuff like this into the federation spec.

Don't need to do gap analysis against SAML because this stuff doesn't exist in SAML metadata, we enforce it via federation management tools.

Having the "CA Bit" - can you issue stuff from this/path length=0 is a fundamental need.

There is a lot of cruft in PKIX that we wouldn't want to bring over. Look at it, "are we going to miss this bit when we don't have it?"

Mike suggestgs looking at this against not just what's possible in SAML metadata, but also how we deploy SAML federations using the tooling.

When they were building OIDC, one of the best things was getting feedback from the developers in Japan. We need implementations and testing of their interop.

Recruiting cross-sector implementers to attend the hackathon at TechEx in 2019.

Introduction to WebAuth/Fido2 (101 Session)

Tuesday 4B
Convener(s): Chris Slade & John Bradley
Notes-taker(s): Nick Roy

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

W3C API spec called credential manager
User agent has a webauthn javascript api, talks to RP and the webauthn device.
Two basic javascript commands are get credential and make assertion.
User agent presents a UI that shows you which authenticators you can use.
Major difference between webauthn and U2F: Resident credentials- you can make a credential that lives on the platform of the authenticator. Passes info down to the user agent, platform authenticator creates keypair, stores persona/key/RP ID, creates pairwise cred for that RP. RP says: "get me this credential." Platform looks at the various authenticators, interrogates them for credentials for the RP, and if there is more than one, gives you a pick list.

RP can specify that user verification is ???/preferred/required. There are local verification methods available on the platform.

The secondary verification is per credential, not per RP.

Authenticator creates an attestation that goes back to the RP. RP can look that GUID up after the fact and examine the characteristics of the authenticator.

Almost any authenticator is going to be wayyyyy better than a password.

Right now almost all of the browsers support web authentication. Chrome, Edge, beta Safari, Firefox is looking for support to finish development. iOS is furthest behind. Apple won't say when they are going to release it on iOS. Brave on iOS supports it right now.

Apple would probably support TPM as webauthn platform backing store via their existing keychain functionality.

Duo has proposed a UDP transport. Pair your authenticator app on your phone with your browser.

CTAP2 transports are defined by FIDO, javascript API defined by W3C.

RP can add username, settable field to the credential which will be returned as part of the authn response. Field size for the settable field is 1K.

RP name and icon are sent, displayed in the browser when the user is asked to select a credential.

Discussion of how to do account recovery- backup authenticator, use of additional key material from the backup authenticator using EC stuff, etc.

A Guide To Hyperledger Aries-Cloudagent-Python Architecture & Implementation

Tuesday 4C
Convener: Andrew Whitehead (BC Gov)
Notes-taker(s): Andrew Whitehead

Tags for the session - technology discussed/ideas considered:
hyperledger, aries, python, verifiable-credentials, introduction

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

Slides from Session:
https://docs.google.com/presentation/d/1K7qiQkVi4n-lpJ3nUZY27OniUEM0c8HAIk4imCWCx5Q/edit?usp=sharing

Project link: https://github.com/hyperledger/aries-cloudagent-python

Cors on OAuth Token Endpoint Not A BCP

Tuesday 4D
Convener(s): Travis Spencer, Curity
Notes-taker(s): Travis Spencer

Tags for the session - technology discussed/ideas considered: oauth, bcp, spa

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

The Best Common Practice (BCP) for use of OAuth with Single-page Applications (SPA) is being discussed and put forward as a formalrecommendation. The use of the implicit flow is being discouraged, and, in its place, the use of the code flow with a public client that uses Proof Key for Code Exchange (PKCE) is being set forth. This BCP is inline with the same advice given for public, mobile clients. However, there are some issues with this that were discussed:

1. The token endpoint is really many endpoints, meaning it has a lot of complex logic and handling in it to deal with the tunneling of different requests types.

2. This complexity is exacerbated by the fact that many clients with many different client authentication methods access this endpoint.

3. If CORS support is added to this, the logic of the token endpoint will be very hard to maintain, and easy to get wrong. How can this be a BCP? The concern is that incorrect issuance of tokens will often be done with SPAs which are public.

4. Because the code flow uses two endpoints, there is the possibility of token endpoint mixup attacks which the implicit flow (or a new protocol like the assisted token flow) do not suffer from.

These issues were perceived as problems that made the use of the code flow with public SPA not something that should be considered a BCP.

This was discussed and decided not be a problem because:

1. The logic and switching to handle various message exchange patterns at the token endpoint will never go away. This isn't a reason to add more and make the logic more complex, but it is not exacerbated by the use of code flow with SPAs because the interaction with public clients already exists if mobile, public clients are supported.

2. CORS does not need to be used; it should be effectively switched off by always returned "*" for the Access-Control-Allowed-Origin response header. The reason being that other public clients, like mobile ones, don't sent an Origin header, so it isn't changing the security posture of the AS/OP. The Origin header can also be stripped off by a back-end of the SPA's making it a non-CORS request even though the client is still public. So, the browser's effort to provide additional security is not adding anything, even an extra defense in depth. So, strangely as it may sound, the BCP is actually to make the browser's use of CORS not applicable.

3. The SPA is actually not making unauthenticated calls to the token endpoint. It is being authenticated using the PKCE verifier. If some other application were to make the same request, it would need the proof key which the SPA would have to provide it. If the SPA, however, keeps the proof key secret, only it will be able to redeem the code. This will protect against CSRF, for example.

4. The endpoint mixup is a low risk because the call to the token endpoint doesn't happen as a result of a redirect. Instead, it's based on configuration of the client. This is usually metadata driven, so the ways to perpetrate this attack is if the AS/OP's metadata is poisoned, the client is misconfigured, or other low-risk vectors.

For all these reasons, the code flow with PKCE for SPAs is actually OK and can can be considered a BCP.

Jobs Shop: Folks Who Are Hiring & Folks Who Are Open To Getting Hired

Tuesday 4E
Convener: Cherie Duncan
Notes-taker(s): Cherie Duncan

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

A dozen people came together. Roughly 1/2 had openings and the other half were looking for opportunities. Great discussions.

Workday Credential Schemas (NOLD)

Tuesday 4l
Convener: Gabe Cohen
Notes-taker(s): Gabe Cohen

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

Workday Credentials Schema Specification; 1.0

- Authors:
  - Bjorn Hamel bjorn.hamel@workday.com
  - Gabe Cohen gabe.cohen@workday.com
  - Joe Genereux joe.genereux@workday.com
  - Jonathan Reynolds jonathan.reynolds@workday.com
  - Rory Martin rory.martin@workday.com
- Last updated: 2019-09-27

Status

- Status: **PROPOSAL**
- Status Date: 2019-09-27

Abstract

The W3C Verifiable Credentials Data Model specifies the models used for Verifiable Credentials and Verifiable Presentations, and explains the relationships between three parties: *issuer*, *holder*, and *verifier*. A critical piece of infrastructure out of the scope of those specifications is the **Credential Schema**. This specification provides a mechanism to express a Credential Schema and the protocols for evolving the schema over time.

Contents

Standards & Compliance

The W3C Verifiable Credentials Data Model specifies the models used for Verifiable Credentials and Verifiable Presentations, and while the Workday Credentials Schema Spec attempts to align closely to the W3C model, it should **NOT** be assumed this specification is fully compliant at the time of this writing. Ultimately, we would like to be fully compliant with the W3C spec; however, due to the fact that the W3C specification is currently under active development and is subject to change, we have diverged from that model with several "forks" that are fully outlined in this and other Workday Credentialing specifications. As such, while the W3C specification is our target for compliance, at this time, *this document* should be treated as the source of truth for interoperating with the Workday Credentialing ecosystem for Credential Schemas.

Formatting

The W3C Verifiable Credentials Data Model provides its examples in the JSON Linked Data (JSON-LD) interchange format. The specification allows for other formats, such as standard JSON with JSON Schema but provides only limited examples. In the credentialSchema section, *JSON-SCHEMA-2018* validation is explicitly called out. This specification does not use JSON-LD. If it becomes evident that it would be useful to include JSON-LD or another format that decision would be made in a revisal draft at a later date.

The Workday VC data model relies heavily upon standard JSON with validation provided by JSON Schema Draft 7. The data model embeds JSON Schema documents inside a larger document that contains useful metadata about a given credential schema.

Specification

1.0 Introduction

Workday Credentialing provides a mechanism for the use of verifiable credentials in a highly scalable, secure, and verifiable way. A large part of the integrity of a verifiable credential is how to structure the credential so that all three parties (issuer, holder, verifier) may have a singular mechanism of trust into what they are using. At Workday we call that document a *Credential Schema*.

This specification provides a standardized way of creating Credential Schemas to be used in the Workday Platform, how to version them, and how to read them.

1.1 What is a Credential Schema?

The **Credential Schema** is a document that is used to guarantee the structure, and by extension the semantics, of the set of claims comprising a Verifiable Credential. A shared Credential Schema allows all parties to reference data in a known way.

A schema can be viewed from four perspectives: the author, issuer, verifier and holder.

Author: An author creates a schema as a blueprint for a verifiable credential, specifying the shape and format of the data in such a credential.

Issuer: Issuers utilize schemas to provide structure and meaning to the data they issue as verifiable credentials. By using schemas, issuers contribute to a credentialing ecosystem, and promote the use and adoption of data standards.

Verifier: A verifier requesting data needs to do so with knowledge of the available credentials shapes. Credential Schemas allow a Verifier to ask for data knowing that an issuer has issued in an understood way and that a holder's wallet can find data matching that requested.

Holder: Holders, or those who are the subject of credential issuance, can make sense of the data they own – values – by viewing it against a schema – keys. When data is requested from them by referencing a Credential Schema, this known structure allows the holder's wallet to return the data specifically requested by the verifier.

1.2 Schema Guarantees

By adhering to the specification, the following guarantees can be made about a schema:

- A schema is *versionable* and new versions can be created to evolve it over time
- A schema is publicly available for any issuer to use and any verifier, or other platform member to *read*
- A schema always guarantees the structure of a credential. The described structure can be used by the Verifier to understand what data the Holder holds. There is no requirement for the Verifier to validate sent data against the schema since this sent data may only be partial, for example in event of a proof request only requiring a single field from a credential with multiple fields defined in the schema.

1.3 Where Can I Find a Credential Schema?

Credential Schemas are created and made publicly available as immutable objects on the Workday Credentialing distributed ledger.

1.4 A Note on Versioning

Schemas are versioned in two ways, via *modelVersion* and *version* properties, both of which are expanded upon later in this document. Versioning provides benefits for schema authors, issuers, and verifiers to make sense of their data.

Authors and Issuers care about versioning to track advancements and changes over time both for formatting changes (e.g. supporting JSON Schema Draft 7 as opposed to Draft 6) as well as fields as a schema converges to its most currently usable form (e.g. adding a new required field). Holders care about versioning to know where and how their credential can be used. Similarly, Verifiers care about versioning to know which data, or model versions they should accept in their systems.

2.0 Credential Schema Definition

This section provides the json-schema definition for Credential Schema along with an example of a Credential Schema for an Email Verified Credential.

JSON Schema

Show/Hide JSON Schema

```
{
  "$schema": "http://json-schema.org/draft-07/schema#",
  "type": "object",
  "properties": {
    "type": {
      "type": "string"
    },
    "modelVersion": {
      "type": "string"
    },
    "name": {
      "type": "string"
    },
    "author": {
      "type": "string"
    },
    "authored": {
      "type": "string"
    },
    "schema": {
      "type": "object",
      "properties": {
        "$schema": {
          "type": "string"
        },
        "description": {
          "type": "string"
        },
```

```
        "name": {
          "type": "string"
        },
        "type": {
          "type": "string"
        },
        "properties": {
          "type": "object"
        },
        "required": {
          "type": "array",
          "items": [
            {
              "type": "string"
            }
          ]
        },
        "additionalProperties": {
          "type": "boolean"
        }
      },
      "required": [
        "$schema",
        "description",
        "type",
        "properties",
        "required",
        "additionalProperties"
      ]
    },
    "proof": {
      "type": "object",
      "properties": {
        "created": {
          "type": "string"
        },
        "creator": {
          "type": "string"
        },
        "nonce": {
          "type": "string"
        },
        "signatureValue": {
          "type": "string"
```

```
        },
        "type": {
          "type": "string"
        }
      },
      "required": [
        "created",
        "creator",
        "nonce",
        "signatureValue",
        "type"
      ]
    }
  },
  "required": [
    "type",
    "modelVersion",
    "name",
    "author",
    "authored",
    "schema",
    "proof"
  ]
}
```

Example

```
{
  "type": "https://credentials.workday.com/docs/credential-schema.json",
  "modelVersion": "1.0",
  "id": "did:work:MDP8AsFhHzhwUvGNuYkX7T;id=06e126d1-fa44-4882-a243-
1e326fbe21db;version=1.0",
  "name": "EmailCredentialSchema",
  "author": "did:work:MDP8AsFhHzhwUvGNuYkX7T",
  "authored": "2018-01-01T00:00:00+00:00",
  "schema": {
    "$schema": "http://json-schema.org/draft-07/schema#",
    "description": "Email",
    "type": "object",
    "properties": {
      "emailAddress": {
        "type": "string",
        "format": "email"
```

```
      }
    },
    "required": ["emailAddress"],
    "additionalProperties": false
  },
  "proof": {
      "created": "2019-09-27T06:26:11Z",
      "creator": "did:work:MDP8AsFhHzhwUvGNuYkX7T#key-1",
      "nonce": "0efba23d-2987-4441-998e-23a9d9af79f0",
      "signatureValue":
"2A7ZF9f9TWMdtgn57Y6dP6RQGs52xg2QdjUESZUuf4J9BUnwwWFNL8vFshQAEQF6ZFBXjYLYNU4hzX
NKc3R6y6re",
      "type": "Ed25519VerificationKey2018"
  }
}
```

2.1 Type

It is important in software systems for machines to be able to understand the context of what a document is. In credential schemas this is declared in the **type** field. This field resolves to a JSON schema with details about the **schema metadata** that applies to the given schema.

2.2 Model Version

After a machine has parsed the type property it should know that the document it is reading is a credential schema. The next field is the version, which simply denotes what version of the **schema metadata** this is.

2.3 ID

A globally unique identifier to locate the schema on the Workday distributed ledger. Each credential schema has its own unique identifier, and each version of a credential schema is required to have its own unique identifier.

This identifier is a method-specific DID parameter name based upon the author of the schema. For example, if the author had a did like did:work:abcdefghi a possible schema ID the author created would have an identifier such as: <italics>did:work:abcdefghi;schema=17de181feb67447da4e78259d92d0240;version=1.0 </italics>

2.4 Schema Version

Schema versioning is defined as **MODEL.REVISION** where **MODEL** is a breaking change and **REVISION** is non-breaking. The version is contained within the schema identifier.

With schemas we are concerned with a new schema and backwards compatibility of existing data on an older schema.

MODEL Updating this number tells the end user that this version breaks the schema for ANY interaction with an

older schema. For verification if a holder presents a credential built from a schema of version 1.0 and the platform is only looking for > 2.0, it is not able to parse ANY information.

REVISION Updating this number tells the end user that this version may prevent interactions with parts of the schema. For verification if a holder presents a credential built from a schema of version 1.0 and the platform is looking for > 1.5, there are likely to be SOME fields that are incompatible with the expected credential.

REVISION

The addition or removal of an **optional** field is what would typically constitute a **REVISION**. Removing or adding an optional field does not break historical data in a schema and in the claims exchange protocol fields that are returned negative in the optional field can be ignored as they are optional by default.

```
{ "type": "https://credentials.workday.com/docs/credential-schema.json",
"modelVersion": "1.0", "id": "did:work:MDP8AsFhHzhwUvGNuYkX7T;id=06e126d1-fa44-
4882-a243-1e326fbe21db;version=1.0", "name": "EmailCredentialSchema", "author":
"did:work:MDP8AsFhHzhwUvGNuYkX7T", "authored": "2018-01-01T00:00:00+00:00",
"schema": {

  "$schema": "http://json-schema.org/draft-07/schema#",
  "description": "Email",
  "type": "object",
  "properties": {
     "emailAddress": {
     "type": "string",
     "format": "email"
    }
  },
  "required": ["emailAddress"],
  "additionalProperties": false

} }
```

In this example we once again reference the email schema, but this time we add an optional field backupEmailAddress. Notice how this would not break the claims exchange because the field is optional.

```
{ "type": "https://credentials.workday.com/docs/credential-schema.json",
"modelVersion": "1.0", "id": "did:work:MDP8AsFhHzhwUvGNuYkX7T;id=06e126d1-fa44-
4882-a243-1e326fbe21db;version=1.1", "name": "EmailCredentialSchema", "author":
"did:work:abc123", "authored": "2018-01-01T00:00:00+00:00", "schema": {

  "$schema": "http://json-schema.org/draft-07/schema#",
  "description": "Email",
  "type": "object",
  "properties": {
    "emailAddress": {
```

```
      "type": "string",
      "format": "email"
    },
    "backupEmailAddress": {
      "type": "string",
      "format": "email"
    }
  },
  "required": ["emailAddress"],
  "additionalProperties": false
```

},

MODEL

When a schema breaks historical data we call it a model change. This is the major differentiating point between other schema versioning protocols which allow for some breaking changes because as we learned in the problem section, even breaking one area can lead to very difficult issues for verifiers through the credential exchange protocol. The most common case of a MODEL change is the addition or subtraction of a required field. It is also important to note that for the change of a key name on a required field constitutes a MODEL change. Why? Because technically that introduces a breaking change and adds a required field.

An example of this rule is when the additionalProperties field's value changes. Changing additionalProperties from false to true **OR** from true to false constitutes a breaking change, necessitating a **MODEL** increment.

```
{ "type": "https://credentials.workday.com/docs/credential-schema.json",
"modelVersion": "1.0", "id": "did:work:MDP8AsFhHzhwUvGNuYkX7T;id=06e126d1-fa44-
4882-a243-1e326fbe21db;version=1.1", "name": "EmailCredentialSchema", "author":
"did:work:MDP8AsFhHzhwUvGNuYkX7T", "authored": "2018-01-01T00:00:00+00:00",
"schema": {
```

```
  "$schema": "http://json-schema.org/draft-07/schema#",
  "description": "Email",
  "type": "object",
  "properties": {
    "emailAddress": {
      "type": "string",
      "format": "email"
    },
    "backupEmailAddress": {
      "type": "string",
      "format": "email"
    }
  },
  "required": ["emailAddress"],
  "additionalProperties": false
```

```
},
```

This time our credentialing requirements for email have changed and email address is no longer enough information on a credential, and we need to attach a name for verification as well to our schema. This is a required field, so we know it is a **MODEL** change.

```
{ "type": "https://credentials.workday.com/docs/credential-schema.json",
"modelVersion": "1.0", "id": "did:work:MDP8AsFhHzhwUvGNuYkX7T;id=06e126d1-fa44-
4882-a243-1e326fbe21db;version=2.0", "name": "EmailCredentialSchema", "author":
"did:work:MDP8AsFhHzhwUvGNuYkX7T", "authored": "2018-01-01T00:00:00+00:00",
"schema": {
```

```
  "$schema": "http://json-schema.org/draft-07/schema#",
  "description": "Email",
  "type": "object",
  "properties": {
   "emailAddress": {
     "type": "string",
     "format": "email"
   },
   "firstName": {
     "type": "string"
   },
   "backupEmailAddress": {
     "type": "string",
     "format": "email"
   }
  },
  "required": ["emailAddress", "firstName"],
  "additionalProperties": false
```

```
},
```

2.5 Name

A human-readable name for the schema.

2.6 Author

DID of the identity which authored the credential schema.

2.7 Authored

RFC-3339 date on which the schema was created.

2.8 Schema

This is where the Credential Schema data fields are defined

```
{ "$schema": "http://json-schema.org/draft-07/schema#", "description": "Email",
"type": "object", "properties": {

  "emailAddress": {
      "type": "string",
      "format": "email"
  }

}, "required": ["emailAddress"], "additionalProperties": false }
```

Extensibility

By introducing a modelVersion field we allow the credential schema to become extensible. Properties such as derivedFrom could be used to reference a schema that a new schema is built on top of. Similarly, platform-utility features such as searchability could be provided by adding a tags array that contains categorization and classification information for a given schema.

These are just a few examples that illustrate the flexibility of the proposed model. It can be extended to support a wide variety of use-cases and make the burden on issuance and verification simpler by facilitating the development of higher-level tooling.

Drawbacks

Within the Workday Credentialing Ecosystem, relying heavily upon JSON Schema makes the data shape for credentials consistent, and could result in an ecosystem with many similar schemas with slight changes (naming, capitalization). Without proper oversight or authoritative schemas to limit duplication or misuse utilization of JSON Schema could result in a poor user experience. At the platform level tooling can be provided to minimize confusion and promote reuse.

Within the broader Credentialing Ecosystem, interoperability could be more difficult if the wider community adopts a standard such as JSON-LD and does not promote or support the usage of JSON Schema based schemas or credentials. This issue can mainly be side-stepped with the metadata we include – the Credential Schema — since our model is flexible to change. A new modelVersion could be introduced that supports JSON-LD and removes support for JSON Schema. A drawback here is the requirement that all schemas have this piece of metadata, which itself is versioned and evolvable.

A flip side to drawbacks of the usage of JSON Schema is that there is a plethora of documentation, libraries, and usage of JSON Schema across programming languages and the web.

Alternatives

JSON-LD schemas is the most prominent alternative.

Prior Art

- The Verifiable Credential Specification is valuable for providing initial context.
- Hyperledger Indy uses schemas in a similar way to the description in this document.

Security & Privacy Considerations

Privacy & security considerations mainly revolve around Personally Identifiable Information (PII) leaks in schemas.

Any field which a user could enter data is a potential area for personally identifiable information. When implementing systems that support the storage and querying of schemas relevant data privacy laws and regulations must be taken into account.

Interoperability Considerations

The primary concern of this specification is to facilitate an ecosystem in which Verifiable Credentials can be issued and utilized. In order to be interoperable, additional schema types may need to be supported. Given the investment into a robust versioning strategy of our **Credential Schema Metadata** interoperability with the current design is less of a concern.

A goal of publishing this document is to promote others to adopt our schema philosophy. It also opens the door for providing feedback and collaborative contribution to developing primitives that would result in a successful verifiable ecosystem.

Glossary

Schema Metadata: Top level information about a credential schema. An example for an email credential schema is provided below.

```
{
  "type": "https://credentials.workday.com/docs/credential-schema.json",
  "modelVersion": "1.0",
  "id": "did:work:MDP8AsFhHzhwUvGNuYkX7T;id=06e126d1-fa44-4882-a243-
1e326fbe21db;version=1.0",
  "name": "Email",
  "author": "did:work:MDP8AsFhHzhwUvGNuYkX7T",
  "authored": "2018-01-01T00:00:00+00:00"
}
```

Credential Schema: The data template for a credential. An example of an email credential schema is provided below.

```
{
  "$schema": "http://json-schema.org/draft-07/schema#",
  "description": "Email",
  "type": "object",
  "properties": {
    "emailAddress": {
      "type": "string",
      "format": "email"
    }
  },
  "required": ["emailAddress"],
  "additionalProperties": false
```

}

References

- Verifiable Credential Specification
- DID Specification
- JSON Schema
- JSON-LD
- RFC-3339
- Hyperledger Indy Schemas

Keri 1: Universal DKMI Roots of Trust Decentralized Systems Primitives

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

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

Link to Slides from Presentation:
https://github.com/SmithSamuelM/Papers/blob/master/presentations/KERI1_RootOfTrust_IIW_2019_B.pdf

SSI (101 Session)

Tuesday 5B
Convener(s): Heather Vescent, Karyl Fowler, Lucas Tetreault
Notes-taker(s): Heather Vescent

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

Link to PowerPoint Presentation:
https://www.slideshare.net/heathervescent/introduction-to-self-sovereign-identity-iiw-october-2019

A Protocol for Decentralization: How Many Data Brokers Will We Need?

Tuesday 5F
Convener: Adrian Gropper
Notes-taker(s): Scott Mace & Adrian Gropper

Tags for the session - technology discussed/ideas considered: Web of Trust, DIDs, OAuth

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

Background: In rebooting Web of Trust, we are trying to figure out what the protocol issues are. Some contention from other groups that want to see their particular architectural things going on. We're all friends, many have done work on the W3C data model side, time for the rubber to hit the road.

Snorre, Orie Steele, Victor, and myself, tackling what is an agent, what does it mean in our content to have decentralization or a protocol that promotes decentralization. 4 slides at http://bit.ly/SoC-IIW.

Here is my framing of the problem.

Alice or Bob's DID, edge agent, cloud agent, MVP, EDV L3 – notification…, EDV L2 – sharing with other entities…, EDV L1 – persist, enforce… per J. Zittrain

EDV – encrypted data vault.

Our group working on minimum viable protocol. EDV wanted to define the endpoints. Wrote a 10-page paper still in draft form.

L2 can reencrypt the data.

In middle is a thing that looks like IP, everyone can use it, compete for the individual's business.

My take on agent to storage protocol functionality (roughly in order of use)

Split into things that are Alice to Alice, or Alice to Bob

Where is data about me

California and Vermont have now required data brokers to register.

Questions.

Q: I really do like the way of don't invent something. New words confuse things a lot. Bot. Hub. How do you define communication without having to confuse things too much?

Orie: I'm most drawn to MVP and cloud agent and edge agent in your diagram. We have this data format agreement issue, how do I talk to agents in a consistent manner. Attempt to define a messaging standard. At encryption envelope layer, not requiring HTTP. Until we see that demonstrated in any kind of way, it will be hard to talk about inter-agent interoperability.

Adrian: I just came from the Aries talk, you would have to fork the library to make it talk to UMA. Relative to OAuth.xyz as being the protocol that wouldn't be invented from scratch to be that agent to handle both Alice to Alice and Alice to Bob, do you see a gap between IETF Oauth.xyz and this?

Justin: biggest gap, validation of key material. Say I have one instance of an SPA or mobile app, want to tie that to some distribution mechanism, a way to prefill if not entirely convey specific user information. Xyz has a space to put all of these things, but it does not have a definition of what these look like in a DID-facing world. Xyz is probably not where it should be defined. Should be in an general purpose authorization or delegation protocol. Your client shows up, says, for my client info, it's this DID, for my key info, it's this DID. As long as the auth server understands those, to have that kind of conversation.

Adrian: Is there any competitive starting point to filling these gaps other than Oauth xyz? Solve HTTP first is another discussion. Within the community as we understand it, is there anything better than Oauth xyz to focus on?

Justin: it's a project that I have started as a means to taking a look at addressing shortcomings of Oauth 2 in a consistent way. Not an extension. Not wire compatible with Oauth 2. By design. Takes a fundamentally different model. Borrows from Open ID connect and UMA. Real value, it brings these together in a way that they are consistently applied to the system. Oauth 2 can stack Uma, pixie, request objects, stack all together with twine, and it will work but it's unwieldy at best. Xyz looks at what everybody is actually doing with Oauth, strip out some legacy decisions made in 2010 that are hindering us now. First step is intent registration. Oauth 2, authorization first. Xyz, I can push in information then figure out if need to redirect the user or involve the user in any way. You end up with something different in a lot of ways. Borrows a lot of its structure from the UMA 2 protocol, which is an extension to Oauth 2 by design. Builds things in a way that when you're starting off, you might not know you're talking to Alice or Bob or Colin. As a client you'll do things the same way every time.

Orie: Issue ID tokens?

Justin: ID assertions alongside access tokens. It's HTTP. Not going to call it RESTful because it's not. It's a multitransactional HTTP protocol.

Adrian: I see this as inevitable. But will raise the stakes. What do we mean by decentralization? We know Oauth works. Will be gaps filled somewhere else. My realization is that in order to have a protocol for decentralization, protocol must handle Alice to Alice and Alice to Bob seamlessly. To some people, it's a capabilities-based access protocol, not an identity-based protocol. That builds in the delegation benefits. Now where the money is, I want to ask about the incentives for actually making this happen for introducing this relatively simple Alice to Alice and Alice to Bob protocol. The landscape, in healthcare and elsewhere, lot of attention being paid by hosts (Microsoft, etc.) coming to me and asking how do we create a good-guy data broker. Their term, not mine. The Equifax session asked the same thing. The question at hand, in this community, where we're all vendors, a data broker or a service provider (who doesn't need to do aggregation to be successful)…like nebula genomics, does sequencing anonymously. We are not by definition going to aggregate your data. Won't go to DMV or Facebook to mix that in. People sign up, Apple with Healthkit, aggregation happens somewhere else. Data brokers depend on aggregation. Not necessarily doing any value-added service. They're subject to the data control of oauth xyz. Data brokers want to add ML, worth a lot more. The problem for our community is explaining the good-guy data broker. As long as they're wiling to resell data, that's their business model. They have another characteristic. They promote something called decentralized governance. That means the governance of data brokerage looks like Apple app store or the Android Play store. The governance behind those is centralized, maybe in next generation, Salesforce, Google building database of consent management to announce in October. Will have a lot more data brokers trying to introduce consent management. Who decides who decides, in surveillance capitalism

sense. We have to have this idea of bundles of policies represented by these communities. Otherwise a race to centralize data in as few places as possible.

Orie: Need a cattle prod to force aggregators not to amass large data sets. Vermont and California hidden data broker laws.

Adrian: DIDs are just the beginning, but I don't see any alternative. How many data brokers are we going to have? My answer is there have to be thousands of them, as many as we have communities, the way our doctors and lawyers compete for the individual's business. People are asking, how do we label apps and services. Setting a low bar that say these people are not evil is not enough. What can Kantara do?

Colin: My sense is we will play a part, standardize something. It's taking the basis of UMA and Open ID Connect, proactively, something the IETF asks to take on board, take charge of that part of the project.

Scott Mace: Rough consensus and running code is their mantra.

Colin: Yes.

Adrian: A more difficult question. Room for something Kantara already does on the money making side. You call it conformance, I call it the registry role in the good guy data broker definition. I envision a handful of orgs like patient privacy rights willing to standardize the nutrition label for this concept. Karin Alliance. I'm asking we have a separation of concerns between the people who define the label and the people who run the registries.

Colin: We could happily do that.

Adrian: Are you powerful enough to convene the good-guy data broker conversation at Kantara>

Colin: Probably not at this time. But things could change that. Mobile guys are asking us to play a similar role. We have a U.S. state asking us to help with their privacy extension. It doesn't take many things to line up to have the political strength to do this.

Adrian: Karin is closed, DIF and Hyperledger can't do it. We need an open forum.

Colin: Many are vendor-play organizations. Kantara is not that. Liberty Alliance prompted a open response. Kantara uses the monetized side of its business to run the free side.

DIDs for Everyday People

Tuesday 5H
Convener(s): Bruce Conrad
Notes-taker(s): Bruce Conrad

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

I presented 3 ways in which everyday people might be exposed to and/or use DIDs.

First, for a high school 50th reunion a year ago, I prepared one pico for each student pictured in the yearbook. When the name is selected on the home page, the yearbook picture is displayed. Each student

for whom I could obtain an email address was sent a DID for their pico. They were invited to copy it and paste it into a certain place in order to identify themselves and then were asked to write a brief bio. About 15 of about 80 graduates did this. No one complained about the unusual look of their DID. A few protested that they were not technical and would not be able to do it. Most did not elect to participate.

Second, I used the page "did.html" which is included in every installation of the pico-engine, to show how a DID resolution scheme might work from within a browser. To see this page, install a pico engine using the command "npm install -g pico-engine" and then run it using the command "pico-engine" (in both cases without the quotes). Then visit this page by entering "localhost:8080/did.html" in a browser. The page describes how to configure your browser to use "web+did" as a protocol handler.

Third, using a Sovrin agent to handle the DID (and its public/private key pair) without showing it to the person. Using an agent running in the browser tab, we showed how Alice had a page of links to websites with which she had an established connection. A single click opens that website with Alice recognized (what we used to call "logged in"). We discussed how the connection would be established in a trusted environment in which Alice is invited, by a person she knows, to use a Sovrin agent app, on her phone, say, to make the connection.

More information can be found at http://picolabs.io and the code repository is at https://github.com/Picolab/pico-engine where you can find instructions for cloning and contributing. The simpler installation mentioned above is described at https://github.com/Picolab/pico-engine/tree/master/packages/pico-engine . Once you have picos, you can make them into agents following the instructions at https://github.com/Picolab/G2S . Running a pico agent within a browser tab can be done using software in the https://github.com/b1conrad/browser-agent repository.

Thanks to the participants for the many questions and explanations offered during the session. Phil Windley referred us to the Sovrin white paper at https://sovrin.org/library/lost-phone for what happens if Alice loses her agent. Thanks to Daniel Bluhm for explanations offered during the session.

For more information, please contact the author at bruce_conrad@byu.edu

Secured Data Storage (The Hub Hubbub)

Tuesday 5J
Convener(s): Jack Ramey @Workday, Daniel Buchner @Microsoft, Danny Strockis @Microsoft
Notes-taker(s): Jack Ramey

Tags for the session - technology discussed/ideas considered:

Secure Data Storage, Identity Hubs, Encrypted Data Vaults

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

Discussed the need for a secure storage mechanism for Decentralized Identities.
Conducted a survey of what is currently being built by which parties. MSFT has been on hold for their ID Hub implementation. Workday is actively developing an Identity Hub solution. Lifescope.io has developed a system for storage but has been hesitant to propose their design as the way to do it and is very interested in building a spec with the community. Digital Bazaar is very interested in participating as well.

Decided to hold a second session to clarify what were some minimum requirements we could come up with for an MVP.

Link to Identity Hub explainer which was shown during the presentation: https://github.com/decentralized-identity/identity-hub/blob/master/explainer.md

Organizational Wallet?

Tuesday 5L
Convener: Chris Buchanan, MITRE
Notes-taker(s): Chris Buchanan, MITRE

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

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

The consensus was that meta-wallets are too hard. Therefore, an organizational wallet must consist of a secrets manager fronted by a UI. The question then became how to manage roles. One method would be to issue various micro-credentials that would, in combination, give the user their role. Another option is to use role tokens that are associated with a user credential in some backend database.

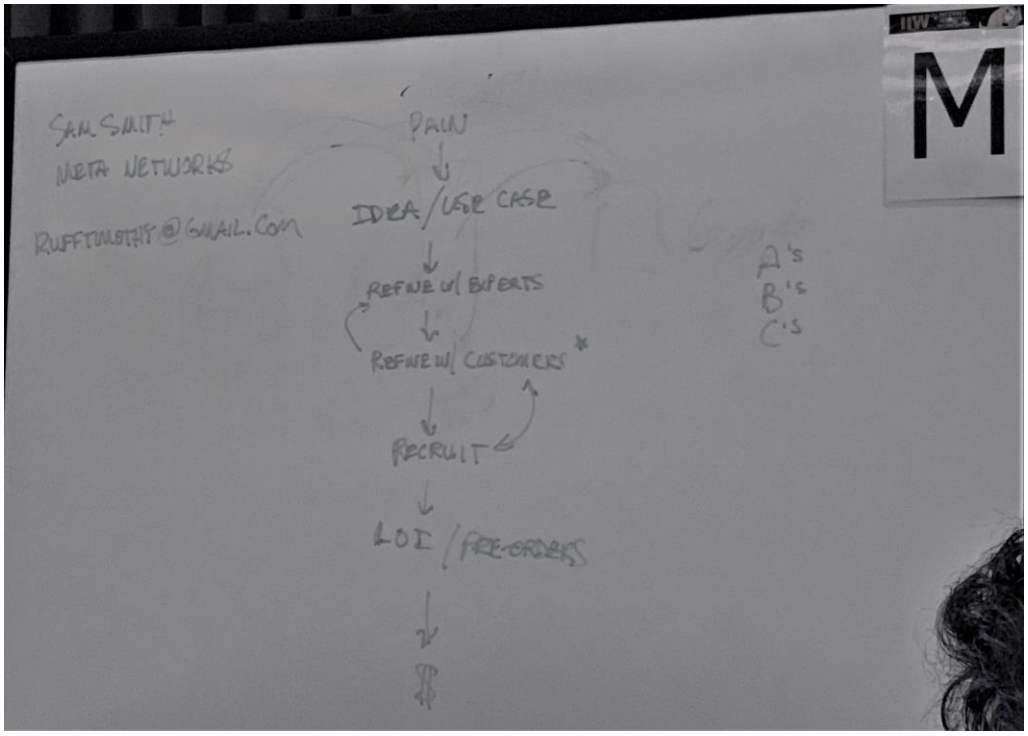
There may be more options and so a followup was suggested regarding OCAP.

Learn Startup For SSI: How To Turn Your SSI Idea Into A Viable Business

Tuesday 5M
Convener: Timothy Ruff
Notes-taker(s): Randy Warshaw

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

- Build value incrementally; minimize early costs
    - Start with compelling story that projects a visionary future state that is better and credible:
        - Everyone is going to have a digital wallet. These can be shared directly, immediately and privately with others
        - Direct, peer-to-peer relationships will become the norm for secure digital exchange: credentials, money, data
        - No more usernames/passwords
        - This is the way the world is going to work
        - Big players are getting behind this now (Mastercard, Microsoft, IBM…)
        - Most of the world doesn't know this yet
    - Use your story to attract experts you can speak with. Get them engaged. Get them to make your story/vision better: how this can be done for different use cases, in different verticals
        - The better the experts, the better the feedback, the more the story improves
    - Talk with prospective customers. Tell them your story. Refine your story. Talk to experts more. Talk to prospects more.
    - When you've refined your story to the point that prospects say they'd pay for it if you could give it to them, get the people you need to build just that.
    - Make a plan to build; go back to prospects and seek confirmation of their willingness to buy. Get Letters of Intent. Even better, get Pre-Orders.
    - Raise needed money to build/grow based on above:
        - expert advice and design
        - customer commitment
        - a highly qualified team that can deliver a focused and needed solution
    - Explored above investment options from Angels, Strategic Investors, and Institutional investors


SAM SMITH
META NETWORKS
RUFFTIMOTHY@GMAIL.COM
PAIN
IDEA / USE CASE
REFINE W/ EXPERTS
REFINE W/ CUSTOMERS *
RECRUIT
LOI / PRE-ORDERS
A's
B's
C's
M

Notes for Wednesday / Sessions 6 - 10

Verifiable Credential Based Authentication Over OpenID Connect

Wednesday 6A
Convener(s): Tobias Looker
Notes-taker(s): Tobias Looker

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

Recording of the session – https://youtu.be/4xneTHIzPhY
Medium article – https://medium.com/mattr-global/verifiable-credential-based-authentication-via-openid-connect-cd2943b17aa4

At MATTR, we've been working hard on an exciting opportunity with the Government of British Columbia (BC Gov) in Canada. In June 2019, the BC Gov Verifiable Organizations Network team put out a "Code With Us" development bounty to integrate KeyCloak, their enterprise Identity and Access Management (IAM) solution, with an emerging W3C standard called Verifiable Credentials. This work led the team at MATTR to a solution that enables the use of Verifiable Credentials (VC) as a means of authentication that is interoperable with the OpenID Connect (OIDC) specification. We call this work VC-AuthN-OIDC, the output is an adaptor which bridges these standards and enables a whole new set of capabilities through a simple extension of most modern IAM solutions.

MATTR – https://mattr.global

BC Gov Verifiable Organizations Network – https://vonx.io
BCDevExchange – https://bcdevexchange.org
"Code With Us" development bounty – https://www.bcdevexchange.org/opportunities/cwu/opp-create-a-red-hat-keycloak-identity-provider--idp--capable-of-processing-verifiable-credentials-using-decentralized-identity-technology-created-by-bc-gov-to-authorize-access-to-a-bc-government-digital-service-
VC-AuthN-OIDC Github Repository – https://github.com/mattrglobal/vc-authn-oidc

A presentation on an approach to integrate verifiable credentials as a means of authentication with OpenID connect.

Link to Slides Presented:
https://drive.google.com/open?id=1caejLpUgDWYfH--HWnY9zp7BYq5e9nKi

We did a recording of one of the sessions and have uploaded it on youtube, and would like to have the wiki updated to include the youtube link and a brief description
please: https://iiw.idcommons.net/Verifiable_Credential_Based_Authentication_over_OpenID_Connect

Decentralized UX: Designing Around Decentralized Identities (DDI)

Wednesday 6C
Convener(s): Bongani Mbigi & Jace Hensley
Notes-taker(s): Bongani Mbigi & Sarah Allen

Tags for the session - technology discussed/ideas considered:
UX, UI, Decentralized, Decentralized Identity, DID

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

Notes from Bongani Mbigi:

Slides:
https://docs.google.com/presentation/d/11TuRRLsjISNfU9Kd97Uurxi1K5V80uCz8rRpe2n_850/edit?usp=sharing

POWER OF DECENTRALIZED IDs (DID):

Decentralized Identities(DIDs): DIDs are fully under the control of the DID subject, independent from any centralized registry, identity provider, or certificate authority.People and businesses can store their own identity data on their own devices, and provide it efficiently to those who need to validate it, without relying on a central repository of identity data.

MOST USERS DON'T CARE ABOUT UNDERLYING TECH:

Unfortunately despite all these advance features for the primary user these advanced security features rarely the focus of most users job. Your average user isn't concerned about what D.I.D. method is being used but rather does this complete the task that is essential to my job. We don't develop for the sake of software development. We develop with use cases and users in mind. User don't care about DID addresses but care whether or not that the representative from a federal agency has verified their certifications.

BASICALLY THEY DON'T CARE ABOUT THE INTERESTING ST:**

We as specialists in this field have a vested interest in the finer details, that don't necessarily interest the greater population.

USERS WANT SIMPLICITY

The Goal of every frontend developer should be improving the user experience. And for decentralized identities we have major pain points around onboarding, recovery, and discovery. Onboarding deals with how quickly can a user sign up and be able to utilize their identity. Decentralized IDs have the difficulty around the fact that did address are not easily human readable. It's not something that people would memorize. This leads into discovery. Discovery deals with how quickly can the find and interact with other identities and utilizes their identity with in other systems. Because did's are not easily readable it is inherently harder to share with other systems and users. And Recovery is how easily a user can access their account when they lose their ability to authenticate. This is very difficult for DIDs. You may have lost passphrase or comprize your mnomic or private keys which renders your newly created identity out of your control. This jeopardizes not just your identity but verified credentials that are associated with that identity. This creates friction for users of DID and it not what users want or

need. Users' perception of a technology is based on the ease of use. Users want something that is as easy if not easier than what they are currently using. They Want they same speed of onboarding, and painless discovery and integration, and easy recovery when things go awry,

ABSTRACT AWAY UNNECESSARY DETAILS

It's important to abstract away what is not necessary for users to complete their jobs. For enterprise users, a good apps reduce friction and allows then to be more productive. For decentralized identity that means abstracting away unnecessary details. Remember every job has their own jargon and terminology, and adding our own jargon to their flow only complicates their jobs. We interact with names like Bongani M. from Transmute not did:eth:1234... . As we develop applications and refined the DID spec, we need to refine processes to resolve DIDs to something meaningful to our users.

We cannot ignore that when dealing with UX around Identities that there existing flows that users are accustomed to. It is necessary to utilize that. Skeuomorphism is something that helps bridge new technologies with existing systems and flows. When we can ground DIDS with existing experiences in helps users accept it as an evolution of what they see as their digital identity rather than change they would push back.

A general rule of thumb is make it so easy that <INSERT_SENIOR_FAMILY_MEMBER> can use it. Because for me, my mum would rather see Bongani @ Transmute rather than did:eth:1234. Process like Seeing TxHash 0x12bb123tfd… mean far LESS than Your "Bachelors_Degree.pdf" Verified By University of Texas at Austin.

FAQ

- ***HOW DO WE DO KEY RECOVERY?***
    - Remember familiarity is key, we have existing methods like the secure enclave where we can safely back up their keys. You can also utilize the concept of an agent, i.e. working on behalf of your user, and hold their keys and manage it like traditional methods. Another method is to encrypt it using a paraphrase in which they can unlock their key. Another way is to revoke the lost / compromised key and have a back up.**CYUA** (Cover Your **User's** A**)
- ***WHAT ABOUT POWER USERS?***
    - This largely depends on your audience. For B2C this many not be an issue, for enterprise users you will need to be able to expose a power user mode for admin, in which they can see underlying ethereum transactions for auditing, etc. It is important to note Majority of users DO NOT need to or care to know this. So this should be on an opt in or need to know basis.
- ***HOW WILL THEY UNDERSTAND PRIVATE PUBLIC KEYS?***
    - Largely depended on personal opinion. We believe that for most users we should abstract this for day to day uses. However It should be easy to find and see them. It is recommended to look for concepts in skeuomorphism: Find a way to related private/public keys to relatable things. Recommended: pub/private -> hand signatures && OAuth flow or literal keys
- ***LATENCY, LATENCY, LATENCY, BRUH***
    - If it's not the user's responsibility, then don't make it theirs. Hide it away in queues and resolve it on the backend
- ***REVOCATION?***

FURTHER READING:

https://medium.com/alpineintel/on-abstraction-and-risk-e981e06830f3

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

Notes from Sarah Allen:

Identity UX

Zuko's triangle

- Human memorable
- Globally unique
- Cryptographically security

Pet name systems

Bloom - human side

- Initially Web app, meta mask based, but people found that difficult to use
- Created mobile app, which is a mobile wallet, but we don't tell the users, they don't care that it Is etherium-based

Meta Mask — Etherium wallet chrome extension — need seed phrase, lots of friction

Bloom app is an agent that is who they are

- Hide the details

Don't have to wait for a transaction
— verifiable credentials can happen entirely offline

Transmute -
Agent is a useful concept, the agent does things on behalf of the user

B2B apps have clear authority (the company),

- employees are comfortable delegating to the company
- Also people must do whatever the company says to do (everyone uses the same tech)
-

Use KeyChain on OSX, iPhone, Android also has a key store

When an DID is created, it's kind of like an infant, it has no powers yet

Looking at verifiable credentials as capabilities has helped

Start with “What does the user need to be able to do?”

Key process improvements — iterate between UI designer and backend engineer

- Need to get your app in front of the user

Simple Cooperative Filesharing. (CHI Paper - on Alan Karp’s website)

- Unguessable URI
- Every policy decision has an artifact in the UI
- When you do someone does it feel like a security step or feel like regular workflow.
    - “If it feels like a security step, it’s an anti-pattern”

What are metaphors that work?

- Documents: each verifiable credential is a document
- Keys - refer to as digital signature (people understand that)

QR codes? Debate about whether this is well-known or not. Easy to learn, but can’t expect that people already know how to use it.

“Shield” — Transmute uses the term “shielded credential” who knows it has been verified.

Lifecycle management for private keys?

- Lose phone with key on it
- How do I revoke / reset?

Backup private key to cloud, can move phones

Use agent, which can revoke compromised key

Enterprise can have key escrow (company has copy of your key)

"Trust in Numbers" Ethical (& Practical) Approach to Identity-Driven AI/Machine Learning

Wednesday 6F
Convener: Mike Kiser
Notes-taker(s): Matt Domsch

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

Attendees:
Asad Ali
Adrian Gropper
Dick Hardt
Wendell Baker
Matt Domsch (notes)
4 others

**** Slides and academic paper available late November after conference publication
Conference link: https://digitaleweltmagazin.de/digicon/program/

Standards aspects
- Well-being - defining your ethical stance. Online Ethics Canvas. Who might you harm and how?
- Accountability - to whom? We often cede accountability and control to technology. "Because the algorithm said so" isn't enough. Users must also hold you accountable.
- Transparency - Users must be able to see how you got to your answer. Explain the "why".
- Fairness - Bias and things you assume.
- User Data Rights - best current practice

Wendell: Similar to Ethical OS? and many others? John Rolls.
Adrian: like privacy policies? There are so many to choose from.
Wendell: If you'd go before an Institutional Review Board(IRB), this qualifies.

Determine the relative strength or weaknesses of an approach, compared to other algorithms, and compared to your own position over time.

Wendell: fairness can't be expressed as a fixed point.

Adrian: will run a session on ML in medicine later today. None of this applies, because Medicine is science, nothing in secret.
The problem is we're turning it into a trade secret and business model, with ethics whitewashing afterwards.

Wendell: this is a way to pierce the trade secret system.
Adrian: but that's not the way open science should work. You've already ceded the ground. We're pre-judging the outcome of how money is made vs how science is done.

Wendell: how is this related to other ethical sourcing: blood diamonds, oil money, coffee, ...

Mike: is there another measurement method?
Adrian: Efficiency? Are we reducing friction only to have to control for bias?
Wendell: IRBs serve as a "confessional effect".
Wendell: is this like Mayak's trancendental effect, beyond human comprehension? Formal systems theory from MIT in the 1970s.

This is pretty subjective. Can we build a more objective measuring stick for each of these dimensions? Similar to the Me2B Harms discussion yesterday.

Adrian: similar to introducing apps into an industry. 2 models:
1. mininmum bar, do no evil, gives maximum flexibilty to any business.
2. Consumer Reports style of strictly objective criteria
Ethics is neither a race the bottom, nor is it objective through standards and independent entities.

Institute for the Future Ethical OS.
Kantara is one of 3 FISMA certifiers.

Wendell: there are other maturity frameworks that this is similar to this work.
Design thinking 5 levels.
Adrian: Twitter #darkpatterns

Identity Standards: The SOAP OPERA Catch Up On Previous Episodes & Review Major Plot Points

Wednesday 6H
Convener: Pamela Dingle
Notes-taker(s): Heather Vescent & Scott Mace

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

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

Notes from Heather Vescent:

0. Kerberos
    a. Mid-90s
    b. Symmetric key management
    c. The only identity was the principle – the name of the account
    d. To do identity for machines, and people in labs, and with cross signing K, it started to look like federation. Large scale interfederation, as late as early 20s.
    e. Useful within a domain?
    f. You couldn't control information flow.
    g. You shared everything or nothing.
    h. Perimeter security. Lab security measurement.
    i. Lack of granular AuthZ

j. Microsoft had an embrace and extend philosophy, that caused issues. (true/false)
k. MIT implementation of K, but they were lazy and couldn't keep up (the real story/drama)
l. Where there is a natural perimeter, K still works.
m. Spinago
n. Thought you could do everything with symmetric crypto.

1. Directories – late 90s
    a. LDAP (x506)
    b. A whole bunch of machines, separately authenticated to, managing passwords.
    c. A central place to store identity information, and validate passwords
    d. Make calls to a central location.
    e. Soap opera: Novell, MS and Netscape – directory was very popular. Active Directory started working.
    f. ADSI – was alternate to LDAP
    g. There was the MS way, and LDAP
    h. Dale Olds, was a prime chief architect in ADS-LDAP
    i. Mark Wall – wrote the book
    j. Roland Hedberg – chair
    k. Federation scheme involving LDAP
    l. Every perimeter had a directory in the middle
    m. Directories are the world of LANs
    n. Extranet was popular – going out was the exception
2. Web Access Management
    a. Siteminder/Oblix
    b. Late-90s, early 00s
    c. People wanted to use LDAP, but needed enforcement of consistent access
    d. Popularize the concept of agents.
    e. Agent would sit on the web resource, and enforce/gatekeeper, if no credentials, redirected to a central service.
    f. Domain limited, encrypted cookie, authorization information, and worked with agents who would redirect
    g. LDAP isn't a good authentication method, so needed to abstract.
    h. The agent is sitting in front of the website, (not at the user try to access)
    i. Apache module or ISAP, NSAPy plug-in.
    j. Siteminder, was first offering, central administration of their websites and was very popular
    k. Oblix – Oracle
    l. This wasn't enough because of cookie based domain based way they did authorization and access management
    m. Single tenet on-tem, inside the corporate firewall.
3. Federation
    a. SAML/Liberty Alliance
    b. WS*
    c. Pam's first conference – Burton Group, MS announced project hailstorm
    d. MS was offering to authenticate everyone – people were terrified that the world would be owned by one centralized company.
    e. Saw a lot of people yelling at each other, the Liberty Alliance was formed by companies with the paradigm that no one company should run anything.

f. Liberty Alliance: Can not be owned by Microsoft. To contain the MS agenda.
g. SAML came out of Liberty Alliance. Every company wanted their own stuff.
h. Scott Canter
i. Tony Nadelin
j. Eve Maler
k. Jeff Hodges
l. These are the gas giants, they still make up the mass of the universe.
m. Sun Microsystems
n. SAML is being negociated. It's nacent. But the cloud is just starting to be a real thing.
o. They want to federate in themselves, and among their partners. Finding more new use cases.
p. Single Sign on became a buzzword with SAML
q. Identity Provider also became a buzzword
r. All big companies driving in a closed spec work.
s. A new generation of people wanting to do identity their way, and own their own identity. This was the rise of OpenID.

4. OpenID
    a. Not started as a specification, but the implementation of an idea – PHP on live journal.
    b. It fit an interesting niche in a way that SAML didn't
    c. It was all about ad-hoc identity, run your server. Johannes Ernst\Dave Reecordan
    d. We weren't good at the signing and leaking issues
    e. SAML had canonization
    f. First OPENID protocol, new redirects and could fool the system and it iterated
    g. Came up with OpenID 2.0, which worked well
    h. Mobile occurred – 2007
    i. Mobile apps that wanted to consume identity, and these clients were impersonating people to tweet for them
5. Delegated Auth2
    a. OAuth 1.0
        i. This came about as a way to delegate id to an API
    b. WRAP
    c. Kerb Constrained Delegation
    d. Web, then mobile
    e. API driven
    f. Before we didn't write website with APIs
    g. Could do openID and
6. Infocard – pre-mobile
    a. Most influential failed standard
    b. You should be able to have a wallet, and put a card in the wallet with the identities and credentials.
    c. No mobile
    d. WS* and secure, WS trust specifications
    e. First driven by MS and mostly about the browser, increasing need to make remote procedure calls, APIs, desktop and server to server. You had secure this.
    f. WS* system, based on API calls using SOAP, XML
    g. You can not tell a lie on the security of a channel.

h. Complicated system for doing crypto, message based
i. Industry participants: MS, Sun, IBM
j. This has a lot of properties we are trying to bring back today
k. This was a high complexity down payment.
l. Provided the basis of information card, which didn't live inside of a browser.
m. Ask any 5 people why it failed, you get 5 answers.
n. Biggest issue for relying parties is you were out of control.
o. Loss of control – FAPI world
p. DID Com is around message based security.
q. Pam D, Vittorio, Kim Cameron
r. Loss of control – SAML branch that figured out how to mitigate that – Trust framework. Walled garden with 10k IDPs, Governance.

7. Oauth2 + OpenID Connect
    a. Huge and growing number of specifications
    b. UMA
    c. OPEN ID foundation – founded by Don Tibeau,
    d. WRAP was next gen of OAUTH 1.0 could evolve
    e. Cloud providers wanted things to be easy for developers – secure, but easy.
    f. Enterprise folks, who wanted enterprise grade for an enterprise audience
    g. Reaction to people's experiences with SAML, OAuth 1.0, WS* - so this was the reaction to the past.
    h. One of the big players, threw down his bat and went home – it was a scandal. Eron Hammer.
    i. The inventor says its bad.
    j. But then things got smoother – oauth 2. Formalized to the identity of the client (the user and the identity of the client working on behalf of the user – the client gets its own secret/token – reintroduced symmetric crypt.
    k. People wanted to use oauth 2 for identity – but only enables a client to ask for a token to act on behalf of a user.
    l. OpenID Connect evolved to fill that. To ask for the identity of the client and use access tokens. It took browser flows, and explained how to request certified id and access token. Claim and description of the access moment.
    m. We gained a ton of stability. Season ended on a high note.
    n. Learnings: SAML was an 800 page spec, Liberty Alliance thought of every single use case, still stuff no one uses, because it was so thougrough, and very heavy. SAML is about sophisticated party talking to a sophisticated party.
    o. OAUTH2 is assymetic model, can have a sophisticated party talking to unsophisticated client, important for mobile. Eg secrets kept on mobile apps.
8. Decentralized Identity
    a. DID
    b. VC
    c. DID*
    d. Key management
    e. Canonialization
    f. What did this inherit from previous points?

g. We are writing it now. What in the history do we need to look at? What are the other pieces that we should write down here.
h. What were the security implications along the line that should be accounted for in DPKI. Looking at APTs and how they interacted with building, to force us to reinvent.
    i. Key/ Signature wrapping – this is why people are concerned by JSON-LD
    ii. Had a lot of vulns because someone did it wrong in implementation
    iii. The systems stopped working, so someone turned off signature checking, and it all worked, so feels like it's not a problem
    iv. There are tons of SAML deployments, where they turn off key. Verification or signature – we have a massive problem how to verify the signature of meta data with it turned off.
i. Nascar – 5 identity provides you accept identity assertions
j. Large number of UX/ security issues/phishing attacks
k. We figured out how to deal with crypto aspects – crypto got better/solved up to 6, but UX has left. UX from the developer perspective.
l. Pick any of the SSI demos that exist today, look at those demos from the eyes from someone who isn't familiar with technology, and see where these can be phished.
m. Multi-Card

What about FIDO?

- Could be its own chapter
- It's not identity
- Mechanism for carrying credential

What about PKI?

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

Notes from Scott Mace:

7 phases of the soap opera

Kerberos was first

1. Directories and LDAP – 1995 to present
2. Web access management
3. Federation
4. Delegated authorization
5. InfoCard
6. OAuth 2 & Open ID Connect
7. Decentralized – today's episode

Q: So this is as the identity turns, episodes 1-7

MIT vs Microsoft Kerberos alone could take up the whole time

LDAP evolved from pain around X.500

Web access management was cookie-based access management. SiteMinder put Web management in front of directory-enabled resources. Oblix.

This is totally collaborative. Don't take it as gospel.

Was also SAML Liberty Alliance timeframe. Also WS*. WS* goes all the way down to Infocard.

Delegated authorization is Oauth 1.0. Not like it just appeared and didn't exist before that.

Q: Plus WRAP

Q: They were a main character in the episode.

Constrained delegation

Q: Air gap security.

Open ID is between 3 and 4.

InfoCard is its crazy little spinoff.

Oauth 2 & Open ID Connect are huge, many spinoffs.

Decentralized – DID/VC/DID-*

Q: Map these standards under different organizations and communities.

Dramatis personae.

Q: Game of Thrones families.

Those are part of the stories. Important for new folks to understand why these efforts occurred.

Q: What did #7 inherit from 1-6?

A good point.

Q: Does FIDO fit anywhere into this?

Scott Mace: How about UMA?

Pamela put UMA under #6.

FIDO may be its own story.

Q: People still use X.509 for identity, but nobody will probably use Webauth for identity.

Q: Kerberos was identity for machines in labs and people. People were looking at large-scale integration of Kerberos realms.

Why did Kerberos not then jump domains?

Q: You couldn't control information flow with Kerberos. Very little specific detailed control. Even today you won't find many AD control points exposed to the Internet. Perimeter security. MIT Kerberos team was lazy, couldn't keep up. The Apple team, Heimdall, was able to keep up with MS.

Q: There was a lawsuit that MS lost.

Q: There are browser plug-ins that do in-house Kerberos sign-in today.

Q: The lost part of Kerberos that was interesting was HTTP authentication. Nothing ended up in #7. Kerberos thought you could do everything with symmetric crypto. Everything is key management. All hard problems in security can be reduce to hard problems in key management.

Diretories. Silos of machines everywhere. LDAP gives you a central place to store identity information but also to validate passwords. Tension between Microsoft and LDAP. Also ADSI.

Q: Windows for Workgroups in early directory land?

Q: Novell NDS was essentially X.500.

Dale Olds was here yesterday. Trying to turn X.500 into LDAP. The other one not here is Mark Wall. Roland Hedberg.

Q: There was also a federation scheme involving LDAP.

Q: There was a project with Patrick Helstrom and Leslie Dagel to build a directory of directories type federation. A way to rebuild whois.

Q: What time was this happening?

Q: Late 1990s. While mobile incumbents were being split up. Had to deal with number portability.

Q: I worked with screening service in 2000, the original multiple signon with AOL and Microsoft. It failed.

Q: Didn't have anything to do with login, necessarily.

Directories were perimeter limited. Part of the chewy center. Not an internet-grade mechanism.

Q: Directories are the worlds of LANs.

Leads to web access management. LDAP needed the enforcement that came with consistent web access. Web access management popularized this concept of agents, the most overused word in identity. Agents were gatekeepers. Without proper auth, would redirect you to a central service. It was an encrypted cookie that contained auto info, agents that redirected to the center.

Q: LDAP isn't a good authentication method.

I agree with that.

Q: The agent here is sitting in front of the web site being protected, not on the user's system.

That tended to be an Apache model, or an ISAPI plug-in. SiteMinder really set this whole thing off. Offered enterprises to centrally administer all their web sites. Oblix came on the heels. SiteMinder went to CA, Oblix to Oracle, still there. But wasn't enough due to the cookie-based and domain-based way they did authorization.

Q: Set the stage for the next stage, which was SAML.

Cloud didn't exist. This was late 1990s until early 2000s.

The federation piece. I will tell you a story. Went to BG Catalyst in 2001, MS announced Project Hailstorm. Offering to authenticate everyone. People were terrified, that the whole world would end up centralized and owned by one corporation.

Scott: Hailstorm was one of MS' responses to the Internet.

Liberty Alliance was the idea of no one company should run everything.

Q: Had to be part of the elite to sit at the table. It was to contain MS.

SAML came out of Liberty Alliance. Every company wanted their own autonomy and make its own assertions.

Q: Scott Kantor turned SAML into something that actually worked. He put in a shim and made a serious thing of it.

Tony Matlin played a role. Eve Maler. Jeff Hodges. A lot of these people are still around.

Q: In the solar system of identity, these are the gas giants.

SAML is gaining support, still nascent, but the cloud is starting to become a real thing. They don't just want to federate with their business partners, they want to federate amongst themselves. 2002-2006. People finding new use cases.

Q: When did SSO become a buzzword?

Q: SAML.

It was all big companies, a closed spec work. There was a new generation of people who wanted to do identity their way and own their own identity. The rise of Open ID. The federation stuff is pre-existing trust. But cloud providers were evolving. Folks like Twitter.

Q: Movable Type. Identity for blogs and comments. That's how I got into it.

Justin: Original Open ID was not started as a spec. It was an implementation of an idea, in PHP on LiveJournal. Use your blog to comment on someone else's blog. Fit an interesting niche in a way SAML did.

Q: It was about ad hoc identity.

All based on URLs. Assert things around your URL in your bedroom.

Q: Johannes Ernst is still here. And Dave Recordon.

Unfortunately the signing and leakage issues, SAML people had problems with canonicalization. The first Open ID protocol, could add additional query parameters to the connects. Open ID 2.0 became quite popular. However at same time this was stabilizing, OAuth 1.0 came out. Mobile occurred around here. 2007. Mobile apps were asking for people's username and password, and replaying those, a massive antipattern, massive fraud, because there was no alternative. OAuth 1.0 was a way to delegate capabilities.

Web, then mobile.

Q: But API driven is the key point. Before this we didn't build Web sites with APIs as a major thing. Couldn't do that much with them. People were building Web sites with an API that were a front end to that API.

Stuff joined Open ID and OAuth together.

Q: That was a disaster.

Information Cards, most influential failed standards effort. Have a wallet, put cards in wallet that rep the ID and attributes you own and control. This was before mobile. 2006.

Q: People couldn't convince the browser manufacturers to implement it.

Was based on WS*, WS Trust.

Vittorio: My license plate was WS*. SAML was driven by MS, mostly about the browser. Increasing needs for RPCs. No way of doing that apart from Kerberos. Based on SOAP. Very complicated system for doing crypto, doing things message based rather than transaction (?? Session ??) based. Sun and others did it. It asked everyone to put down a high down payment in terms of complexity. Huge adopting in MS but also floundered. Info Card was an active client in the OS.

I wrote a lot of open source RP code for WordPress etc. The big issue is the loss of control. Something the decentralized efforts need to take into account.

Q: A lot of DID discussion involves messaging.

Q: Loss of control thing, an entire branch of SAML figured out how to mitigate that, lives on in academic framework. Now has 10,000 IDPs. Governance is a big part of it.

Don forms the Open ID Foundation, resulted in chapter 6, a group of folks, WRAP came up as a next gen of how OAuth 1.0 could evolve. It was difficult for developers.

Vittorio: Also scenarios were restricted.

Justin: It also didn't work well on mobile applications.

The cloud providers wanted things to be easy for developers, secure but not overkill. Enterprise folks wanted that for an enterprise audience.

Justin: Ch 6 was reaction to people's experience with SAML, WS*, OAuth. We don't want to do the exact same mistakes.

Then a big player threw down his bat and went home. Big blog entry. As much of a scandal as standards have.

Justin: The inventor says it's bad. I've had to explain things so much.

[Put a link to the blog entry in the notes HERE]

Now you can separately authenticate the client.

Q: It reintroduced symmetric crypto as well.

OAuth 2 has 4 flows, 2 are back channel (no browser) 2 front. OAuth 2 enables a client to ask for a token to act on behalf of the user. A lot of things that were created in Open ID Connect are starting to become part of OAuth. ID token is claims and description of the authentication moment. A point where we gained tremendous stability.

Learnings here, cool thing about OAuth 2, SAML was an 800-page specification. Every single use case. Still things in SAML that solve problems we have today. But it was also heavy. It was a sophisticated

party talking to a sophisticated partys. OAuth 2 for the world of mobile was important, sophisticated parties could talk to unsophisticated party.

We're writing decentralized right now. Trying to figure out what in history should we be looking at?

Q: What were the security implementations we should be accounting for in DPKI? Looking at APTs and how they interact with things you're building.

Signature wrapping is a big one, comes along with canonicalization. JSON LD, vulnerabilities because somebody did it wrong.

Justin: Someone turned off signature checking and everything works. It does not break the app. There have been and still are tons of SAML deployments turn this off.

Q: Turning off signature verification.

In Open ID 2.0, people didn't trust assertions from people they didn't know. So they trust only 5 identity providers and no one else.

Q: UX issues. Leads to phishing attacks. We figured out how to deal with crypto aspects of security but the UX aspects still remain.

Vittorio: Cartesian product of things you can do now.

Q: Everybody should pick any SSI demos that exist today, city, get credential riding the bus, look at it through your grandma's eyes, figure out how many ways they can be phished.

Sovrin 101: Permissions, Codes Bases, Value TXfer, Issuing & Edge Agents

Wednesday 6I
Convener(s): Nathan George
Notes-taker(s): Nathan George

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

Link to Slides Presented by Nathan:
https://docs.google.com/presentation/d/17DOlkubSAa_oihSAQKCRnEPMSL6d6x1bxB4GG_aPr1w/edit?usp=sharing_eil&ts=5d96152e

Open Source Business Models

Wednesday 6J
Convener: Mike Schwartz
Notes-taker(s): Mike Schwartz

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

Mike gave an overview of how and when software startups that use the open source software development methodology can balance giving away software with building a successful startup.

Open Source Underdogs Podcast
https://opensourceunderdogs.com

Slides are here:
https://gluu.co/foss-slides

OAuth Pushed Authorization Request

Wednesday 7A
Convener: Torsten Lodderstedt & Nat Sakimura
Notes-taker(s): Nat Sakimura

Tags for the session - technology discussed/ideas considered: OAuth, OpenID, JAR, PAR

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

Torsten explained his presentation.
https://www.slideshare.net/TorstenLodderstedt/pushed-authorization-requests

The problem statement:

1. Authorization request integrity protection
2. Size problem.

The solution for 1. is JWT Secured Authorization Request (JAR) and 2. Is the request_uri defined in JAR. Pushed Authorization Request (PAR).

Q. How long should AS keep the request?
A. It is one time use as it contains state, nonce, pkce_challenge etc.
Q. When the authorization request must be checked?
A. When received because there are user_hint etc.

Q. What goes into the front channel?
A. Only request_uri

Q. What would be the migration path for OP?
A. Let's talk.

Advantages

- Significantly improved security
    - Request integrity
    - Client authentication
- Robustness
- While offering a simple migration path.

Q. Please add the writing on the security risks of not doing this.
A. It is not only security but the robustness problem caused by the size.

OAuth Rich Authorization Request (RAR, Formally known as structured scope)

Torsten went over the slides.
https://www.slideshare.net/TorstenLodderstedt/rich-authorization-requests

Discussions on why new parameters and not re-using the "claims" parameter came up, and a heated debate ensued. It will probably have part 2.

Delegatable Credentials: Guardians, Controllers, and Delegates with Any W3C Credential Type

Wednesday 7B
Convener(s): Daniel Hardman
Notes-taker(s): Daniel Hardman & Gregory Rocco

Tags for the session - technology discussed/ideas considered:
W3C, DIDs, Verifiable Credentials, Delegation

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

Notes from Daniel Hardman:

> **Summary:** we can implement delegatable credentials on top of any W3C-compatible credential mechanism. We just need to implement some lightweight conventions.

We reviewed this slide deck:
https://docs.google.com/presentation/d/1NzWB4gyaj43TEYUsTNL4O4-t35x-DP_ubS0YqunN5Rg/edit

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

Notes from Gregory Rocco:

Notes [bolded includes individuals other than the convener]:

- http://j.mp/2pnXqKx
- Ordinary credentials aren't easily delegatable
- Physical credentials (like a driver's license) – my kids will try to borrow particular credentials like a credit card. They can use my credential but if they get challenged, they can't assert their position.
- Verifiable Credentials – it's not impossible to delegate but there's no standard yet
    - Can we come up with a standard way to behave with VCs so delegation works right
    - This isn't ZKP specific
- One of the things to think about: in an organization (company that needs to give signing authority to three managing directors for example) – you might need delegation. If you think about it as one holistic wallet, you may arrive at an example that might work, but won't be ideal.
    - Another example isa science organization that wants to delegate pilot and maintenance privileges to other staff members
    - Parents want to delegate medical care decisions to a babysitter for a few hours
- **Isn't delegation a subset of authorization?**
    - Yes – it's the process of giving part of your authorization, and part of your responsibility
- **How do you handle consent?**
    - Definitely need to think about this in a form of delegation model
- One thing I want to bring to the table: are we doing this right
- [Confused Deputy Analogy https://en.wikipedia.org/wiki/Confused_deputy_problem]
    - Fooling someone to give you more authority than you should have
- Acid Test:
    - There's a national car rental company which has an office in Houston Texas (subsidiary), and the company buys the cars in the fleet and own them. They have a traditional credential that is a title to a car (they can prove title ownership). They want to give to the Houston office the privilege of operating that car – the privilege consists of (rental, maintenance, selling it, driving it, or delegating further).
        - **If you give me a permission with a do-not-delegate, I'm going to just have to share my credentials. Delegate is not a good permission – it's a "please don't delegate"**
        - There's an assumption with VCs where you should not be transferring them. I'm assuming that you can prevent transference of credentials.
    - Now, the credential chain delegation starts – then Alice walks into the office and wants to rent the car. Alice receives the drive and delegate credentials (less privileges) with constraints like 7-days and only in Texas. Then Alice goes to a restaurant and gets valet parking where she delegates with "drive" and more constraints.
    - Let's say the FBI calls up the Houston office and says they believe the person that drove the car last week committed a crime (nobody can drive or touch it). Houston revokes their credentials to Alice, now when the valet comes out, the car doesn't open the door because the valet doesn't have authorization
    - If we can solve that use-case, then we've solved the delegatable credential problem.
    - **What is the use case? Can we lock Alice out?**

- This is generally about any use-case (example: generation of new credentials, or demonstration of existing permissions)
- **You can have delegatable credentials and revocable delegatable credentials**
- If you want to talk about delegatable credentials that *don't* support revocation, don't have the chat here.
- **If the valet puts a scratch on the car, there's a chain of responsibility**
- Houston office is going to blame Alice.

· Standard W3C VC with special sauce
- Field name: `schema` (self-contained)
  - § Could be a well-known schema, but you have to have the credential say this is the schema of what you're about to see so we can be creative about delegation.
- Field name `delegationProof`
- Satisfies "proxy credential" conventions
  - § What do I need to say about the holder – if you say "this holder has the following biometrics," you've bound it. There are other possible ways. If we are going to say something about the holder that has received the delegated privilege, we need the name to go look for it.
  - § **Public key isn't good enough**
  - § Need to be able to describe the party that did the delegating
  - § Then there needs to be a place where you can say the holder has the following role, and here's the permission model that's associated with some roles that interact with that so you can derive what the actual authorization is.
  - § Need to be able to impose constraints (alice can only do this for x time, days, whatever)
- Field name `trustFrameworkURI`
  - § Needs to be a relationship to define the problem domain. Example – guardianship in a refugee camp – which would have rules like not letting a child leave the camp. Or "every time -this- event happens in a camp, we need to check credentials."
  - § In a car scenario, check them when they leave the lot, check them when they get back, or anything in between.
    - · Pulled over by the police.
  - § Any given problem domain will have its own framework.
  - § **How do you propagate new frameworks?**
  - § If the trust framework evolves: you can probably manage that either way – you can say trust frameworks are immutable in respect to the credential which would be safe, or you can make it a URI with no version number.
  - § **I disagree, that's very dangerous**
    - · My preference would be to lock it.
    - · Generally speaking, you don't want to change the rules.
    - · **You can also have a Malware attack**
    - · **Couple places where you can change these frameworks, but my question is: do you think the car is enforcing these things?**
      - That would be a decision that the trust framework would make
- Public key of downstream holder

· Embedded `delegationProof`
- There's a simple way that we can do delegatable credentials without fancy fields: simply Alice has a credential in her hand when she gets stopped by the police and Alice can tell them who she got it from. Police calls the office up and checks and wants an email about it.

We don't want to have to do this. The delegation proof field is a way to short circuit all of that.

- It pre-calculates for whatever point you're at, what are all the reasons to believe that this is a legitimate chain.
- The first credential is a car title which generates a presentation that proves ownership which is embedded in the first delegatable credential.
  - This then moves to the next delegatable credential.
  - **You missed the best advantage – alice can delegate without asking the car rental company.**
- **So the ownership goes downstream. Is there a possibility that each entity can add their own proofs without the upstream entity knowing about it?**
  - We're making assumptions about the problem domain. Or if you get further down the chain, you replace the trust framework.
  - **So the assumption is that corporate trusts Houston, Houston trusts corporate, but there's no way to enforce Houston from adding things on its own.**
  - Everything that Houston does has to be subsetted.
  - **So this doesn't drive control of the surrogates in the chain. Example, national doesn't want regional to maintain their cars. Regional decides they want to do that so they assert authority themselves**
  - Let's assume everything is defined at the top with all forms of meaning.
  - **Let's say regional wanted to add car-washing – new things (they can just make it up and add it in the chain)**
- [Multiple voice discussion on nuances with trust frameworks]

· Here's the point: in an ordinary credential, the reason that someone would accept this is because you trust the root issuer's reputation. There's probably a trust framework for large bodies/organizations/types. Only the top organization needs to have some form of reputation – all you care about is whether or not you can follow the lines back to the owner of the vehicle.

- **If at the end when someone is verifying it- I think what's better is different kinds of credentials, trying to remove definition issues.**
- So there's another assumption I should make explicit: automated software doesn't have to understand every nuance. Human's evaluate whether something is a valid problem. Guardianship is a human evaluated thing.
- Trust frameworks can be written with humans involved

· **I don't dispute guardianship trust frameworks, I think the thing to keep in mind is that there are all of these external mechanisms that we repeatedly appeal to those in order to understand and intemperate what those frameworks mean.**

· RFC104

Aries Toolbox: Demo & Feedback Tools to Work with Agents

Wednesday 7C
Convener(s): Sam Curren
Notes-taker(s): Sam Curren

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

I showed a demo of the Aries Toolbox alongside the Aries Cloud Agent Python, as well as an instance of Aries Static Agent Python. The demo will likely be given in the future on the Hyperledger Aries working group call.

https://github.com/telegramsam/aries-toolbox

http://www.github.com/hyperledger/aries-cloudagent-python

https://github.com/hyperledger/aries-staticagent-python

Me2B, #SSI, #VRM, #IIW, #Identity, @Cluetrain (Separation of Concerns)

Wednesday 7F
Convener: Doc Searls
Notes-taker(s): Scott Mace

Tags for the session - technology discussed/ideas considered:
Me2B, VRM, Customer Commons

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

Doc Searls history of IIW

Yesterday I was with people not aware of where different pieces come from. Especially work on VRM. To some degree this is my personal story. I come from open source and Linux, from 1994 on. Linux Journal killed in August. In Linux community involved in decision to talk about open source not just free software. Term open source prior to that was used by military community. In 1999, Cluetrain Manifesto came out. Markets are conversations. Was adopted by the marketing world. #Cluetrain tweeted on a daily basis since then. Got pulled by Andre Durand into the identity conversation. Closing keynote at Digital ID World. I give me my rant about what's wrong about DIDW. All the talk about federation, companies having sex with each other using customer data. Late 2004, ran into Kaliya at a ball game. Steve Gillmor called me up to do a podcast. I sent out a note to 12 people involved in identity conversation, included Kim Cameron, Dave Winer (who created blogging, podcasting, RSS). 2nd to last Esther Dyson, people met. Brad Fitzpatrick sells LiveJournal, gives Open ID code away. Notion: All of us independent actors, peers in the internet, but better able to engage. Devin Lafredo, wrote to the VRM list, coined the term self-sovereign identity. Should start with individuals. That sat there until others picked up and ran with it. The SSI movement came out of that and out of IIW. In 2006, I got a fellowship at the Berkman Center, started Project VRM. Mike Vizard on the

Gillmor Gang, talking in fall 2006, was all about to some degree SSI, encouraging development of tools more power to engage with the company. Vizard named it on the Gillmor Gang. VRM. Has never been more than a blog, a wiki, a list and meetings twice a year on the Monday before IIW. That's all it will ever be. Needs orgs to spin off of that. The first is Customer Commons. A knockoff to some degree of Creative Commons. Where licenses live that others can point to. Also the worldwide organization of customers. Consumers Union.

Me to B, came up independently. A much better name than VRM. Uses me, all of us call ourselves that. Better also than C2B which is a business term, abstract. You can make Me2B into a hashtag. Can use some Customer Commons work.

So much privacy violation over recent years. We have regulations that have energized companies. CRM/CX.

GDPR, we got the regulatory cart in front of the tech horse. That's on us.

Q: Survey by Axios. Asked consumers to agree/disagree. The privacy threat is a crisis and we need to force companies to change. 58% of respondents agreed with the statement. We're arriving at this place with consumer sentiment.

I agree. ClueTrain still sells in 9 languages.

I wrote a book called The Intention Economy, in 2012. We didn't have the examples. Every company is dead. People working on them are still in the room.

Q: In the book you talked about meeting with Target. Trader Joe's. What is their perspective on VRM.

Jose Alvarez who had been the CEO of Stop and Stop / Giant Stores, he was the guy behind one of the most inhumane things in a store, scan bar codes, read outs saying here's a discount on fried beans, you get to checkout, no human being, scan bar code, then leave, maybe later get a discount at the Shell station. He told me we screwed up, that's too mechanized. Talk to Doug Rausch, just retired president of Trader Joes. Jose was teaching history of retailing at Harvard. Retail ideally should be working for the customer. The Trader in Trader Joes is that agent. Jose said we could use VRM. A better conduit from the customer to the company. Trader Joes has nothing but customer interaction. Doug said we do what we do already.

Adrian: Businesses all understand what they want in life – scale. "We" don't have a word.

It's not scale.

Adrian: Would love to get people's ideas, if this is not the right problem, what is.

Examples of what VRM would be. One is a wallet of my own. Has a kind of scale. Various IDs and credit cards. This is kind of an agent. An idea Joyce had way back in 1995, why can't I get a shopping cart I can take from site to site. That turned into Intent Casting. Why not a normalized way to do subscriptions. If it's only up to the big companies, it's not going to happen.

Joyce: It's the user's idea of convenience.

VCs require lockin and an exit. I want our customers to love us. The internet is one of those. Email. A key thing Doug Rouse said is, we don't go to retail trade shows, all about screwing the customer. We know we're not the only store.

Adrian: #DarkPatterns. The people who design the idea of convenience are UX designers. They themselves are always only paid by the Bs. We as Mes have no equivalent way to paying them. They use Twitter with #DarkPattern, put screen shots on Twitter as a form of penitence. It's basically stop me before I kill again. This is not a deep thought. We are not going to achieve the alternative of scale unless we can bring to bear the expertise that the Bs get to bring.

Join the Project VRM list: https://bit.ly/vrml1st

Drummond thinks he has a wallet with connect.me.

Adrian: HIE of One, we're not willing to move any faster than the standards. My criticism is none of us are working together on anything.

Q: I came here a year because I didn't want to build it. Make really cool personal AI. Could get creepy quickly. Have to tell our users it won't run amuck. I learned of this community, can I retire a lot of what we're building. We thought would need hardware stuff Johannes is building, I was told last year none of this stuff is good for production. Seems a year later inching toward a place where we can build something. The AI.

Q: The core driver is the consumer's need. I worked at Sears in the e-commerce group. Online pickup in store. 0-48 hour need state. Thought could compete with Amazon at that time. How do we know what a customer needs and our experience to fulfill that? Definitely not a lockin. Matter of convenience was what we were building. Driver from the person side was what is that need state. I believe that AI as an agent for consumer has a real role to play here, trying to capture that. To have a mechanism to publish those states to actors that could fulfill them.

Johannes: You had a bunch of use cases I wrote down, wallet, shopping cart. I'd like to understand, is there no way of getting it adopted, have we not found a way to get it adopted, or has it not been built yet?

Doc: Project VRM wiki, page of developments, 20 companies doing intentcasting. None of them have caught fire. Lots are in personal data collection and aggregation business. Liam has one. Digi.Me is another. It's really hard to get the UI right on this stuff and make it viral.

Having figured out how to make it work.

Yes. So easy to get it wrong. AT&T. Apple Newton. Esther Dyson said nobody is ever going to write on glass. Blackberry ran with that in a huge way. Palm, Nokia. Nokia would give me a phone, the US version didn't do WiFi, wanted to disable that, partners in phone business quashed that. Apple and Google win by having you write on glass. Will be something that's going to be in this. Digi.Me is great for one thing. Finding things on Twitter that Twitter won't find. Search is getting really deprecated. Anything old disappears. I put lrfmstrdl in old blog posts. Google won't find it anymore. Google is only following the live world right now, the archival world is deprecated and going to hell.

Adrian: Can we consider the design, the architecture by which the three of us and the other six can split the separation of concerns in the VRM umbrella so that by design as open source projects under this flag we start to literally architect scale for this wallet, this shopping cart, this app on the app store. Do we have critical mass in IIW to now actually establish kind of a pact that, Liam's going to do the AI, Johannes do the hardware, I'll do the regulatory.

Doc: Come to Lisa's talk and to Nitin's talk. You're all doing Me2B work. Needs to be a term that catches fire. The other is, Nitan and Sean Bohan and Lionel Wallberger worked on a VRM maturity model, will be very useful in Me2B also. He lives and knows everything about what will click with businesses.

Nitin: Full disclosure. I spent two decades in CRM. Know that space really well. Doc mentioned customer experience, the definition of that came out of a group of 4 or 5 folks at a very small company, we invented a market called CX which caught fire, we got acquired by Oracle. We open sourced the language of CX. But that's a win. The struggles I've had with IIW, all these initiatives. I'm not a technical person. We decided to build a framework. We identified 5 participant groups: A developer, a customer, vendor, market maker, policy maker. Not perfect. Most of those are self-explanatory. The mall is a market maker. Ebay is a market maker. A business unto themselves. These are the constituents that make VRM happen. What is the technical stack? What layer are you playing at? We did all this stuff back in 2015.

Adrian: You are describing exactly the components we modeled at HIE of One. It's perfect. But then what next?

Q: The work that me and my team have been doing may slot into this in a way that is complementary. Holochain is the idea of instead of having a web server, users themselves end up not only end of sharing burden of storing, but also the validation. An app is really a shared grammar with other participants who meet the rules of whatever the participation is. Doesn't dictate what the interface looks like. Decoupling ends up being interesting and powerful. Opens up possibilities of the thing the customer has. They visit all of their contexts.

Adrian: Data about me. Will be in my session, last of the day.

Q: Holochain not in production, getting close.

Adrian: We have a lot of work to do to enlarge the tent beyond the 4 of us. Probably does have to happen around IIW.

Q: Encourage, there may be paths that are indirect paths that get us there.

Adrian: How do we get Nitin to help us?

Q: But orgs come to me, should we use Holochain for identity stuff. I say no. Focus instead on supply chain coordination, passing information between customers, that's a context where you're not boxed in by the framing of the problem in the first place. A 360-degree solution.

Identity For All: Refugees, Human Trafficking, Women & Marginalized Populations. Tech Meets Real Life Experience + The Humans That DID & SSI Can Help Most – How & Why.

Wednesday 7H
Convener(s): Kristina Yasuda & Jessica Hubley
Notes-taker(s): Ben Gregori & Pam Dingle

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

Notes from Ben Gregori

Identity for a Refugee - Survivor identity needs

1. High demand for security and recoverability. Survivors have various devices over their journey (from trafficker to recovery; across multiple types of device) – needs anonymization.

2. Passwords are not good – trauma impedes memory

3. Recovery mechanism (based on Kaliya's paper) might work by using facial recognition without storage (using a hash – enables recovery with face without storing data; also allows revocation for corrupt staffers or other system participants with access to these credentials)

- overlap with refugee population (no identity and needing to create one – used name has no record, a lost identity – documentation is lost, reborn identity – assuming a new identity to escape trafficking space, guardianship – those who cannot speak for themselves such as minors) - all of these conditions must be considered.

- The role of a certified identifier (by aid staff, camp staff, etc) can provide the verification for identity.

(League of Nations created passports after WWI to reconstruct identities based on their skills, financial, and educational backgrounds) – how do we extend this?

- Trust waterfall strategy: people who already have social trust use your identity wallet, and once they use it, they can help their patients/students to help train/educate
- Can we digitize a personal dossier of medical information so that individuals own medical information instead of doctors/hospital systems (Bangladesh works like this).
- Facebook in Myanmar has filled the place of digital identity for Burmese citizens; these systems were not framed for any consent by the individual and there is little education on it. However, it's functionally a huge improvement

There is always an infrastructure question when working with vulnerable populations (such as in refugee/migrant situations) – how do we help people where there is no mobile connectivity?

Digital identity frameworks (or imposing one on a population) created by authoritarian governments enable majority populations to persecute minorities. So developing this should be independent of government, but enable government to plug in.

Lost identity workgroup – how do you secure biometrics when they can be forced?

There is a competing priority between future-proofing a identity system and creating a well-thought system that cannot be abused in different contexts in the future, versus helping refugees and vulnerable populations immediately when some populations may be willing to sacrifice privacy for greater benefits, such as receiving needed aid.

Guardianship is really important: mothers may adopt children out of good will that have been orphaned or their parents cannot care for them, and that may be a valid context. However, being lose with guardianship leaves holes for trafficking.

Community attestations – how can we use community attestations (that can localize identity frameworks to the relevant popluations) in conjunction with government/official sources of attestations, with different weights applied to the importance of each attestation relevant to the situation and the level of trust a verifier is willing to accept (eg community attestation may be fine if there are no other alternatives and it's a low-risk consequence if there are errors, versus more community attestations AND GPS location verification AND a government record to take a child across national boundaries).

ITU: SDG Digital Investmetn Framework – removes the dilemma of solutions either being for-profit or open source with regards to questions about sustainability and adoption.

"Beyond the Hype of ID4D" – short paper to gather critical literature of ID4D

UNHCR virtual summit portal (DIF)

How does this solution look from a tech perspective?

Notes from Pam Dingle:

- Jessica - anniecannons.org
- Kristina - internetbar.org
- Jax - innovationforgood.com and stopchildtraffic.org

Background:

- Sharing experience for people with marginalized identity. Working with people who are at risk such as refugees and domestic violence victims (survivors of gender-based violence, human-trafficked)

Annie Cannons trains victims referred from shelters to be developers. Some are for hire and some are the ideas of the people themselves. Ideas coming from Shelter victims often cover "how can we improve access to services"

Issues that came up:

- every software solution used at an agency is built for the agency, to help them manage cases and people
--- not designed with the idea that a survivor could use it
- some folks are born into slavery and have no real identity
- some folks are PHds:

People end up at the same facility many times, because they are being re-trafficked. The system doesn't understand when we are helping the same person vs helping different people.
Can we put agency into the hands of the survivors?
Can the system check if you are eligible?

In trafficking scenarios, devices change all the time. Sometimes traffickers sniff traffic in local areas. Therefore there is a high bar for multiple devices, device security

Phone may come from trafficker or by Verizon home line. Anonymized data is important, can't trust the phone
- if you are highly traumatized you are probably not going to
- eg app loooks like a period trafficker to get past supervision but has extra features.

Need face recognition w/o storage of a face

- sometimes actors at the help orgs are in fact traffickers or abusers
--- need to revoke but also to track WHY they were revoked

Use cases for Human Rights Causes:
1) No identity - you need to create one
2) Lost identity -- you had identifying docs in origin country but none in new country. some might be reproduceable
3) Reborn Identity -- a kid who was in forced servitude might need to start new
--- somebody might need to be trusted or not trusted
4) Guardianship for those who can't speak for themselves

eg: 78% of pimps in bay area were themselves abused as children

Earning money means earning food and water yourself - how to create an identity that gets you there?
- gov'ts don't always do this

Trust Waterfall strategy
- people who you trust start to use your wallet (doctors, case workers, teachers)
- they set you up and then teach victims how to use it
- in bangladesh, patient owns their identity
    - paper based, they have a dossier
    - can that be digitized
- talking to refugees in Greece, Syria, Lebanon
--- each camp is very different
--- eg in Bangladesh, some have smartphones, access to digital stuff

In refugee context, how do you tell what works
- collection is local, doesn't need deep technological learning
- verifiers act centrally to look at the local

Myanmar:
- as of 2012, the most a citizen could have is a paper card with information filled out in pen.
- if a kid is caught in a raid, there is no way to get that
- facebook *is* the internet in Myanmar. Today, facebook is a defacto identity infrastructure for burmese gov't
    - those systems have not been framed for consent.
    -

For refugee: very often this is an infrastructure question not a technology question.
- there was infrastructure yesterday maybe, but not today

UNHCR worked with Facebook - if they don't hand over any data, then those people will never have status.
- if they do hand over information, the gov't can persecute, but Myanmar has a fledgling digital identity effort.
Dilemma: is it better to be known and hated than not known, when it comes to asylum seekers?

If you are fleeing and your fingerprint will expose you as a known identity - what do you do?

Here we talk about user centric identity as privacy preservations but in developing countries, the issue to be resolved is just identity - having one at all.
- eg: aadhar: yes, central identity was stored, but purpose was different - goal was to give the ability to billions of people to prove they are a person to the government. Lots of people in lower classes especially gained huge benefit even if the privacy concerns weren't perfect
-- access to services is critical, not a privilege

Women coming in to these programs have never had privacy in their lives, ever. They are asking questions like "how do I know that my email is being monitored".

Note from Joy - Denmark is 50 years into their national id and the privacy issues are coming home to roost. Need to build it in

Neha - it is important to understand the scalability and remember why this was done.

Jennifer - refugees really do care about privacy because their personal safety depends on it.

Part of the consequences of any technology we put in place needs to take in the GRAY area
- eg - woman has 5 children, 2 are her own, 3 she claims to protect them. Some of them might be trafficked. This gray area is where someone is trying to do good, but some identity requirements might put those children in danger. We need to be aware of the consequences of the cold beaureaucracy need to be viewed in the lens of protection

Colombia - all the immigration projects right now are tough - colombia is small and refugees are overwhelming. How can colombians manage the identities for example the children born in the camps. do refugees care about privacy or belonging to a place (or both)
- in some places, the importance of belonging is huge. If you have not one single document.

Maybe we end up with an identity solution that can work with a government and one that can work independently - maybe these need to be independently considered

question: Do we need a global identity for everybody?
-- some countries are abusers. We need to

Question: does iris scanning work as well for dark eyes? Answer yes, but still working on what happens with children under 5 can be reliably identified?

An attendee worked on Identity for land registries - somebody came up with the idea of weighted attestations - records from NGOs, camps, community attestations, could we take some of those methods

Global identity:
- Could you trust someone that has shown a cycle of bad activity
- entities that aren't a government could offer an identity to people that might be more valuable
GlobalEntry - works in 15 countries, gives privilege to go into/out of airports
-- adds a risk

Project in Papua New Guinea - iris recognition powers an ATM - just talking to village owner, they could distribute the ATM without the gov being involved.
Counterpoint - you can't exist without cohabitating with the rule of law.

Paper currently written that points out - not every identity needs the same level of security, but the services that the identity can become a problem - eg, the level of identity needed to get into a camp vs. the level of identity to get government payouts
- need to determine when the next stage of security is needed.
- security decisionmakers sohuld be able to determine this.

Tradeoffs between government support and privacy -- how do you give people a choice?
Most consent today is ONE WAY consent. There needs to be a way to take it back.

George: as engineers, we try to solve edge cases but this is about real people who are in danger. We need to start looking at the good of the system and weigh it against the possibility of evil. We are thinking about edge cases and ways that this can be abused - but in our world there is nobody in physical danger.
- local tribal policy is drastically different across the world. We (as americans) should be careful to force our idea of privacy across these very different worlds

Most folks here are for-profit companies. Adapting a for-profit product for non-profit beneficiaries may be incompatible.

INitiative is being put forward by the ITU - DIAL and ITU "SDG digital investment framework" argues for interoperable components, identity, payments, messaging are the core components. The for-profit and not-for-profit

Smart Africa is another digital initiative

Balacz: Europe is building the worlds largest biometric database -- but users can't opt out, and terrorism trumps these rules in reality. Once gov'ts access the data, how do you put everything back in

Jessica: It is great that for-profit companies are interested but it is the people who are at risk that need to be involved in the design process.

Cannot do this alone: need a global lens, need lens of a survivor, of Identity, of enterprise, design thinking
New paper - Hype for ID4D

How does this work with technology - - this is a great use case articulation -
Iris scanning BSP www.irespond.org

Gender Is Harder Than You Think

Wednesday 7J
Convener(s): Annabelle Backman
Notes-taker(s): Annabelle Backman & Alan Viars

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

Notes from Annabelle Backman:

What is Gender Identity?

- Gender identity is the innate sense that you are male/female/bigender/etc.
- Everybody has one!
- Huge spectrum of identities beyond male/female (e.g., bigender, agender, genderqueer, non-binary, etc.)
- There is no gender identity taxonomy
    - Terms are being coined and redefined all the time
    - Meanings are subjective, fluid

Why is Gender Hard?

"Legal" Gender

- This doesn't exist! There is no one notion of legal gender in most jurisdictions.
- Consider: Driver's License, Birth Certificate, Social Security, Passport, etc.
    - All of these are independent, disconnected systems, run by different agencies
    - Rules vary across agencies and jurisdictions
        - for what can go on them (e.g., M, F, X)
        - and how to change them (e.g., requires court order, letter from doctor, etc.)
- Rules are changing over time:
    - Example: as of Oct. 1, 2019, Rhode Island allows X on birth certificate

"Biological" Sex or Gender

- Also doesn't exist, at least not in the way most people think!
- Chromosomal combinations other than XX/XY exist, and XX/XY don't always result in what people typically think of as female/male

- Hormone levels often matter much more than chromosomes, and these can be altered by medication
- Significant variants in anatomy exist, and anatomy can be surgically altered
- Secondary sex characteristics vary wildly, within and across ethnic groups

Variability

- Individual self-identification can change over time.
- Self-identification can depend on context, e.g., a transgender woman may present female at home and in their personal life, but male at work because they have not come out at work yet (and may never will).
    - "Coming out" is a continuous process, repeated in various contexts and as new people are met.
- Gender on legal documents may or may not be updated, depending on an individual's ability to meet the jurisdiction's requirements, and depending on whether the jurisdiction allows the individual to identify in an accurate fashion.

What to Do?

Do You Need It?

- Often gender is used as a proxy for something else. E.g., whether or not the person should be asked if they could be pregnant before prescribing medication. Consider eliminating the proxy.
    - E.g., Are you capable of becoming pregnant?
- Be wary of "side-channels" for gender
    - Asking for a title such as Mr. or Ms.
    - Inferring from pronouns used by the individual
    - Inferring from names

Self-Identification

- Let people self-identify whenever possible
- No taxonomy, so a free text field is important
- If you need a "computable" value, consider:
    - Do you *really* need it? (see above)

- Offer a curated list of values, and a free text field in case an appropriate value isn't available.
- Nothing others people like asking them to identify as "other"!
- Consider checkboxes instead of a dropdown menu

Discussion

- Asking for pronouns can be good, as long as you need them and aren't using it to infer gender or other properties.
- Standardization of a set of gender identities is unlikely to be successful
  - Terms are too fluid
  - Lack of trust between tech and gender and sexual minorities
- A "Best Current Practices" for gender identity collection/interpretation/UX could be a helpful middle ground.
  - Tech, advocacy orgs, and LGBTQ community would all be key stakeholders
  - Don Thibeau: Interested in hosting a conversation toward that at next IIW
- Tech can't make the whole world "woke" on gender identity, but BCPs and guidance impacts implementation, increases exposure, helps people do the right thing.

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

Notes from Alan Viars:

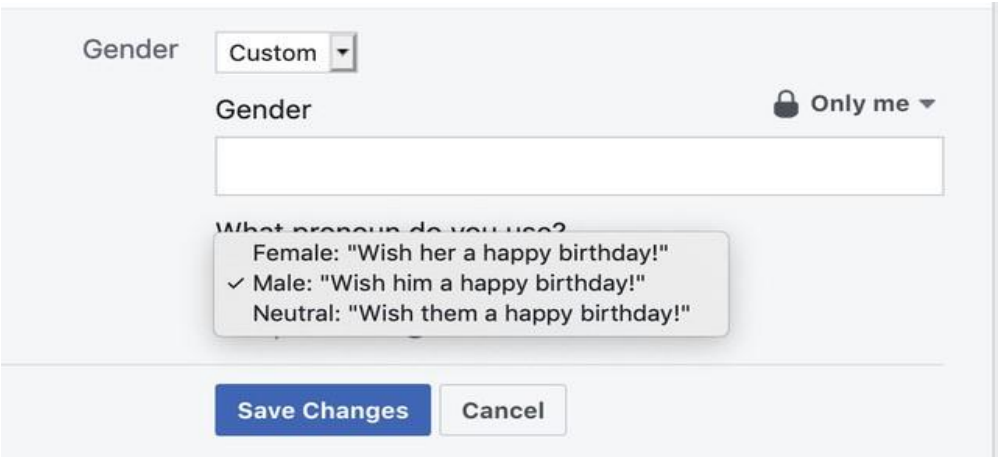
General Notes:

- It was determined it s virtually impossible to create and agree on an enumerated list for gender identity.
- Facebook got this right after some controversy. Beyond, male and female, gender identity needs to be free form.

Gender on Facebook:

Select Male, Female Or Custom

If custom, allow free form text.



Notes on OpenID Connect Implementation

To emulate this model in OIDC, we could make the following updates to OIDC.

These changes should not break legacy implementations.

- OIDC to add optional field/claim for "sex" to include values "male", "female", and "other".
- OIDC to modify gender field/claim to include the new enumerated value "custom".
- OIDC to add optional field/claim gender_custom_value. When, gender value = custom, gender_custom_value SHOULD not be blank.m gender_custom_value is free form text.
- While pronouns

Best Practices for Using Sex and Gender in Applications

- Avoid collecting sex and gender unless necessary.
- Instead, ask questions such as:
    - Is there a chance you might be pregnant?
    - Do you have a uterus?
    - Do you have a prostrate?

What's Going On With DID-Auth? + SSI & SIOP OiDC

Wednesday 7L
Convener(s): Lucas Tétreault & Tyler Ruff
Notes-taker(s): Lucas Tétreault

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

The session was mostly on the SIOP work that Tyler Ruff and crew have been working on.
They demo'd registering and authenticating to a website using SIOP OIDC with nothing in the middle to translate between the mobile device and the website. They talked about how they had extended the standard OIDC functionality to add some back-channel calls to authenticate from the phone instead of the browser.

A more general conversation on DIDAuth did not occur. It seems the community is focused on OIDC at this time and people see "DIDComms" as sufficient for any other use-case that requires authentication.

TXAuth (XYZ, RAR, PAR, JARM JARM…)

Wednesday 8A
Convener(s): Justin Richer
Notes-taker(s): Júlio Santos & Justin Richer

Tags for the session - technology discussed/ideas considered:

OAuth2, OAuth XYZ, PAR, RAR, JAR, PKCE, DYNReg, JSON, DPoP, UMA2, CIBA

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

Notes from Júlio Santos:

OAuth XYZ = PAR+RAR+JAR+PKCE+DYNReg+JSON+DPoP+UMA2+CIBA

There is a new mailing list about this, txauth@ietf.org, 2 days old, please join

there seems to be a general agreement that the world is moving towards this, so standards should evolve with it

Justin didn't so much invent any of these ideas, just attempted to bring them together in a way they can work in a holistically consistent way; he thinks when you're doing a standard, if you keep deleting things and the standard becomes more flexible with it, you're going in a good direction

Why DYNReg? We have a lot of use cases where it's either the user's consent that's the driving trust anchor for the process, or the combination of this plus an attestation the software can make. Now that we have developer facing portals, self-service registration etc, this stops working.

A lot of the same checks you have to do around redirect_uris etc, you should be doing these same checks in a static environment such as a self-service portal. So why are we pretending that we have this middle-man thing?

XYZ starts by pushing a bunch of info to the server (identity, capability and intention). It also helps in cases where you can do a dynamic lookup of attributes about the client, by the client providing a verifiable reference. E.g. the solid project, where everything is based off webid. Similar to SAML RP discovery but smarter. It allows the auth server to say "yes, i know who you are and you can indeed do those things".

The most important output from DYNReg in OAuth2 is that you get a client id, to pass in the front channel. If we didn't have that, we could just use keys directly (ID you through your keys, or secret, no need for client ID).

The way that XYZ works is the client shows up and it pushes a bunch of info about itself, authenticates itself, can be in JSON in XYZ, and gets back if necessary a URL to have the user go and interact with. It's a ref to the tx that only the auth server knows about. Not passing scopes, client ID, no more info, no need to protect this info because it's not in the front channel.

This is the fundamental idea of XYZ — stop using the front channel.

PAR allows for better security and simpler client code. There are a lot of use cases where in XYZ the auth server can get enough info about the request to determine that it doesn't need the user to actually interact.

RAR. Scopes in OAuth2 are not expressive enough for certain classes of clients. Where Justin thinks we're trying to sell, and this is active debate, is that we should have a JSON object but also have there be a schema such as URL locations, types of actions etc. You can send this things as either an object that obeys the schema, or as a single string in the same data structure. It represents a pre-filled out resource object aka a scope.

Someone asks "How would the scopes be defined? At runtime, registered with the AS, or...?" Registered with the AS at build time, Justin says. The AS would have a list of scopes.

Someone suggests this could be more flexible, and is potentially too restrictive for OAuth2 to define.

Someone suggests it would be more powerful if the client could also specify the scopes. It would allow scopes to be more powerful (e.g. aliases). Someone else observes the mechanisms for this would live outside XYZ. Justin agrees.

Someone asks if XYZ allows you to specify both JSON and strings, if there are rules to help reconcile this. Justin says they need to be defined, and ultimately would be up to the AS.

OpenID has a lot of functionality that's independent from resource servers. There's work to be done in XYZ to figure out how to support this.

JAR. The big idea is that you don't have to send everything as query parameters on the front channel (vulnerable to a lot of attacks). XYZ gets around that by not using the front channel as much (see PAR).

XYZ gives you a lot more flexibility about how to interact with the user.

The client talks to the AS (XReg), gets back an interact_uri (and a tx handle X_H, meaning "we're not done, next time you talk to me, give me this"; this is how you distinguish a first from other requests). The client just asks the user agent to go to it, no parameters added. The client has no way to modify what's in this url.

Keeping clients dumb is really important, as it's one of the biggest things we got right in OAuth2.

User gets redirected to the URL, then to the callback_uri. In XYZ, this has an "interaction handle",which allows the client to continue the tx (XCont) by saying "yes i can prove i got sth back from the front channel".

Someone asks if the expectation with the XCont is that the transaction actually continues or could be complete.

People don't handle error cases in the front channel properly. XYZ helps because it's easier to tell state because of interact_url, X_H etc.

We don't need a whole bunch of error messages coming back, because if the user denies the request, the client will know when it tries to proceed.

Once I get an AT, I can also get another tx handle X_H with the AT. In OAuth2, I'd need a refresh token. In XYZ, this is done through continuing the tx through its handle.

Someone asks if we can do downscoping etc through this process too. Justin doesn't know what, but he feels like this would be done through creating a new tx based off the results to a previous tx. "and btw I've already done this bit". There's still work to be done in specifying how these things would work.

PKCE isn't needed anymore since you're not relying so much on the front channel. XYZ grants you the same type of crypto protection without needing PKSE.

DYNReg. There aren't really "public clients" anymore, because when you start a tx you start it with a key.

In OAuth2, everything hangs off the client. In XYZ, you don't need that. The client is just an aspect of the tx itself, and the tx is the primary model. The client is just about "who started this":

Someone says that from an implementation perspective, the client is super important. They'd need to know that this request is coming from this particular entity, with a high level of assurance. Justin says "sure, that's why you use the client secret". They object and say this makes it harder to disable bad actors. Justin says this is possible with XYZ because your AS always know the client's keys, and you don't need to expose a client ID for that.

Someone else says the client identity's may not matter from a protocol/sec protocol, but it does matter a lot from an operational/Deployment standpoint. They don't think key IDs are sufficient, because if they are an operator they want to be able to aggregate txs from one client across all devices, and not just one. Also

important for end users to manage their active sessions. Someone else agrees and adds to this to say this is super important from a user consent perspective. Justin says this supports his point about moving away from client id, in which you can't diff between 2 instances of a client vs 2 different clients.

Someone says this all sounds like we shouldn't be rebuilding OAuth from the ground up just because OAuth2 isn't perfect. Also that DYNReg would be an issue from a regulatory perspective because it allows for anonymous registrations. Someone else agrees. Justin doesn't respond.

JSON allows us not to use form encoding anymore.

DPoP gives the client agility to be able to say "this is the kind of key i want to prove, and here's how i can prove it". What kinds of keys are allowed to do what kind of things? This proof happens and is included in every request.

UMA2 is about no longer making assumptions that the person using the client is the resource owner, and this can be done asynchronously in XYZ because of tx handles and continuation requests.
Someone asks how you communicate the next url for resource discovery, in subsequent requests? Justin says resource discovery is hard and hasn't been properly specced yet, but it'll be easier with the use of RAR.

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

Notes from Justin Richer:

Please add the following URLs for all the related specifications and workgroups to the session notes.

XYZ: https://oauth.xyz/ https://tools.ietf.org/html/draft-richer-transactional-authz-02

PAR: https://tools.ietf.org/html/draft-lodderstedt-oauth-par-00

RAR: https://tools.ietf.org/html/draft-lodderstedt-oauth-rar-02

JAR: https://tools.ietf.org/html/draft-ietf-oauth-jwsreq-19

PKCE: https://tools.ietf.org/html/rfc7636

DynReg: https://tools.ietf.org/html/rfc7591 https://tools.ietf.org/html/rfc7592

DPoP: https://tools.ietf.org/html/draft-fett-oauth-dpop-02

UMA2: https://docs.kantarainitiative.org/uma/wg/rec-oauth-uma-grant-2.0.html https://docs.kantarainitiative.org/uma/wg/rec-oauth-uma-federated-authz-2.0.html

CIBA: https://openid.net/specs/openid-client-initiated-backchannel-authentication-core-1_0-02.html

TxAuth: https://www.ietf.org/mailman/listinfo/Txauth

Problem of Provenance of Digital Content Roadmap to Solution

Wednesday 8C
Convener(s): Kathryn Harrison (Deep Trust Alliance)
Notes-taker(s): Sarah Allen

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

Why are people here?
- Supply chain - media, ads
- Gov ID - root of trust, how do you know the provenance of public keys
- provenance of research, starting with real-world objects, creating a chain of trust

Hypothesis
- Long term solution around understanding digital provenance
- Start with digital content, chain of custody

Digital Provenance
1. Something happens in the real world and you take a photo
    1. Potential for standard in the h/w (heavy lift, h/w provider)
    2. New iPhones use specific points to identify your face, could you get a standard, register an identifier, so you can identify a specific image ==> Unique Identifier (UID)
2. Then there are a number of manipulations, chain of custody all tied to that original UID, see chain of actions (attestation of what happened)
    1. Contrast
    2. Crop
3. Send to internet, track this chain of custody (That others can add to)

What do you need?
- Standard set of data
- Tons of meta data standards (figure out what small amount of info will persist)
- Some kind of UI (e.g. little blue checkmark, which you can click into and see this chain of provenance)

Not saying the content is real,. Good or correct, just that we know the provenance

What about governments going after sources? Is there potential for unintended consequences?

Need a privacy layer to avoid Orwellian authoritarian state

Each edited asset then has a new UID

Use case: figure out if a specific image is valid

Movies, Images already have fingerprints that can detect user misbehavior

What about the user detecting media company misbehavior?

Chaos computer club — series of videos about system that is live in North Korea

- Put an image in, it gets watermarked, the government can find the computer and the human who uploaded that image

Corp use case: insurance

Attempting to track back to a source
Each step of the chain could have specific requirements for a specific context

Digital cert at each step

Turn It In — system for student plagiarism

"Is this image trustworthy?" —> this is not the question

rather "Does this photo/video have the context for the viewer to decide whether to trust it?"

The question is about object integrity. Difference about integrity and trust.

It's a pipeline problem.

Idea:

- Create a centralized corpus of deep fakes
- Companies continue to own them, yet provide decentralized access to them
- Companies could contribute source material, build provenance into this niche data set to identify these sources
- Would need to have a system of authorization around this

Can the beneficial outcome be described in more detail?

Consider toy sources that could serve the same purpose… maybe a demo "We want to do this, but at a bigger scale"

Want to see mapping out use cases

Careful about making tools for the Deep-Fake-Creators
— see Genomics for ways that resesarchers / publishers have found ways to create "protective wrappers"

Consent Receipts for Financial Services and More…

Wednesday 8F
Convener: Colin Wallis & Erik Lamb
Notes-taker(s): Colin Wallis

Tags for the session - technology discussed/ideas considered:
Consent Receipt, API, FDX, Kantara, Finicity, Datafund

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

Extended discussion on how FDX and its members propose to 'API' the consent receipt for the financial services sector. We overviewed the two orgs, the announcement and an example published on Youtube of a Consent Receipt Generator and Viewer developed earlier in the year by Datafund in Europe.

Links to slide decks:
https://kantarainitiative.org/confluence/display/infosharing/Home?preview=/37748979/120619091/Kantara%20Consent%20Receipt%20Infographic%20-v02.pdf

https://www.slideshare.net/AndrewHughes6/kantara-privacy-control-panel-demonstration-2019-0515

Me2B Intro & Org Finder Wiki

Wednesday 8G
Convener: Lisa Levasseur
Notes-taker(s): Scott Mace

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

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

Me2B Alliance, market creation through consumer awareness

Did a presentation at MyData 2019 Helsinki last week

Vision: Ensuring human dignity and agneyc in connected products and services.

Real challenge, how do we influence change.

As we sat trying to figure out our principles, want to bring this concept of Me2B relationships in the common vernacular. No longer buy things like a 1 to 1 moment in time. It's an ongoing stream of bidirectional transactions with service providers and brands in general. We're having relationships with them but we don't think of them as relationships.

We have more of these kinds of relationships than we do anything else – our personal, family relationships. I really want to get people thinking about the fact that this is a relationship. Hold it to the standards of relationships.

We know how to behave in relationship. As social animals, we've developed a lot of universal principles.

This list started from the characteristics for healthy human relationship.

Me2B Rules of Engagement.

- Freedom
- Respect of Boundaries
- Repspectful Defaults
- Fairness & Non-exploitation
- Good communication
- Non-harming
- Problem solving

This is the ethnical underpinning of Me2B. 3 principles

1. I'm in charge
2. We agree to play nice
3. No data without Me2B relationship. (I need to elevate it to a Me2B principal on the web site)

A direct confrontation with data brokers.

How do we get there?

The world everybody is trying to get to is a word where there's more good technology choices than not. That is not the world we live in today. Today we have precious few.

Interesting discussion at VRM day.

- Thought leadership
- Community building
- Movement / activism
- Common vocabulary

The first priority the room collectively thought

- Standards
- Codes of practice
- Certification
- Interoperability*

The individual being the point of interoperability

- Governance
- Rights
- Policy / regulation
- Ethnical business models (proven examples)

A free relationship is more valuable than a surveilled capitalism relationship. A hypothesis. We need data to back that up.

Consumer education and marketing.

Hypothesis: Most people are not fully aware of the risks. We ran a session yesterday on a harms dictionary we are building, to create a resource for people so they can understand what the harms are.

Vendor education and marketing.

I take for granted vendors are aware of what they should be doing and what the rules of engagement are. Enormous lift of vendor education and marketing.

Usability.

It's vital to actually deliver on this.

Me2B

A different kind of standards organization. I was in cellular and internet standards.

Coming out of CDMA, CDMA Development Group, CDMA spec wasn't interoperable. A huge problem. The market was created because the standards org specified what interoperability was, and certified, and did PR. I saw the power of how a standards body could create a market. Another example was Bluetooth. A long road but they made it.

- Multi-stakeholder by design
- More than technical specification. Ethics & usability
- Results / change-focused

We were talking about dark patterns. Nefarious use of UX to manipulate in sometimes harmful ways. Usability is often an afterthought. Certainly not regarded in any standards work.

Doing surgical strikes of things.

Tactic #1: Create the means to collect, amplify, and share the voice of the individual with technology vendors.

We have 100 people on our mailing list. Our work attracts lawyers.

Q: And they're really cool lawyers.

Don Norman, father of human-centered design, is an advisor to us. But his lab at UCSD doesn't have a lot of resources. We're actively trying to foster this here at IIW

Kaliya: Recently formed SSI UX group. Sovrin plus non-Sovrin people. Some usability foment happening. At least a dialog with each other.

Mei Lin Fung: SAP might want to engage.

Thinking user panels, market research projects, for the whole community. We're trying to raise all boats and get to the nirvana of more good technology than not. All our stuff is on our Web site. Did a code of practice, probably premature. Tried to create certification criteria. Were getting in the weeds, throwing it out and starting a new tack to going directly to consumers, what would change your mind of how to make safe technology choices.

Scott: Do not track

A lot of that no-tracking, touches 7012, we are using the customer commons no stalking use case for 7012. The respectful defaults, one of my personal missions in life is to get no tracking as the default. Just like it is in real life. Will also apply to real life as well. Have in our harms dictionary that hybridization situation.

Johannes: No tracking is not the objective. Tracking can be part of healthy relationship. In limited cases. Click-through agreements.

Sheldon's agreement with Leonard. It's that big.

Johannes: We have so many of those relationships. The pushing of upsells. Constant followups. Would be harmful in human relationships.

Q: Analogies in real world. I always start giving people 100% benefit of the doubt. If interaction in the internet worked that way…ask someone a question, if they say "well to be honest" I stop them with don't waste my time with anything less than that. Would be nice to see that on the web.

Q: It's like "with all due respect"

"I don't mean to interrupt" but you are.

There's precedent for tactic #1 in product design.

Tactic #2: Complement work already being done. Identify gaps, fill, glue, and support.

Multiple Stakeholder Organization by design

Me: People

2: Catalysts & support orgs

B: Businesses

We've commissioned a project to create a tool called an Org Finder Wiki. Just a living resource. Figure out who is working on SSI, dark patterns, deepfakes. To make sense of who we are. Today our index is Kaliya.

Kaliya: I would add Michael Becker. Stuff in our heads, constantly connecting. How do we get that knowledge out of our heads. Will be really helpful.

2019 projects:

Me

- Market research
- Digital harms dictionary

2

- Graph-based "Org Finder Wiki"

B

- Code of practice
- Certification mark
- Policy & legal work

Working groups

- Good CoPs WG – certification criteria
- PaLs WG – policy & legal work, Richard Whitt, chair
- Consumer Stakeholders WG – outreach & education, chair position is open
- Usability & UX – new, chair position is open

Board of directors

- Johannes Ernst
- Lisa LeVasseur
- Doc Searls
- Joyce Searls

Get involved: http://Me2BAlliance.org/join.html

What is the target horizon for the work of each group.

Mei Lin: We shouldn't try to load any one repository with everything. Me2B, a lot of things going on, let's fit this so the pieces interoperate without any one piece trying to boil the ocean.

Johannes: Find events related to all of us, and local user groups. Meetup is not it.

Mei Lin: A group called Open Collective.

Q: Job search.

DOMI: Digital Rental Passport, Architecture & Data Brainstorming Workshop

Wednesday 8H
Convener: Katrie Lowe, Pavel Metelitsyn, Juan Caballero
Notes-taker(s): Katrie Lowe

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

Link to notes which includes diagram/images – provided by Katrie:
https://drive.google.com/open?id=1C9vwtgOJRxQafXxsff1YF8v9C7BPq0Tq

Related links: http://www.domilabs.io

Intro to Domi:
Domi is a digital rental passport and a decentralised data management platform that empowers renters and applicants to fully control their personal data through the entire application and renting process. Domi enables tenants to "passport" their rental data wherever they relocate, and landlords handle rental applications in a more GDPR compliant way.

The Domi team is part of the SSI incubator program (ssiincubator.com) and is focused on building a proof of concept over the 12 weeks of the program.

Session objective:

Get feedback on how to approach delivering some of the features of Domi in the context of SSI data flow / architecture.

Session discussion:
Suggestion that Domi was building a "reputation system".

Team stated that we are definitely not intending to build a subjective/scoring reputation system.

The principle behind Domi is to improve fairness in the way renting happens so what is recorded in a tenant's passport will be just pure fact based events so that landlords assess tenants just on this, like a CV.

Discussion was had what "reputation system" means. The concept of a "subjective" based reputation versus one that is "fact-based".

The problem with credit scores being used to judge people in rental application is that credit scores are designed with not sufficiently narrowing context that they aren't suitable to be used in the context of renting.

Measure theory concept introduced - the question of what ration / interval scale in which things are assessed. E.g. Uber lift rating is really not 1 to 5, because if you drop below 4 you are out of the system. It is actually are 1 or 2 rating system (yes/no).
Subjective ratings are gamed and corruptable.

Suggestion: Map Domi against existing rental management tools and see how we fit in/alongside

Native or hosted wallet
Suggestion: Tenants will prefer to use Domi's cloud service / hosted wallet. Landlords (big corporate landlords) might want to manage their own wallet

How to address linking multiple issued VCs together if they below to a single contract (e.g. in when there is a rent price increase)

Domi idea: Issue new VC with old contract embedded within and revoke the last VC.
Question was asked why we need to revoke the last VC - it was explained that there are two ways to think about 'revocation':

1) Change in (definition???)
2) Credential that has a definitive time of validity

So... revocation is immaterial in Domi's situation. May not need to revoke old VCs.

Other points suggested for consideration:

1) Landlords will want a complete history (so perhaps tenant's are not able to selectively disclose what they share of their tenant history)

2) Need a dispute process - Domi explained that VCs can only be issued with consensus from both parties. If sign off from one party is not achieved, we would use existing 3rd party arbitration if consensus from both parties is not possible to provide the 2nd signature needed.

Brainstorm of other items people might want to see in their passports

- Providing rental payments
- Maintenance being done (repairs to be recorded)
- Approving renovations

Proving payments

Domi idea: 4 options identified 1) VCs issued by banks confirming payment; 2) Landlords issue VCs - a commitment to be done as part of using Domi; 3) Tenants self attest; 4) Payments are processed through Domi.

Feedback:

Re: 2) Incentive for landlords to participate? Need to see what landlords would actively Participate

Re: 4) Domi could also be an escrow agent. Also support the management / return of security deposit. Extra risk Domi would need to take on board as an escrow agent, but it is another revenue stream opportunity.

freeclaims.org: Let's Encrypt for Basic Verifiable Credentials; Also, DiD-OAuth2

Wednesday 8l
Convener(s): Wayne Chang
Notes-taker(s): Gregory Rocco

Tags for the session - technology discussed/ideas considered:
DID, OAuth2, Verifiable Credentials

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

- Centralized server and issuer that issues W3C verifiable credentials to anyone
- Based on a Google account and phone number, everything was wrapped into a verifiable credential
- The idea is to donate the code to the DIF and figure out how to decentralize the governance of it and figure out the issuance component.
- If you're a user and you would want to use it somewhere, you would need a wallet, to begin with. Until wallet infrastructure is built, then it's usable.
- OAuth2 is widespread, and what if we allowed anyone with an OAuth2 account an implied DID automatically. The caveat is that they're centrally controlled.
- How do you show control? You would check with the issuer – but you can issue to anyone with an account with other services
- **This is called a verifiable credential – if I have a phony facebook account and phone number, what am I really being verified for?**

    - You can check that freeclaims.org signed the data packet. They would need to sign in with the user's OAuth2 account.
    - **If you phish them, and had the credentials to log in with their account –**
    - If you get hacked, it's similar to losing your private key. I think it's a fair point – you can do that today with compromising individual accounts.

- I think we should classify DID methods – if there was a garbage category it would go in there.
    - **Can you remove the PII?**
    - Yeah we can salt and hash it

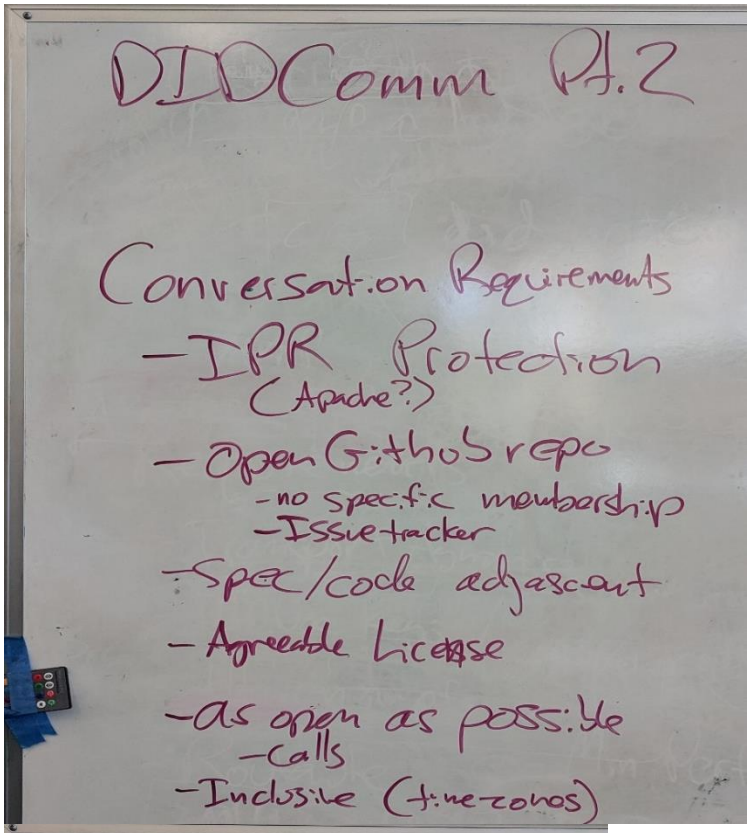
- *The purpose here is to bootstrap everyone on existing systems to use DIDs* – what if you used a user-controlled DID in conjunction with this? You can then migrate your set of claims off these providers. We're not just going to hop on our decentralized Noah's ark and go to a brave new world – this is a stab at a bridge.

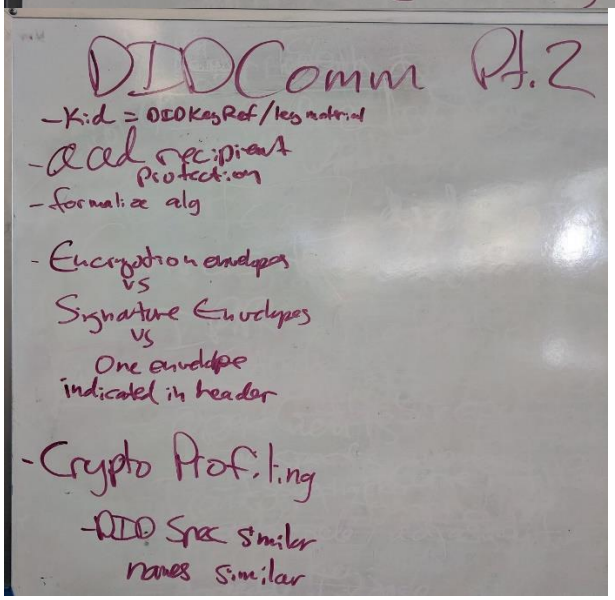
Associated link: https://gitlab.com/alpinefresh/freeclaims.org

DID Comm Part 2

Wednesday 8J
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:





Highlights from 12 Months of DHS Private Sector Research: Election Security, Supply Chain, Legal & IOT ID

Wednesday 9A
Convener(s): Heather Vescent & Juan Caballero
Notes-taker(s): Heather Vescent

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

Links to Three Reports Generated from 12 Month DHS Research (downloadable):

1. Voter Report – www.bit.ly/vdsreport
2. Global Supply Chain – www.bit.ly/GSCreport
3. Non-Person Entity – www.bit.ly/NPEreport

Proof-A-Palooza: Standardizing Presentation Request Language for Verifiable Credentials & VC's in Application (Part 2)

Wednesday 9B
Convener: Nathan George & Martin Riedel
Notes-taker(s): Alexander Tam & Nathan George

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

Notes from Alexander Tam:

how an issuer gives a credential determines how a holder can share, eg. if they can share one component of the credential

- credential
  - subset of claims
  - subset of zero knowledge prove

  - generate a proof
    - how to structure building the proof in the credential
    - merkle tree and envelope of all claims in the credential

workday

- json based verifiable credential
- no zkp claims
- proof request format
  - schema that outline what the verifier wants

- generate
  -
  - claim proofs that sit along the claim
    - move into proof body

sovrin
- calls the claim a proof instead
- probably best to call them presenting a credential item

- credential request, (credential offer), credential send
- proof request, (proof offer), proof present
  - gives the party the optional to offer an alternative, eg. offer >21 instead of age

- schemas aren't owned, and are immutable. To update, create a new schema that references the old one
  - placed on the ledger

- proof block similar to workday,

- proof request, want claim Y, and a property of that claim, not necessarily the property itself, eg >21
  - check the crypto (signatures are correct, but they gave me the data I waned)

- comment
  - problem, requires the holder to look through their credentials and choose which the verifier wants
  - wallet would know which crednetial is more appropriate
    - does holder ever have the power to do this? Don't want vista situation

  - can automate this but may want more sophasitcated
  - sovrin is thinking of an overlay: schema of what is appropriate to share with certain parties that are supported by some third party, eg. EFF says you should only share X with websites
  - no good solution yet, but not a problem we have now since small amount of use cases

  - issuer can help by defined a good credential, preventing the holder from oversharing
    - could be an access token
      - however gives too much power to issuer, no longer self sov

- comment
  - attack vector with infinite proof request by figuring out what the holder is willing to share
    - not a problem yet since immature ecosystem
  - attack vector by asking proof request for small amounts of data that eventually reveal too much over a long time
    - more of a governance framework problem, GDPR would be helpful here by forcing to ask for as little as possible

- civic, workday
  - specifies what combinations of credential items can be shared, does sovrin?
    - yes, calls them attributes which are bound to linked secret to show ownership of the credential (join identifier or schema def)

- sovrin
  - issuer doesn't define how and what holder discloses to a verifier
    - trustframework definition takes care of cases like expiry credential item

  - can't share the proof for another party to verify

comment
- combine workday and sovrin?
  - yes, can provide a combinature proof of credential
- can you make a wallet to handle different types of credential
  - try and standardize proof request procedure first (same schema)
    - 80% the same currently
  - eg. sovrin driver, workday workplace, use both for a loan
    - have to solve same schema problem first

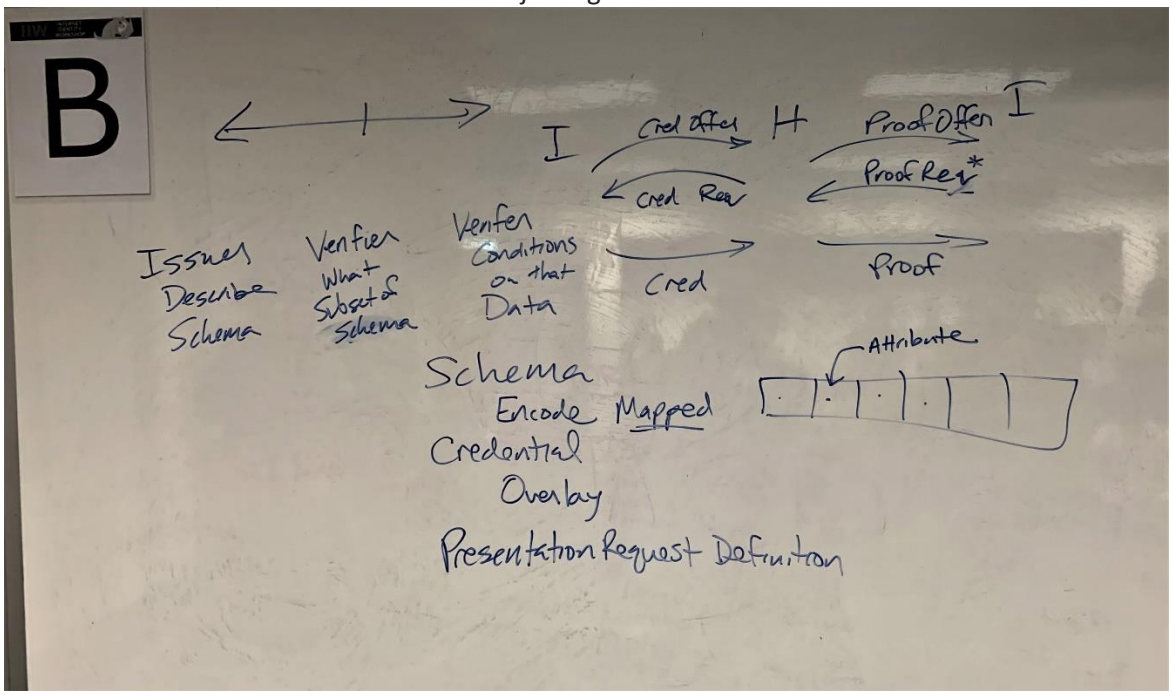
- standards for proof request working group

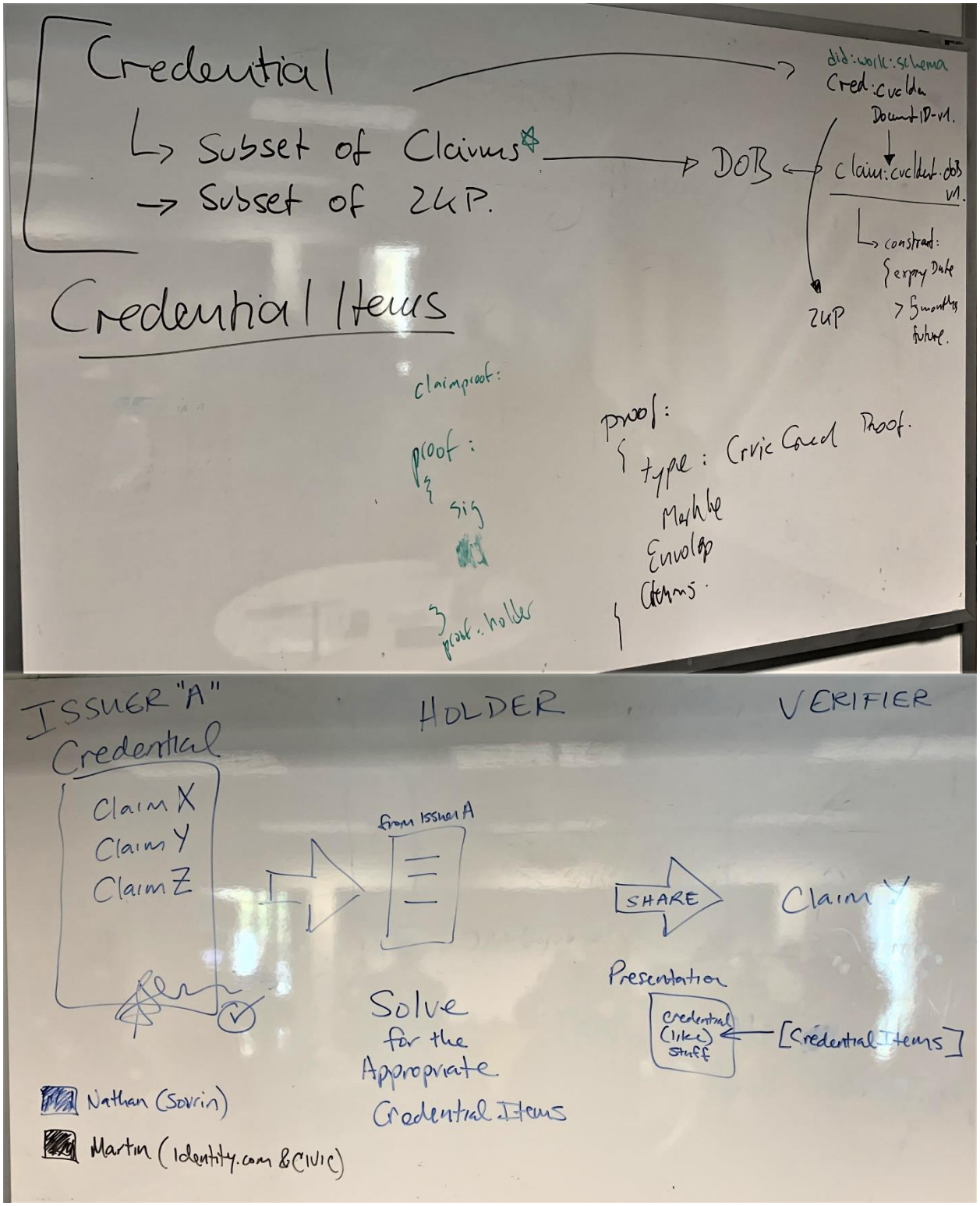
- comment
  - microsoft doing something similar, wants to join standards
  - jwt instead of linked signatures
  - use in openidconnect
  - use did not linked secret for issuing crednetials

- standardizing on crypto is the least of our concerns, since most use the same curves
  - might be a problem if agent vendors don't comply

Notes from Nathan George

We discussed selective disclosure data architecture and how to request a subset of a credential's data and combine data from multiple credentials. We also went into vocabulary for those selected parts of credentials in our systems and discovered a lot of overlap and potential for standardization. A list of emails was gathered for use to kick-start a more official standardization effort. Bjorn of Workday, Martin of Civic and identity.com and Nathan of the Sovrin Foundation (all co-presenters in the session), can provide more information to those who are interested in joining.




Credential
↳ Subset of Claims
→ Subset of ZKP.
DOB
did:work:schema
Cred:CvcIdCard
DocumentID-v1.
claim:cvcIdCard.dob
v1.
↳ constraint:
{ expiryDate
> 5 months
future.
ZKP
Credential Items
claimproof:
proof:
{
sig
proof:holder
proof:
{ type: CivicCard Proof.
Mapble
Envelop
Claims.
}
ISSUER "A"
Credential
Claim X
Claim Y
Claim Z
from IssuerA
HOLDER
VERIFIER
SHARE
Claim Y
Presentation
Credential
(like)
stuff
[Credential Items]
Solve
for the
Appropriate
Credential Items
Nathan (Sovrin)
Martin (Identity.com & CIVIC)

Privacy Chain Update

Wednesday 9C
Convener(s): Wendell Baker
Notes-taker(s): Wendell Baker & Scott Mace

Tags for the session - technology discussed/ideas considered:

IAB, PrivacyChain, Hyperledger Fabric

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

Notes provided by Wendell Baker:

Slides from presentation:
http://wiki.state-space.solutions/page/Presentations

https://cdn.fd2c-8c49-8713.net/state-space/downloads/PrivacyChain_IIW29_2019-10-02.pdf

Notes provided by Scott Mace:

Wendell Baker, Distinguished Architect, Targeting & Identity, Verizon Media
IAB PrivacyChain - IIW29 2019-10-02
Lessons, 2018-2019
Pilots, 2019 & 2020

IAB Blockchain Working Group

Gave talk at Data Responsibility Data, organized by the IAB. To explain advertising has a privacy problem. Laws and societal expectations and most importantly the browsers will change how tech underpinnings will work. PrivacyChain first talked about here last fall. IAB Blockchain WG, I took over that standard specification and stewarded it to where it is today.

I had 20 minutes, carefully scripted. A lot of things have been summarized here. Marketers are not too technical. I acknowledged those who had come before and started the project. Any time you get blockchain, it's not entirely clear what it does.

Lessons learned, in the world this thing lives in, they do open source, but usually at spec level, more rarely in light Javascript. Rare to have this group develop actual running code and systems. I had to explain to that room how open source works.

History and participation.
2018-10 – First proof of concept. Acxiom, now broke into three pieces. One of the successors is LiveRamp. Joe Shai is here at the conference.

Time passes.
201901 – I assembled a group of others. Didomi, LiveRamp, Sabio Mobile, Viacom, Verizon Media.

We have one of these things at Verizon Media. It's a consent manager. It's interesting if you can get

multiple companies to operate these things as a shared resources. Regulators are practicing. PrivacyChain would have a consent record, a logged chain of these things in the database.

More practically, what these consent manager do:

Who can consent, how are they named?
To whom (what) is consent given, how are they named?
For which operations is control granted, how are they named?

In reality you are giving consent to other machines. This thing is building a control channel so you can decide what these machines can do at you, for you.

Need a lexicon.

An IAB standard called DigiTrust. Controversial. Idea is how a principal in business names somebody else is actually an act of ownership. This is not amenable to business practices where you are buying and selling audiences. If we have different ways of naming that, better to work with someone else than with someone who will go to sell the same audience at a different price.

In terms of how the ad trade worries about identity, they're quite happy with the cookie-syncing model. It aligns very well with commercial practice. Even though it has many technical problems. But these are businesses who want to control their business over time. How we name the who is quite political within the ad trade.

I can take this in the direction of DIDs and SSI. We think at Verizon that's the way to go.

Q: DigiTrust is an ID created by the publishers?
It is an ID owned by the IAB. Can look it up on GitHub. Mild business terms for the trade to get involved in the consortium. It's a universal ID.

Q: End user gets a unique ID?
Almost. Every browser. Naming of persons behind the browser is an even more controversial act. Large publishers like Yahoo lets them know who are. We prefer that. But 50% of our business, and 100% of others' business, is as a third party. The new controversial thing here is how do we name persons or devices. DIDs and SSI require some explanation. New is not necessarily good in advertising where you want reach and known technology to work with.
Next two are names of companies and activities. Two public standards.
…see slide

Priniciples, vision and concept.

People consenting to machines. Has to be simple enough for machines to process it.

Persons control Machines as a consent statement (who, what, which)

PrivacyChain is a control channel in the modern media environment.

PrivacyChain is "always-on" and "everywhere available"
Has distributed operation "like infrastructure" "like a utility" "like DNS"

Has auditability.

The cable industry has standardized on this thing called TV Everywhere. You have to log into this thing and prove you pay a cable bill somewhere.

If you are out of town, you will have to give your cable address and cable bill number.

That's the sense of everywhere.

More practical – The simplified MVP

A back office service.
Expect a few separate deployments "as a service"
The service offers Consent Management Platform (CMP) recordkeeping.

I'm using Hyperledger Fabric 1.4. Could swap out for other storage, even local storage.
Standard Hyperledger Fabric, sets up the transaction. A permissioned system. There's a PKI system, all the connections are over TLS, connections can mutually authenticate.

Q: Is the data considered public?
Yes. Somewhat of a controversial point. Security in big numbers would keep bad actors from knowing who had consented to what.

The piece I added here was clarifying north and south side. Simple CRUD operations on your consent on one side. Consumers won't go update their consent a lot. Not that intricate.

Q: What's being verified on the blockchain?
Smart contract is a stored procedure. The chain code has 4 operations - get, set, history and revoke. At this level, there's no smartness to the contract.

Four tracks of development. An open source project. A lot of this is finding and structuring ways other companies can come in and contribute but fits with the overall project. Hyperledger projects like Indy and Aries have a couple years' track record and lots of funding. Here, individuals can come in and contribute various ways.

What we've uncovered in a year: databases break. Usually means an employee and a paycheck. We are formalizing what that looks like. May take the shape of a legal entity. Looks like a lot of work. So we are not rushing into that.

Everything is owned by some thing. Requires some sort of operating vehicle. Right now I'm making the technology worthy of being staffed.

Lessons learned, 2018-2019
Product requires constant evolution, from laws, business, technology, etc.
Engineering in the open source mode is not standards development
The distributed ledger technologies are very new
If infrastructure operations is hard, distributed operation is harder
A business model is an important component of product

While the society has a conversation of what is consent, at least we will have a reference implementation

Say showing a page costs so much. What percentage of revenue could this service acquire
Q: Price paid to CMP today?
No one knows.

I took the original proof of concept. This is not about privacy and blockchain. The brand name is wrong.

Going to leave PrivacyChain for a while, but one can imagine it will be rebranded.

On github.com/yahoo, look for state space, the southbound side speaking into hyperledger fabric and other related projects that speak to the northbound side. What we will be doing over the next year is assemble it into modern container delivery, and an operating implementation. Some with HL fabric and others with exotic databases to prove scalability. A range of back ends are envisioned.

Invitation to participate

IAB Blockchain WG is actively seeking participation around:

- Product fit and function defines the future evolution of the specification
- Consortium operators coordinate the business side; consortium operators hand the "on call" nature of the service
- Software engineering for web-friendly north-facing APIs; software engineering for distributed ledger south-facing APIs
- Database operations for the distributed ledger technologies

Reason why you wouldn't ask for consent – such as digital media rights that trump all consumer rights

How receptive is the industry? There is a spectrum. There are people in the third-party business still exiting denial, moving on to bargaining. No one likes it when your business changes beneath you, and this is a really good change.

Different companies have different appetites about where they want to be on this. Some comprehend DIDs, some not.

Cookies are being changed in the next 200-300 days. Going away.
Go read Webkit.org, Apple announced what they will be denying. Mozilla blog post is a year older. Firefox already launched. Chrome has announced, a blog post there, third-party cookies will be different. The cookies will not appear.

My shop refactoring a lot of ways we do things. Including our "fake third parties" – HuffPo, AOL, etc.

Google third-party sets. A small number of first parties can announce they are friendly with each other. Size of that set, when it will be in Chrome is unspecified. Could be a solution, no commitment to it.

You can be a first-party cookie or a third-party cookie but they won't mix.
At some point, ad tech can't trust the browser anymore.
George Fletcher is talking about it now.

Financial Grade API (FAPI) & CIBA (Client Initiated Backchannel Authentication)

Wednesday 9G
Convener: Taka Kawasaki
Notes-taker(s): Nat Sakimura

Tags for the session - technology discussed/ideas considered: OAuth, OpenID, JAR, PAR, FAPI

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

Taka went over his slide, explaining the FAPI and using his slide including the history, security enhancement etc. https://speakerdeck.com/takahikokawasaki/financial-grade-api-fapi-and-ciba-iiw-fall-2019

Client Authentication
RFC6749 uses Basic Authentication (client_secret_basic) or Form Parameters (client_secret_post). However, they are not allowed in FAPI. Only jWT-based or certificate-based client authentication.

JWT-based client authentication (RFC7523) generates JWT and passes it to the token endpoint using client_assertion. The JWT is signed using either (a) client secret (client_secret_jwt) or (b) client_key_jwt.

Certificate-based client authentication establishes mutual TLS connect to the token endpoint and the client certificate is presented for the client authentication.

Certificate bound access token.

A stolen bearer access token can be used. A certificate-bound access token is not.
In the case of a Certificate-bound access token, the client certificate used at the token endpoint will be bound to access token.

JARM
Reponse_mode=query.jwt, frangment.jwt, form_post.jwt, jwt. Does the enveloped signature instead of detached signature in the case of response_mode=code id_token

CIBA
CIBA introduces three new authorization flows: Poll, Ping, and Push.
This is a decoupled flow for user not in presence use-case.

Travis called out the danger of CIBA being phishiable due to the login_hint being required.
Nat mentioned that it is still going through formal verification, and all the holes will be closed during the process.
Several people predicted that in the end, it would become device flow.

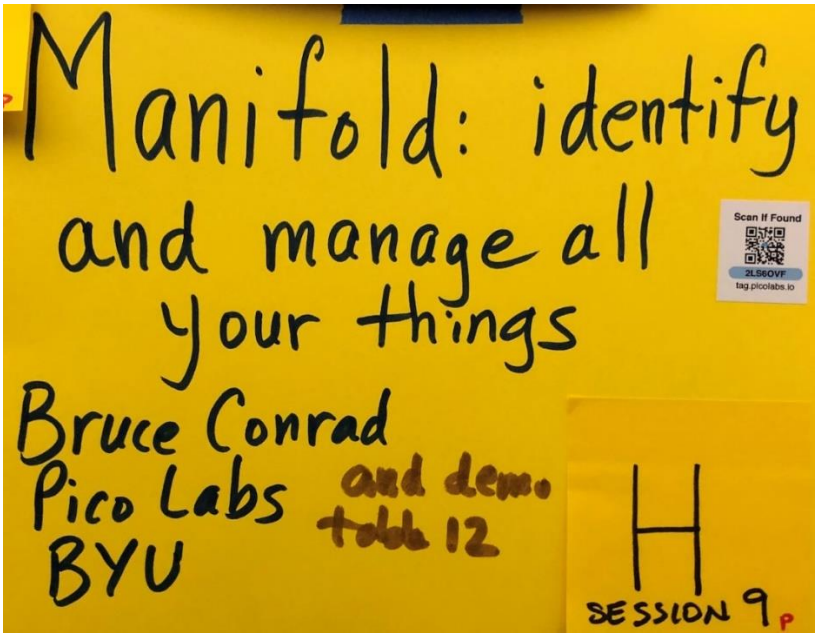
Manifold: Identity & Manage All Your Things

Wednesday 9H
Convener: Bruce Conrad
Notes-taker(s): Bruce Conrad

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

One person attended and we had a great QA session regarding mainly the technology stack provided by picos. Also demonstrated one-click access authenticated to sites with which the user (machine) has an agent-to-agent connection

We will keep in touch/ See little QR Code labelled "Scan If Found" in photo below. This was actually part of the idea that was discussed for the session.



Mark of the Beast? Religions Impact On Identity

Wednesday 9I
Convener(s): Alan Viars
Notes-taker(s): Alan Viars

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

This session was held to discuss general reservations and apprehension towards identity systems based on faith. It became quickly apparent that there are a number of subgroups of people who have a moral or religious objection to identity systems in general. The notes include key observations and mitigation strategies.

Key Observations:

- Our session did not have representation from all religious groups. We would love to have content added here.

- While no factual or statistical information was introduced, we identified that there is a particular aversion to identity systems in certain Christian groups.

- We surmised these opinions amongst certain Christian subgroups were more common in the United States than elsewhere. We also hypothesized here exists a geographic correlation coincides with these beliefs. (e.g. these views found often in the Bible Belt / Rust Belt).

- The Christian belief stems primarily from "end of days" prophecy. In particular, it comes from the Book of Revelation chapter 13, verse 17. "And that no man might buy or sell, save he that had the mark, or the name of the beast, or the number of his name". The gist to the relevant parts of Revelation is that it predicts that at the end of time there will be a single world order. People will have to take a "mark" of 3 6s ("666") in order to buy or sell. Any required identity system may seem a step in the direction of this prediction.

- A quick Internet search reveals apparent politicizing identity in connection with this religious imagery. The following example compares Obamacare with Nazi Germany.

- Aversion to identity systems is not limited to people with objections based on religious beliefs. There are many secular people who also have aversions to identity with similar thought patterns. Aversion arises from privacy and security concerns. The implication is that identity systems = being "tracked". They view identity broadly as "big brother". Many non-religious people share the fear that identity systems mean tracking and a loss of self-sovereignty.

Real World Effects

Some systems are designed not to hand out identifiers with "666". Some Examples:

1. A social security card cannot begin with "666".
2. A National Provider Identifier may not contain "666".
3. A notion of a National Patient Identifier has been gagged, but now https://www.modernhealthcare.com/politics-policy/house-votes-overturn-ban-national-patient-identifier

Ways to Mitigate Aversion Real World Requirements:

Some ways to mitigate aversion were discussed.

- Anytime participation in a system is optional, aversion is automatically lessened. This may not always be possible. Sometimes it's a hard choice. For example: Real ID. While a Real ID proofing is not required, not having it means you will be unable to board a commercial aircraft.
- Allowing people to choose their ID was cited as a way to people feel for comfortable using an ID system.
- Limiting information collected and disclosing its uses may reduce aversion.
- The concepts of decentralized identifiers and self-sovereign identity may work to combat aversion.

Consent is Broken: Privacy Implications for SSI

Wednesday 9J
Convener: Amanda Stanhause
Notes-taker(s): Amanda Stanhause

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

Slides: https://docs.google.com/presentation/d/18eFOj9JH7HTVzUZHio6tWrHjGTh2Vax5qBQ07ihV7Jo/edit?usp=sharing

Informed consent is broken: privacy implications for self-sovereign identity
Amanda.stanhaus@consensys.net

Creative Commons - I am comfortable at this level. Broad societal norms of what is appropriate and what is not? Instagram model and work for the government so keep things separate.

Explore options available vs defaults

No transparency today

First step is transparency and then can start writing tools to check

No way to give scoped consent today

Making transparency actionable / revocable

What is the tipping point

As society we aren't willing to pay for services we are receiving. Paying for it to go online by "informed consent"

Most people won't know what to do with it

We need some sort of agent or guide

Consent receipts and get delivered to some place. Then businesses analyze those receipts and give you recommendations.

You shouldn't be screwed over bc they don't care about privacy

Social contracts with different social media providers

To their user experience, it goes away but it really doesn't (content)

How do you even design consent in a rational way if you want it to be done right?

Sarah Allen Answer: if I want to keep data from a user, how do I keep it for them not just for me and I happen to be holding it for them and they can see all the patterns I'm tracking. Don't have hidden features.

A lot of data value is in aggregates.

Giving them data analysis that might relate to them or show them they are learning.

Big companies make money off of data.

Start ups can be disruptive if people like it better they don't make money off data.

These companies need to make sure this isn't a burden

we don't necessarily have to get people to care but make it as easy or easier than how it is now.

Compensation for user if company uses their data. But do I want them to do that with my data is in the first place? Even if I do get money for it.

Could also get coercive if people don't have money. So can only the rich have privacy?

We need to be pragmatic about the way approach privacy. Dangerous for us to assume all services on the internet should be free and take care of my data. More and more sites are putting up pay walls.

If you want content, you have to pay for it.

You are always paying whether in monetary or loss of your data. People who are poor are benefitting from free services.

The more data you give out the less valuable it is.

Looking at GDPR compliance where it is now and where it is going.

Should be illegal for parents to put kids on the Internet. Personas that cannot be tied back to kid.

AI looking at behavior but what defaults to start what AI is looking at

Can AI tell what my intentions are and act accordingly?

Browser plugin to look at cookie consent green to red.

Grades of privacy for search engines but trade offs for making this simplistic.

Camera surveillance you aren't owner of home but you are visiting friends so do they have consent to take video of you?

Where is the privacy violation? How long should they have it? Transitive if consent to record but then it goes to another company.

Should be a sign in front of house that shows consent.

CCTV example. Private person has been found bc of wrong installation for cctv camera.

Facebook messaging listening right now.

Consent makes illegitimate legitimate

GDPR consent is hardly ever a legal reason for releasing information. Monopoly on data then consent is not legal.

We will get smarter at defining and finding technical solutions for consent problem. Will it be normal populace?

VC's In The Supply Chain GSI

Wednesday 9L
Convener(s): Paul Dietrich & Gena Morgan
Notes-taker(s): Gena Morgan

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

GS1 Standards are considered the Global Language of Business. The GS1 systems provides for the identification of products, logistics units, entities, and locations among other things> GS1 standards also encompass data carriers used for capturing those identifiers linked to things as well as a standard interfaces for data sharing of transactions (EDI X12), product, entity and location master data, and physical event data (EPCIS - Electronic Product Code Information Services and CBV - Core Business Vocabulary.

Globally unique product identification and data about those products are core to GS1 and its constituents, which include over 2.5 million businesses. Indeed GS1 standards are used in 6 billion scans per day.

Online commerce has introduced new challenges for brands and retailers as they look to provide product data of the highest quality to their consumers. Online data about a product stems from many more sources today and it is not always from an authoritative source, leading to inaccuracies that can lead to a lack of trust with the consumer. Presenting quality authoritative data - from a multitude of the legitimate sources with a strong degree of trust is a challenge the GS1 community is looking to solve. This includes master data, chain of custody data and the like.

We reviewed the following use cases to gather feedback from the IIW community. The use cases included:
Product Data.
After some discussion and feedback perhaps we should look at this as a data provenance solve. There is so much data out there, stemming from so many sources that it is hard to get to the truth. Understanding the origin and provenance (and proving it) of any given set of data seems to be the tie in.
Some discussion and advice to turn GTIN into a DID scheme/DID method? Can the GS1 resolver return a DID document?

Chain of Custody.
Need to make assertions about the product that pass through multi-partners where you do not want to reveal identity of party but need to share an assertion about something. Proof linked to product (how is this done?)

Org equivalent as a person needing to provide credentials without revealing certain things about themselves. Pairwise DiDs (again)

Credentialed supply chain could move independently from physical supply chain -- requires serialized identity.

Can we apply pairwise DIDs and ZKP? Need identification at the unit level.

Cross perspective of credentials is what makes the supply chain more trustworthy. Combination and comparison of assertions.

Asset becomes single source of truth - permissioned access to different levels of info about the product because there is data you need to reveal about the product and zero knowledge proof

Two experts believe ZKP could help share supply chain data without revealing identity (supply chain use case)
Drummond - 2 efforts in Canada regarding multi-tiered supply chains - Clean Energy supply chain work in Canada (John Jordan). Harvest One - Cannabis Supply chain (GS1 Canada)

Peer-wise DID relationship, the DID becomes the identifier for that party - no VC needed because DID proves identity. Output of onboarding process

Supplier On Boarding. Most straight forward use case and indeed is the foundational use case across many of the solutions here. Not necessarily all focused on "supplier" onboarding, could be a bank customer, someone getting a driver's license, etc. But the point is there is a requirement to get some entity (a person, an organization… I wonder if a thing) "set up" in the system. Today the process is often layered, paper based or requires some form of data gathering from multiple places. This aims to digitize and streamline that process. Additionally, the entity maintains and then shares their identity, versus having their identity owned by multiple organizations. Novartis has started with this use case as well. Although the direct tie to GS1 may not be as direct - except for GLN being a credential perhaps, this may be a good PoC to start with as it seems to be common issue. It would allow us to explain some otherwise complicated concepts (decentralized identity).

GS1 is looking to explore these use cases and the value decentralized identity and VCs may bring with any number of partners in this space. The goal is to understand the benefits and value in layering this technology into the existing system, but also the requirements – of individual companies from a systems and process standpoint, of industry – from an adoption and use standpoint and of GS1 from a governance and central root of trust perspective. This is all in a drive data quality and trust in the supply chain – in the digital world.

Please find the session presentation here:
https://drive.google.com/file/d/1AKoxkcmJoElBY-LI4-1d-12tfVlE3-rg/view?usp=sharing

KERI (Part 2): Universal DKMI Events Primitives Witnesses Architecture

Wednesday 10A
Convener(s): Sam Smith
Notes-taker(s): Sam Smith

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

Link to Slides Presented:
https://github.com/SmithSamuelM/Papers/blob/master/presentations/KERI2_Details_IIW_2019_B.pdf

Understanding & Implementing Peer DIDs in 60 Min or Less

Wednesday 10B
Convener(s): Daniel Hardman
Notes-taker(s): Daniel Hardman & Alexander Tam

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

Notes from Daniel Hardman:

We reviewed the following slide deck: https://docs.google.com/presentation/d/1T25zaBt__s3Y0vGJuFrh2yTKw-22IwykN_ONHwbbNo0/edit
Short summary: You can implement peer DID support in your codebase in 60 min or less--maybe in just 5 or 10 min in python or node.js. We talked about the tradeoffs that peer DIDs make, what they're good and bad for, and how their authorization mechanism works.

For more info, please see:
http://j.mp/peer-dids-group
https://openssi.github.io/peer-did-method-spec
github issues at https://github.com/openssi/peer-did-method-spec
https://github.com/evernym/pypeerdid (ref impl of layers 1 and 2)

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

Notes from Alexander Tam:
slide 1

- most did methods have a relationship between two parties that is mediated by did control
  - eg. bob and acme want a pariwise relationship
  - acme would have a public did (green), pairwise did: A.did@A:B
    - register and update on central source of truth (eg. blockchain, facebook servers)
  - bob would have a pariwise did: B.did@B:A
    - register and update on central
  - acme can resolve B.did@B:A
  - problem:
    - everyone can resolve that did, can be a security issue

- don't need the public resolution (resolve) for pairwise did

slide 2
- same idea without central source
- bob creates pairwise did and registers and updates it with acme
- acme does the same

- idea simple, but execution can be difficult

- comment

- peer did have different features than public dids
  - no discovery
- can have multiple key pairs in a relationship
  - eg. bob has many devices all connected with acme
- groups?
  - two ways to do groups
    - hub and spokes model, talk to hub and hub routes message to correct person
    - n-wise model, all members enumerate all other members in the group (direct commuication)

slide 3

- why interesting?
  - all listed items in slide

  - trade offs
    - no discovery
    - others

slide 4

- how to create?
- solution is a pull request at the moment

- *stuff on slides*

- identifier of numeric base algo, for backward compatability

- self certifing identifier

- guuid instead?
  - no, cause you can't prove the person using is the one it was assigned to
  - no proof at beginning at chain of custody

slide 5

- how to share

- *stuff of slides*

slide 6

- 3 layers of support
- layer 1
  - be able to recognize a valid did, can do if you understand regex
  - trivial

- layer 2
  - can accept and give static peer dids (static = can't update)
  - few hours
  -
- layer 3
  - complexity of decentralized protocol for state of updates (key rotation)
  - DIDcomm + week

can have a mismatch of different did definitions, or different of static and dynamic did
  - just have to communicate that you are using static or dynamic when communicating
  -
- comment
  - can't have did in diddoc since you generate did after

slide 7
- *stuff on slides*

- open issues
  - look at repo on github

comment
  - if only static, why need dids
    - case 1: flow with normal dids, would be annoying to switch to public key
    - case 2: need ability to distribute trust
      - eg. need 3 of the 5 keys to do operation, cant do with public key
  - didkey vs peer did
    - use ssh key in a did context
    - missing characteristics that are present in peer did
    - daniel has a spreadsheet showing why use peer did

- going through code on first page slides
  - line 12 is layer 1
    - just a regex line
  - line 14 - 17 is the resolver
  - line 23 -34, one liner of getting did from doc
    - raw bytes, sha52 hash, prepend a byte (multiple codex), base58 encode
  - line 76 - end, authorization of identity controller
    - reason why you don't just use public key, code is how to do 3/5 keys needed

slide 8
- update peer did's did doc

- delta says
  - add this key
  - just delete id

- *stuff on slides*

slide 9
- json showing profiles and rules, can make as complex as you want depending on the context
  - eg. phone was stolen, what do I do

slide 10
- crdts, same tech that allows multiple people to edit a google doc
  - conflict free replicated data types
  - look on wiki

- doesn't solve all problems but a lot of them

slide 11
- agent knows pending change but hasn't been endorsed yet, so you can gossip about it before it's true
- eg. need 3/5 keys, first key to endorse is pending

- send all changes along until enough have accumulated to pass

slide 12
- include state in communication so they know if they are out of sync

slide 13
- skipped

slide 14
- more info
- peer did discussion gorup, first link

- last link is peer did implementation in python

- comment
  - permission and auth are built into did methods, so no need to put in diddoc

  - peer did is a method spec not a protocol
    - for exchange use aries protocol
    - or roll your own

    - spec says how dids look and have certain security properties

  - aca py is not yet compliate with spec

  - if can't reach bob, on failure what happens?
    -

- going through an example of the gossip protocol (not in slides)
  - see how gossip works if communication is blocked between certain parties
  - state becomes out of sync, however as soon as another party that got the update starts to communicate with the out of sync parties, the in sync party brings all the out of sync parties into sync since state is shared with communication
  - ordering is not enforced, making it not a ledger

- did is associated with genesis version only, have to use deltas to get new doc

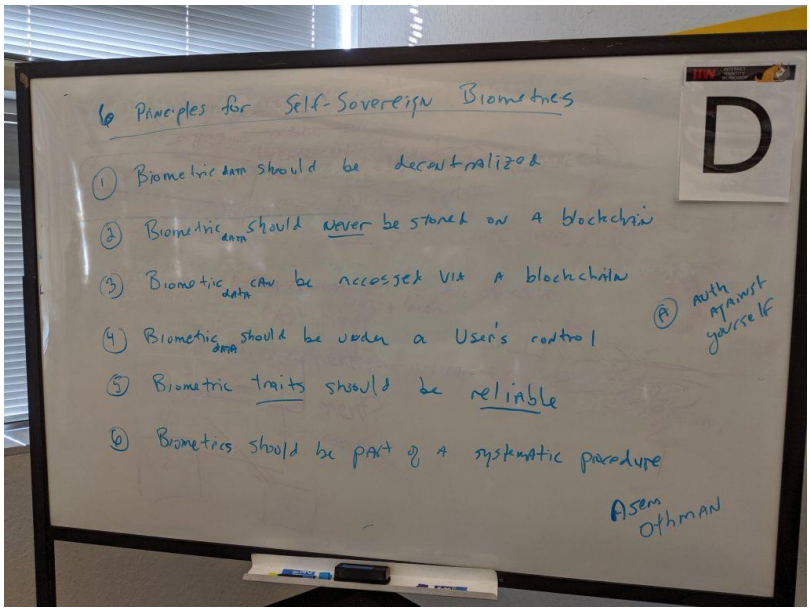
- public reputation and discovery are reasons for public dids

Finish RWOT 6 Principles for Self-Sovereign Biometrics

Wednesday 10D
Convener: John Callahan & Kaliya Young
Notes-taker(s): John Callahan

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

Link to Biometrics Draft Document:
https://github.com/WebOfTrustInfo/rwot6-santabarbara/blob/master/draft-documents/Biometrics.md



Browser Changes (SameSite, ITP) Affecting Identity on the Web

Wednesday 10F
Convener: George Fletcher
Notes-taker(s): George Fletcher

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

You can find the deck published here:
https://openid.net/oidf-workshop-at-verizon-media-september-30-2019/

A Machine Learning Perspective on Data About Me

Wednesday 10G
Convener: Adrian Gropper
Notes-taker(s): Scott Mace & Adrian Gropper

Tags for the session - technology discussed/ideas considered:
Machine learning, big data, privacy

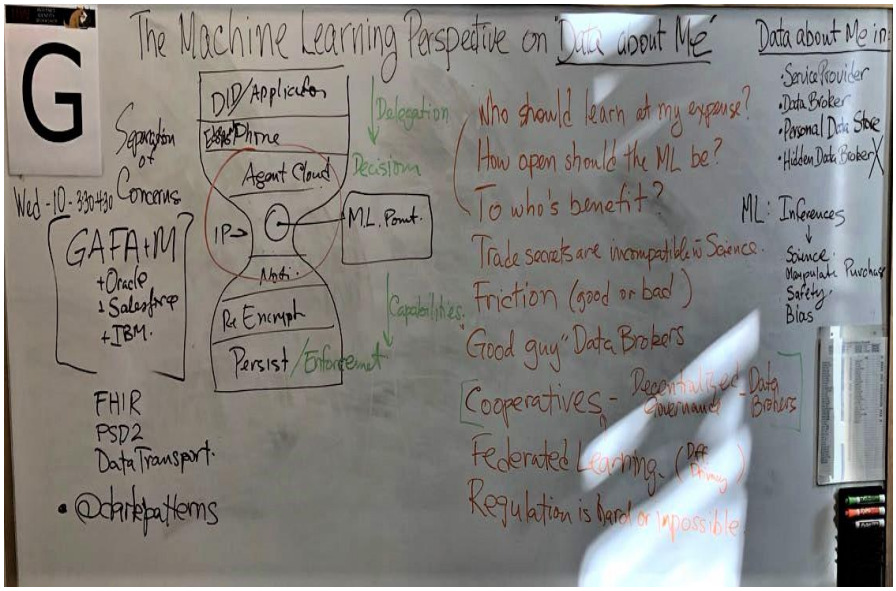
Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

The ML perspective on data about me / Adrian Gropper: Platforms are trying to add even more value. Look at your phone. Apple or Android. Microsoft couldn't get into it. That's an extreme case.

Now something is happening in Washington and with standards development.
GAFA+M+Oracle+Salesforce+IBM.

As industries develop useful ontologies, APIs like Amazon no longer have to sell stupid bits, they look at the data and add value, based on inferences based on ML.
With ML inferences, advance science, manipulate purchases, safety.
Who should learn at my expense?
How open should the ML be?
To whose benefit?
Trade secrets are incompatible in science
Friction (good or bad)
"Good guy" data brokers
Cooperatives
Federated learning, a way of dealing with who should learn at my expense
Decision points, enforcement points (from policy)

Photo provided by Adrian Gropper:



High Assurance OAuth/OIDC Profiles for Government Use Cases

Wednesday 10H
Convener(s): Mark Russell
Notes-taker(s): Mark Russell

Tags for the session - technology discussed/ideas considered:

- OAuth 2.0 Mutual-TLS Client Authentication and Certificate-Bound Access Tokens
- OAuth Token Exchange
- OAuth Assertion Flow

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

We discussed high-assurance requirements in certain types of government environments (e.g. intelligence, defense, etc.) and the current security architecture which is heavily dependent on direct client TLS authentication of users and systems. I described a current US Government effort to profile OAuth 2.0 and OpenID Connect 1.0 to create a suitable security profile for this environment. Government-specific concerns and considerations include:

- Existing robust and highly capable PKI, which should be taken advantage of
- Strong concerns over the use of bearer tokens - requirement for some form of proof-of-possession
- A requirement to provide assurance information in authentication assertions (e.g., via OIDC)
  - Specifically, a requirement to convey the Identity Assurance Level (IAL) and Authentication Assurance Level (AAL) as defined in NIST SP 800-63-3
- A desire to tighten requirements around basic security parameters - cipher suites, assertion signing algorithms, key sizes, lifetimes of tokens and codes
- General distrust of the front-channel
- Aversion to dynamic registration
- Aversion to JWT-based authentication, primarily because clients will generally already have client TLS credentials

The US Government would ideally like to engage with existing OpenID or IETF working groups if possible to define a public standard that is not government-specific.

The group discussed these security requirements and there was agreement that many of these requirements are in line with general high-assurance requirements in other areas such as finance. Some of the differences between FAPI and the US government profiles were discussed, and also the fact that some aspects of FAPI may be revised based on changing requirements. It was broadly agreed that the US Government profiling project should engage with FAPI to identify common ground and potentially work towards a FAPI high assurance profile. Potential engagement at the IETF Security Working Group meeting in Trondheim was discussed.

We then discussed an additional government use case involving chained service calls, in which an OAuth PR needs to call another PR (which may in turn call another) where each node in the chain must be aware of both the end-user's identity and the identity of all systems in the chain of calls. In the simple case, these calls occur within a single security domain, all PRs trust the same AS, and token exchange can be used in a straightforward way. In the cross-domain use case, additional considerations come into play. The group generally agreed that both scenarios were solvable with various solutions that entail different trade-offs.

Workshop: Universal URI for Deep Linking In All SSI Mobile Apps

Wednesday 10l
Convener(s): Alexis Falquier
Notes-taker(s): Alexis Falquier

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

Universal deep linking for SSI mobile apps

-Protocol vs Address Mapping

-Mix of both through a page that tries to handle the protocol (html first then protocol)

-protocols asks user which app to open

-Option to register address as well

-address mapping should resolve to a site that follows a set of standards of what instructions are displayed

-Invite generating entity maps to an address of their choice, they can define what is on there as long as they abide by the initial set of standards that are defined in the spec

RFC to be made

Intro Page Requirements Spec:
-launch page that tries to launch the protocol handler
-if protocol handler fails, present a user friendly guide to install a didcom compatible wallet (which wallets are displayed is up to the sender)
-Provides link or QR code for once the wallet is installed in the same page
-Page must allow to copy the message to then be pasted or saved according to wallet capabilities
-if URL shortener used, information should not be disclosed and shortener should not persist longer than x
-?a way for the page to validate the message and make the recommendations accordingly?

^wallet spec may need to add copy/paste capabilities

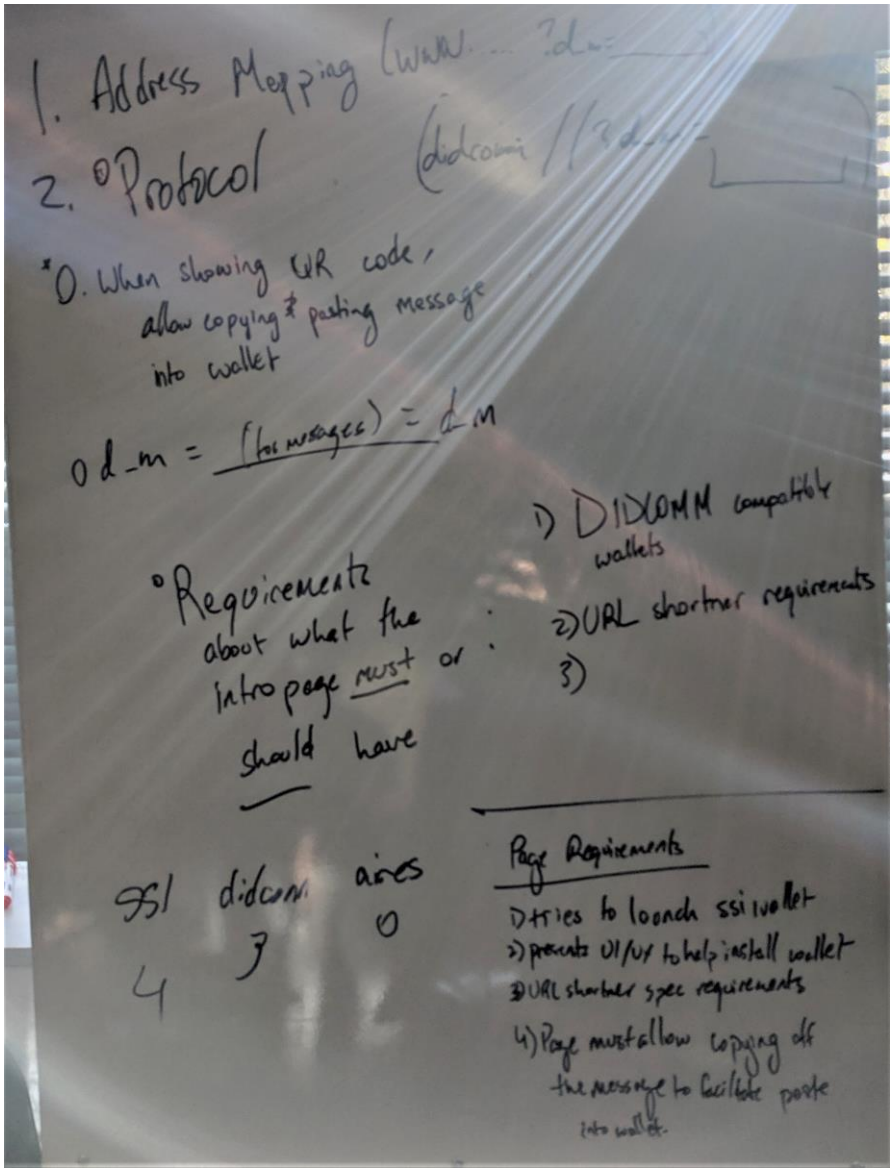
(URL shortner might need be a separate RFC spec in it of itself)

Message requirements:
-message URL query d_m meaning didcom_message for universal message availability
-JSON base64 URL encoded messages
-JSON must be in the shortest form possible (no extraneous white spaces)

Deciding which Protocol URI to use
SSI vs DIDCOM
SSI wins
wait nevermind:
DIDCOM

Why DIDCOM: less political, the message sent will inherently be a didcom message

RFC to be revisited when all common platforms support didcom spec then instead of http first, protocol takes precedence



"I Am Spartacus!" Privacy Via Obfuscation For Vulnerable Populations (Victims of Abuse, etc)

Wednesday 10J
Convener: Mike Kiser
Notes-taker(s): Mike Kiser

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

Link to open-source tool discussed: https://github.com/derrumbe/Spartacus-as-a-Service

In addition to the below content, we discussed how this could be useful to immigrants (U.S. visa application requires 5 years of social media accounts), victims of abuse needing to relocate, and journalists who report on topics that those in power would rather not gbe investigated.

1) Spartacus, Kirk Gibson, and the Right to Privacy Retelling of the ending of Spartacus as inspiration for the right to privacy through obscurity. [see: https://www.youtube.com/watch?v=-8h_v_our_Q for entertainment and informative purposes.]

(2) Use Case: Seeking to be Forgotten Follows the difficulty of users to remove accounts and data from online networks and applications, using a sample identity as a typical use case.

> (a) A sample identity was fabricated (name, photo, backstory, etc). Note that this kind of wholesale creation of identities is much easier now with sites like http://thispersondoesnotexist.com . Accounts for this identity were created at 26 different services representing a wide swath of online activity:
> • Ashley Madison • Bumble • Dropbox • Evernote • Facebook • Gmail • Google • Groupon • Instagram • iTunes • LinkedIn • Medium • Myspace • Netflix • Pinterest • Skype • Soundcloud • Spotify • Steam • Tinder • Tumblr • Twitch • Twitter • WhatsApp • WordPress • Xing • Yahoo
>
> (b) Summary findings are shared based off of these systems ("How many sell your data?" "How many let you retain rights to your creations?" . . .)
>
> (c) Content was then produced for these online systems and resulting search results and targeted advertising were noted (based off of this activity). (d) An attempt was then made to delete all accounts and their data (with mixed results depending on the target service.)
>
> A wide swath of success and failure comprises this set of services. Some are forced to retain some information even with an account delete request—particularly those that are commercial in nature. Other sites may also have already mined these sites for data (photos, other collateral, etc.)—rendering account deletion relatively unhelpful. More regulation is shown as not being that useful, either, given existing retention requirements and the difficulty of enforcement / incentivization.

(2) Inadequacy of Privacy Legislation Super brief overview of current legislation, showing how it widely varies around the world and the lack of protection, along with daily headlines, is encouraging people to delete their online information/accounts and value their privacy more highly.

The lack of adequate legislation and the current tendency of enterprises to misuse personal data and sacrifice privacy leads to the need for an alternative that would "encourage" these services to provide deletion of data and accounts.
In short, a better way is sought, which leads to . . .

(3) Privacy Through Obfuscation

(a) The goal is obfuscation of the "real" person or data. This is done through injection of additional accounts or data that creates false positives in the environment and creates confusion as to who the real person or data is.

[see https://mitpress.mit.edu/books/obfuscation for a solid background on obfuscation techniques]

(b) Many of these techniques are also based off of previous research done on location obfuscation:

[e.g. https://link.springer.com/chapter/10.1007/978-3-540-73538-0_4
Ardagna C.A., Cremonini M., Damiani E., De Capitani di Vimercati S., Samarati P. (2007) Location Privacy Protection Through Obfuscation-Based Techniques. In: Barker S., Ahn GJ. (eds) Data and Applications Security XXI. DBSec 2007. Lecture Notes in Computer Science, vol 4602. Springer, Berlin, Heidelberg]

(c) Three primary techniques explored:

a. "Enlarging the Radius" —this technique constitutes the creation of additional identities / accounts on the target system with the same name but slightly different personal data. This enlarges the pool of potential targets and helps to preserve the privacy of the original identity. ("one name, many accounts")
b. "Shifting the Center" — this technique employs the creation of additional identities / accounts in such a way as to bias the peer group into a different center—one that no longer focuses on the original identity, but one that makes the original identity an outlier. This is primarily focused on a common photograph or other visual marker, with the other data varying per account. ("one photo, many accounts")
c. "Filling the Channel with Noise" — a technique which floods the existing account with extraneous false data to help mask the real data. (e.g. Liking various activities or postings on Facebook as a cover for real preferences.) [see this previous research for more information: http://www.kevinludlow.com/blog/1610/Bayesian_Flooding_and_Facebook_Manipulation_RD/]

Note that flooding the channel is site dependent – for example, Facebook restricted the ability to put in bogus content into a user's account in 2008 (but they still left "life events" open to manipulation). By contrast, Twitter still allows for the programmatic flooding of accounts with content. Others are more restrictive. Polluting past search results for engines such as google is also possible. Each app or online site may call for its own technique to ensure obfuscation.

(4) Presentation of an open-source proof-of-concept is introduced that facilitates these obfuscation techniques. Named, for obvious reasons, "Spartacus as a Service." This will allow for automatic obfuscation of a chosen identity on a small scale, and lessons learned from its usage will be discussed.

a. Current version of Spartacus as a Service may be found at:
https://github.com/derrumbe/Spartacus-as-a-Service

b. It is an open-source tool written largely in Node.js under an MIT license
c. Development is ongoing, and this is expected to be a long-term project (first official release would coincide with BlackHat/DefCon)
d. Authorization for obfuscation is done via OAuth for a signed in user (explicit consent is therefore given)
e. Additional resources have been incorporated to accommodate this content. A Markov chain is used to generate new content based on a textual repository (ranging from political platforms to the oft-used Jane Austen canon to Aaron Franklin's book on BBQ (he's a big deal here in Austin.)) Amazon Mechanical Turk may be used to circumvent bothersome pieces such as captchas.
f. Note that this is not a tool that *prevents* targeted advertising and the like, instead it seeks to dilute the value of information that companies know about a user, masking the true information from the fake, so that it is impossible to tell what the real content (or in some cases, who the person) actually is.

(5) Results for these techniques are examined, with primary results being search results and targeted advertising rates / topics. (with baseline already established from the original identity.)

(6) Finally, lessons learned from obfuscation will be discussed, as well as the practicality of this technique going forward. (Spoiler alert: it's not practical at scale, for a few obvious reasons.) But false personas might be a thing in the future, much like many people use burner email addresses (see apple's new email proxy service, for instance.) [What it should do is push the consent receipt concept - empower people to know and control what they've shared w/o it being sold off

The Trust-Over-IP Stack:A Path to Global Interoperability for SSI & Verifiable Credentials

Wednesday 10L
Convener: John Jordan, Province of British Columbia; Drummond Reed, Evernym & Sovrin Foundation; and Chris Buchanan, Mitre
Notes-taker(s): Drummond Reed

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

First John gave an introduction that the solutions we are developing with SSI (self-sovereign identity) are actually much bigger than identity—they form the infrastructure required for a trust layer for the entire Internet. And this "interoperability stack" bears a strong resemblance to the TCP/IP stack that is what produced the Internet itself. That's why John coined the term "Trust over IP" (ToIP) for the stack that has emerged.

Drummond then presented this set of slides that show the progression from the previous models of identity into the SSI stack and then the ToIP stack.

Finally, Chris shared his hypothesis that government customers are going to want to start making purchase orders for "SSI compliant" solutions and the industry is going to need to have a way of certifying solutions as being "true SSI". We had a long discussion about this because there are many such tests, including the Decentralization Rubrics that the W3C DID Working Group is going to be publishing. So it may be difficult to come up with a single overall certification. However Drummond made the point that the individual layers of the ToIP stack could each have certifications against specific governance frameworks developed for each layer.

Drummond closed by sharing that anyone interested in this work is welcome to join the Sovrin Governance Framework Working Group—it is open to anyone to participate.

Notes for Thursday / Sessions 11 - 15

Are We Boiled Yet?

Thursday 11A
Convener: Alan Karp
Notes-taker(s): Alan Karp

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

Notes from Alan: https://alanhkarp.com/SecurityRant.pdf.

LifeScope: Meet Your Digital Twin (Data Hub/DB/Wallet + Identity + Cred + Me2B)

Thursday 11B
Convener: Liam Broza
Notes-taker(s): Liam Broza

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

Link to the original notes provided by Liam:
https://www.dropbox.com/sh/nog9lwofd6ztkym/AABX2TXj3aUKl6GY6w3HssQ1a?dl=0

- LifeScope started as a personal desktop Java app in 2010 named SmokeSignal
- Introduction to the current LifeScope team and asking for more collaborators.
- We went over the existential problem of trust and control of our data.
- Went over simple descriptions of SSI, Credentials, and Data Proofs
- Went over the history of projects similar to LifeScope: PDMs, PKMs, Solid, Data Wallets
- Reviewed our current lack of biodata, HIPA, and our future plans for medical data.
- Went through a demo of the LifeScope app and platform.
- Reviewed our current API and OAuth implementation.

Discussion continued in afternoon session 12I: LifeScope.io Digital Self (AI, HUB, DB, DID, SSI)

If you are interested in contributing to LifeScope.io, please reach out to liam@lifescope.io

Platform Architecture: Building The Back Ends & Systems That Support AS Servers. State? Scale? Price? Persistence?

Thursday 11G
Convener: Adam Hampton
Notes-taker(s): Neil Thomson, Query Vision

Tags for the session - technology discussed/ideas considered:

Performance, User vs. app/service Authentication, Scalability

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

The application context is a Multi-Tenant, SAS, Cloud application w Open ID Connect, with RP's, AS, Resource (API) Servers, utilizing Hardware Load Balancing, Service run-time data caching and persistence where multiple instances of the same service component exist

Also assumed was a Continuous Development/Deployment cycle were new software instances are hot swapped, with Load Balancing doing the swap out by redirecting all traffic away from the instance to be updated allowing all requests to complete, swapping in the updated instance, waiting for it to indicate to the LB that it's ready, then doing the same with other instances.

Issue with swap out is the preservation of state and related data which typically will be done with RAM cache on a separate server, with disk backing with replication across instances of the same service. Replication, sync … of the state cache is the responsibility of the cache service. Examples including MemCache, Redis

Scalability notes

For JS clients, including SPA's, which can be treated as static pages, solutions like CloudFlare can significantly improve performance

Scalability model is more boxes (Horizontal) vs. bigger boxes for app, cache and non-relational db components. If Relational is used for the persistence model, is mostly Vertical (bigger boxes) with up to 2 instances (or 2 pairs if primary/hot standby structure)

Between the RP, AS, Caching and persistence servers, in 2019, all communication is via HTTPS or (where possible) Mutual TLS. The idea of terminating HTTPS at the RP (tip of the "stack") is no longer sufficient.

The stack of service, cache should be pairwise for each instance.

Each service should be responsible for their own persistence which should be independent (and can be independent technologies)

An example of scalability via caching (see green on the diagram) is where a (reference) token is validated with the AS, which returns the actual access_token in JWT form or the JWT contents by the token_inspection_service , which should be cached by the service, with an expiry that matches that of the access token.

An unresolved issue is the "big red button" revocation of a user's sessions (or multiple user's session) in the case of lost/stolen device or credential compromise. OpenID Connect does not currently define a full

featured workflow, capabilities, etc. for the Revoke scenario.

It was noted that it is not sufficient to remove the OIDC tokens, the application must immediately purge all data, data presentation or transaction – all of which may be beyond the OpenID Connect workflow and control (app specific behavior).

Possible CAEP has a mechanism (or should develop a mechanism) to cover this scenario.

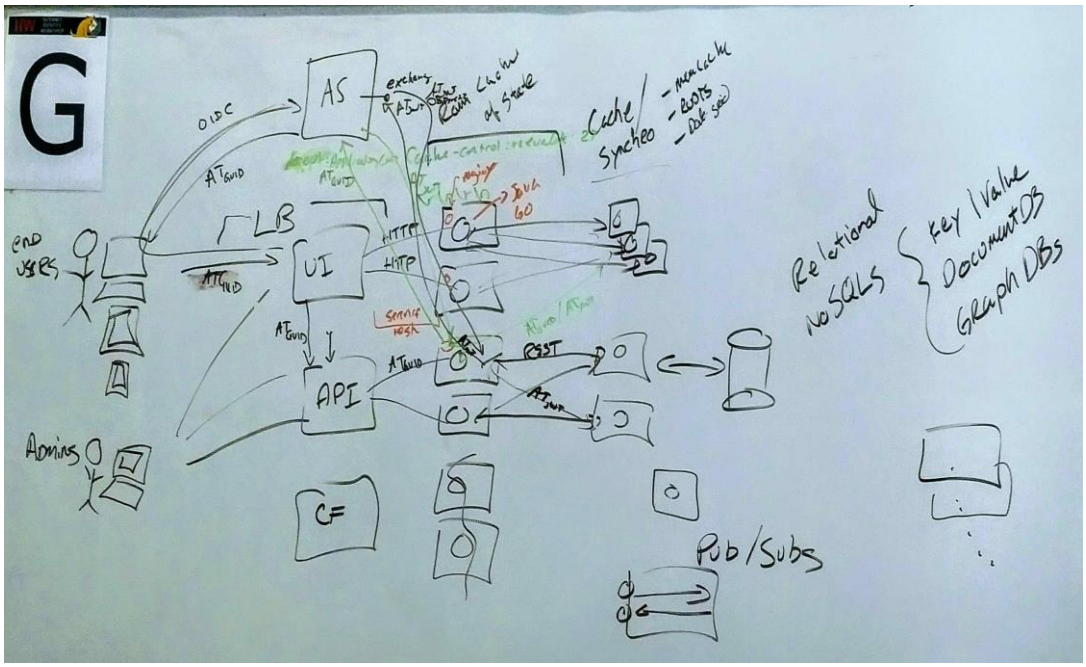
Different persistent store technologies were reviewed, including SQL and no SQL, including Key/Value, Document DB (Mongo DB) and Graph DB.

Key requirements for technology selection and scalability:
The "query" profile – what type of queries (extract) and create/update/delete
The volume of each (over time, including peak times)
Read/Write balance (e.g. mostly read or equal read/write)

Cautionary tale of not knowing the impact of operations on performance/scalability – Kafka Topics have a very high cost to create and delete, which was not known until after implementation, which had consequences

Authentication "Reach" - User authentication should only be used as deep in the stack as required where the user related privileges apply. Past that point service/machine accounts should be used (service to service).

<Photo of Whiteboard Below>



Pico Agent In A Tab One Click to Identify?

Thursday 11J
Convener(s): Bruce Conrad
Notes-taker(s): Bruce Conrad

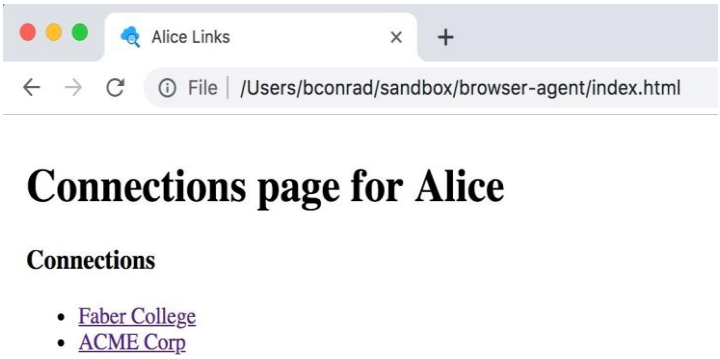
Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

I invited Sam Curren to join us and his contributions are hereby acknowledged.

We began with the end in mind.

Alice, who has a relationship with Faber College, goes to their website and
is recognized as Alice. *Just one click*.

Alice Links page shown here. It is a simple UI face or surface for her agent, which is running inside this browser tab.



The agent here surfaces one link per agent-to-agent connection which involves a web page.

Faber College page which opens up when Alice clicks on that link in her connections page.

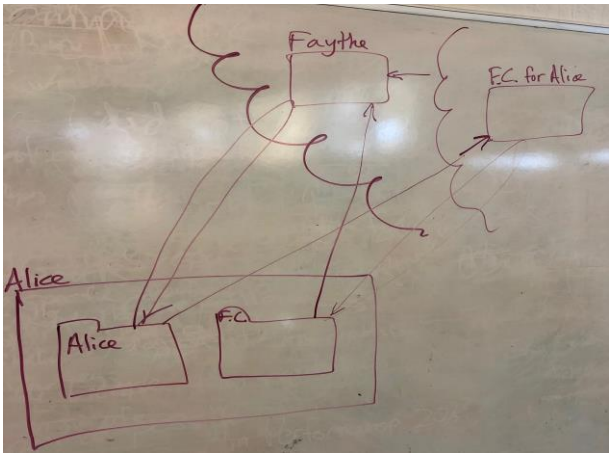
Notice that Alice is recognized, because of the pre-existing agent-to-agent connection between her local agent and Faber College's agent.

Mallory, looking over Alice's shoulder (physically or by network package sniffing), tries to impersonate her (simulated here with an incognito browser).

When it is Alice, Faber College recognizes her. Anyone else using the same link will not be recognized because they do not have possession of Alice's agent.

The fragment portion of a URL is not (normally) sent to the server, although some browsers do this. Even so, it is of no use to Mallory.

Sam described routing agents, and we came up with this diagram.



Two agents are operating inside of Alice's hardware domain. A local tab has Alice's agent in it, but a tab with content from Faber College (F.C.) has Faber's agent for Alice's machine in it. Both require a routing agent (because Alice is using a hardware edge device).

Alice (her local agent) accepts an invitation to connect from the F.C. agent and a connection is made between them. The URL fragment (introduced by the "#" character) consists in this prototype of simple the DID for Alice's side of that connection. The F.C. homepage uses that fact to recognize Alice. The same DID used by anyone else will not "work" because the attacker will not have an agent with a connection to F.C. using the same DID.

We then had a very interesting discussion of how this might be applied to a call center application to pre-flight a voice conversation. This was largely between Vic (of HearO) and Sam, and was fascinating. Hopefully it will continue, perhaps over lunch.

Identity For All (2): How Can Tech Present At IIW Help w/Digital Identity For Marginalized Populations?

Thursday 12A
Convener(s): Kristina Yasuda
Notes-taker(s): Pam Dingle

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

Identity for All – Part 2

- How can we address these situations with technology
- recognition w/o tracking -- not storing direct biometrics
- identify abuser/explain (eg an abuser is in an aid organization)
- revocation of contributed identity
- identity reconstruction
- trust waterfall
- Adaptation to local tech situation

Recognition w/o Tracking
- Cancellable biometrics
-- store template not actual picture
-- ISO industry standard for this - SC 37
    - Name is changing from "cancellable biometrics" to something

Trust Waterfall
- guardianship of credentials in the cloud -- SpacemanID
-- "paper sovereign" or series of words

Readouts from Breakout Groups

Privacy vs Belonging
- tensions between privacy and need to belong
- local laws will require certain disclosure - this is a reality
- disclosing more than legal minimum becomes a need for convenience
- self-sovereign identity - what techniques can be applied for preserving privacy in that legal context
-- facial recognition: emerging trend that invades this sense of privacy
-- other modalities such as 2d face or 1 finger makes sense for some things but 3d face or iris are important for others
--- best practice is to store as little as possible in actual databases, eg identifier + template only

Recognition without Tracking
- Looked at a use case:
    European refugee management - discussion on organization and efficiency versus privacy, in certain circumstandces privacy may need to be given up in pursuit of getting urgent access to services
    What is more important? Immediate support or maintaining privacy, even if technology is amazing?

- Legal situation when someone applies for status multiple times in multiple jurisdictions - what happens if someone has already enlisted to start the process? if they are rejected? Should that information be shared?

In the case of doctors without borders - if medical record is created, could that record be linked to the person as they travel through camps?

Trust Waterfall - another word for web of trust
-- Use case for migrant workers trying to get credit
- two things to counter abuse in a peer-to-peer systems
1) ZKP zero knowledge proofs - I can attest to abuse without being identified
2) Notable member of community/chief of tribe can influence reputation positively

XYZ & DID Deep Dive

Thursday 12B
Convener(s): Justin Richer
Notes-taker(s): Sam Curren

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

http://oauth.xyz

Transactional Authorization.
Oauth has always been a transactional protocol.
Send user to get token, use token they bring back.

Send Tranasction Request
- info about who you are, what you are capable of, etc.

Get Transaction Response
- do your stuff

How you can prove yourself.

Starts in backchannel, as opposed to current practice of starting in the frontchannel with the user.
Can Request interaction with the user if necessary.

Similar mechanisms to Oauth.

Can pass information about the user.
API client is a wallet with access to Verifiable Credentials or similar.
It makes sense for the client to pass information about the user to avoid unnecessary user interaction.

This is Transaction Oriented rather than Resource Oriented.

It isn't about the client.

Like a user interupt, but with allowances for automated responses that may help solve the problem without direct user interaction.

How to prevent unintended data leakage?
This is going to the Auth server, not the resource server.
We will have to be careful to not leak data during that flow.

The transaction is intended to be stateful.

What is a token except the result of a transaction.

Audit trails.
might be a place for ledgers.

We can give it it's own identifier, and refer to it or record it within ledgers or within DIDComm protocols.

Use Verifiable Proofing as part of a user assertion.

We may want to allow multiple user assertions.

Interact can be browser but can also be wallet interaction.
Interact can also be a proof request or a didcomm message.

XYZ intends to generalize already explored patterns with CIBA etc.

XYZ has a looser model for model passing related information.

The resource section has semantic support to describe the resource you are requesting.

Can we bind a DID key (URI ref) to the HTTP Request?

Do ZKPs apply for http request signing? Probably Not.

Verifiable Credentials for Mobile Skills Schemas & UX

Thursday 12D
Convener: David Masen & Chris Winczewski
Notes-taker(s): David Masen

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

Note of clarification: "mobile skills" refers to transferrable/portable skills, not handset-based skills.

Overview:
"Skills as currency" — allow individuals to curate their own diverse skills, eventually in an SSI way, that can be exchanged within large organizations and across organizations, from very formal, a university degree, a course, to soft skills that are assessed based on work experience
Examples: Data science, writing, collaboration, empathy, creative thinking, storytelling, analytical, ability to learn (growth mindset), adaptability, flexibility

Working with institutional partners who have their own stacks and taxonomies
- user groups inactive
- bootstrapping exchangeable naming, or will it be wild west?

Schema discussion:
Priorities:
Discoverability
Start simple
Relating many taxonomies

Let's talk about:
- use features of linked data?
  - not to create an AI but to build on and create consistently relatable schemas (eg schema.org)
- skos/definedterm?
- same as, subclass of, is level?
- put schema on ledger? (stack dependent)
- or -
- orgs and vendor defined, fully ad-hooc

VC W3c recommendation good, but not enough - completely different languages, even simple ideas like start dates aren't easily relate-able
Simita: User groups? Is it a standards bodies task? Focus is on DIDs
Anthony: European commission XML - transferrable to US?
Sumita: translate between them, organically, use Linked Data
Open badges - IMS Global?

- Proprietary perspective
- Not easily interchangeable
- Companies moving faster than them
- Healthcare - EPIC (proprietary) - can't exchange patients
    - Use federal intervention

Who to talk to about why or how to use JSON and develop structural content:

- Similar scope research projects that had rich "semantic web" models, eg DARPA
- People in W3C, key companies like Digital Bazaar
- Google
- Library science people
- Hiring sites - toptal, etc

How do we organize, do we try to align in a year?
Where is the best place?

- Interop project in the DIF (claims and credentials)
- Survey of group (about 12 people):
    - Half people are DIF members
    - Half are w3c-focused
    - A couple Hyperledger Aries focused
        - Join technical group (using json-ld)

Chris: 3 areas
Interop working group, focus on DIF/hyperledger aries (not w3c). They are converging?

- Hyperledger aries - Wednesday meetings
- DIF not open enough?
    - Interop meetings - public repositories, weekly calls, looking for do-cratic approach

UX discussion:

- Experience of SSI so far is pointing a smart phone at a QR Code
- Streetcred
    - -deep linking to applications
    - No out of band, DID communication
- Need a wallet
- “Choose your wallet” screen in apps
- Wallet at an operating system level?
    - Samsung working on DID/wallet at the mobile device level including hardware level (trust zone/secure enclave)
- Impossible on IOS?

Me2B: "Me" Side Interoperability & Integration (Part 2)

Thursday 12F
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:

This was Part II of the Kim & Johannes session on Tuesday.

We discussed the following VRM tool use cases:

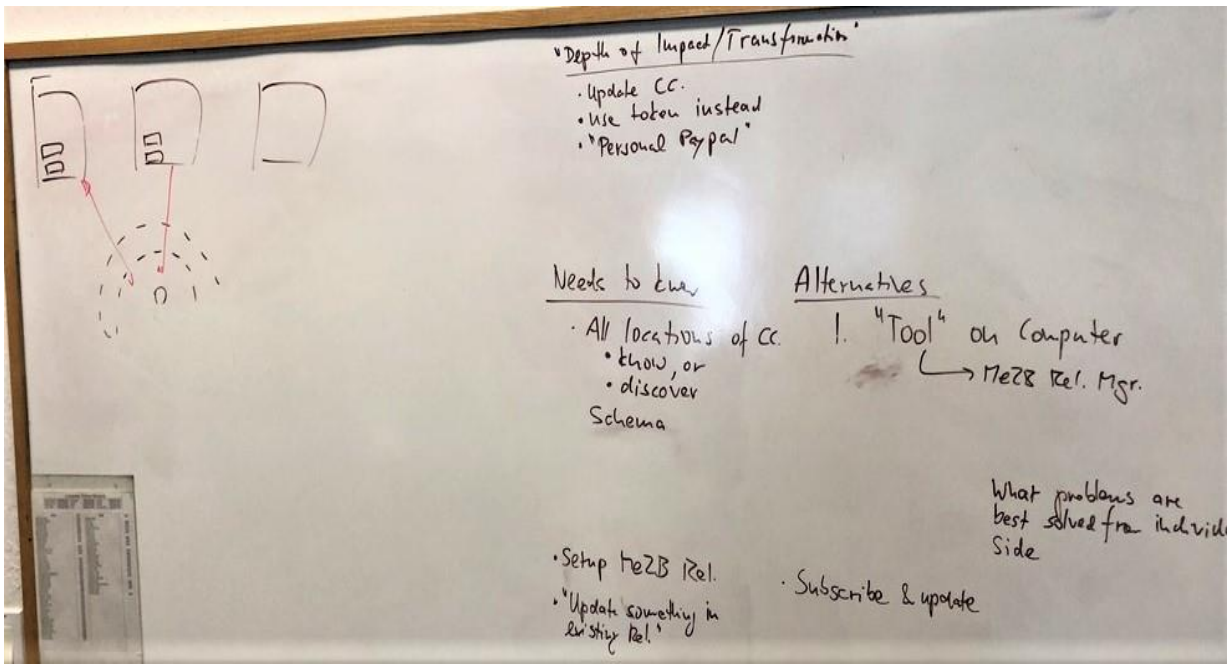
* Wallet:
  * cards to interact with multiple vendors
  * interchangeable, non-branded wallets -- there is a business in that

* Shopping cart across sites

* Normalized way of doing subscriptions

* Change your address / name once, and it goes everywhere

Whiteboard photo attached, and I believe Doc might have taken some more notes.



Retrofitting OpenID to Existing Apps BCPs?

Thursday 12G
Convener: Neil Thomson
Notes-taker(s): Adam Hampton

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

Overview:
This was a good session discussing the challenges and pitfalls encountered on the way to retrofitting a legacy web application that relied on AD+LDAP for AuthN to support SSO via OpenID. Neil has slides that accompany this session, to be sent separately.

Notes:
A BCP here is to use small reference tokens for modeling the session when injecting an OpenID login sequence to the legacy web application. A big lesson learned was that some systems (web servers and browsers!) have maximum cookie and token database size limits and these limits are small enough to cause issues with mixing the new OpenID tokens alongside the application's native tokens. Keep the footprint small and minimally invasive.

Other lessons learned: minimize introspection calls to where they are strictly needed. In an example case given, an AJAX heavy web app, putting introspection calls in the security filter stack added unacceptable latency in several use cases post- authentication. Keep the number of introspection calls (presumably made synchronously during the session authN chain) to a minimum and used sparingly.

DID:GIT: Where Is It At?

Thursday 12H
Convener: David Huseby
Notes-taker(s): David Huseby

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

- After IIW 28, a group formed around writing the did:git: method spec.
    - The latest version of the spec can be found here: https://github.com/dhuseby/did-git-spec

- Hyperledger hosted a summer internship project focused on modifying Git to support DID signing.
    - The project page is here: https://wiki.hyperledger.org/display/INTERN/Git+signing+with+DIDs
    - The intern selected to work on the project is Ibrahim El Rhezzali ibrahim.elrhezzali@gmail.com
    - Ibrahim successfully fixed and completed the patched I had started a year prior. He submitted them to the Git community here:
        - [RFC PATCH 0/5] New signing interface API with pluggable drivers https://public-inbox.org/git/Z2XOTcGuVovMKhcdrrO08KWI2I7L9s0CyFITvvj3jkmGTQPB6FkCiyOtT

m6GdYWbnf25dsPD8M08kDCuD37EE1B-sxHQ3se9Kn1zVBrCPZw=@pm.me/T/#u

- [RFC PATCH 1/5] Signing API: Added documentation for the new signing interface https://public-inbox.org/git/N31G34oKnfr3MVifk42-Kt3YtM_3fHuCp3V1cpGOK5f1jn1vbg1TaSCy9ukI-YD8qRfu4xMcHcPc78xFE0MSwJQWNrSvuQuer9wSNugNRLg=@pm.me/T/#u

- [RFC PATCH 2/5] Signing API: Added new signing interface API https://public-inbox.org/git/8AMhjK19PJ35u3LCR57IvtAzOBN5bKK2vUn0Ns-4mmZzK9U14W5CGW5R8aITNXBm78J4Z7nd09RTVKW2pGaB4PnF7p2PireF_vzRST8DngE=@pm.me/T/#u

- [RFC PATCH 3/5] Signing API: Migrated to the new signing interface API https://public-inbox.org/git/0oTOrSdJdIaEfs3NVkfRmLxjYRvUPkucwwaXPuhCjS2QL3ztRJLfllBkcpjSRiZQaY70SKSkg8_w20rxnuD4Vu3IbRcGOZM-fht8G7ySEHk=@pm.me/T/#u

- [RFC PATCH 4/5] Signing API: Removed old gpg interface and gpg mentions in code https://public-inbox.org/git/T4zS1hogOjySpdv7lDjVaZV83KKSeK9fx8m33SIo-e_BH4RtKcm67btmGzTPeflbRnQr7mWjTpObB0hCkX8VkGZElkQbLEgbrETg6Aq4nUg=@pm.me/T/#u

- [RFC PATCH 5/5] Signing API: Duplicated signing tests using new config aliases https://public-inbox.org/git/74R10RrvOffzj20d_Owd_1WFMh1bWq8mIhEEBSzbhkHfbvW5BLHZj-L-AgHYnpqkxgZdCfW5b72GoIvKHucQz7tdiGZEzietp0IKpU1_wuI=@pm.me/T/#u

- The Git maintainers rejected the patches saying that they didn't want to have to add a C driver for every new signing tool Git supports in the future. They requested that we look into doing a configuration based solution.

- Ibrahim and I collaborated on a new design that was more in line with what the maintainers requested. The following is an email Ibrahim sent to one of the Git maintainers to discuss how to move forward:

- Hello Brian,

  My name is Ibrahim, i submitted previously the proposal for the new 'generic signing interface' in the git mailing list.

  I'd like to thank you very much for your feedback about adopting a "config based approach".

  We've been thinking the last few weeks how to go about it so the C code in git isn't aware of any external signing tools. We've come-up with a few ideas:

  - At first we thought about keeping a generic driver in the C code that handles operations just like the current code (Pipe / Stdin /

Stdout) and all other variables would be handled by the user config (like the command to run the signing tool, its parameters and options, Regex to parse existing signatures, etc.)

- Then we realized that this option would be very difficult for the user on one hand and on the other hand we're making the assumption that all signing tools would handle the signing process same as GPG (exit codes, status, output, etc.). So we found another idea which is to use Assuan, an IPC protocol developed by the GPG team to use their signing tools in server mode:
This would have been a clean way of coding the interface but it had it's drawbacks: Is it worth adding a new C library in git just for the signing operations ? and again only tools that handle Assuan would work, namely as of now GPGSM handles it and GPG not fully, which is not so great.

- After much thought, we landed on a middle ground solution and we think at the moment it may be the best way to go: Just like you proposed, make the signing interface in C not aware of any signing tool and completely standardized. On top of that the user would have tool specific configuration that contains information like signing key and identity. Then we use simple bash scripts to drive the tool correctly. We would have for example a "git-signing-gpg.sh and git-signing-gpgsm.sh" and so on for the other tools.

Adding a new tool would be as simple as adding a bash script and the necessary config to make it work, without touching the C code. Since git already bundles many bash scripts for different purposes, we didn't think it would be a problem.

I really want to find the best way to do this properly and in a clean way, that's why i contacted you directly before submitting the proposal to the mailing list. What do you think ?

    - The response has been great and Ibrahim is continuing to work on this version of the abstraction.

- At the same time as the internship, I also started a conversation with Konstantin Ryabitsev about inline identity management in Git repos and why we think git:did: is necessary.

- Konstantin responded with a really inspired blog post: https://people.kernel.org/monsieuricon/patches-carved-into-developer-sigchains

    - Konstantin's concern is about preserving the nature of the email+git lifestyle of kernel/git developers that he serves.

    - I think it is important to note that Konstantin and I agree that inline identity management is important but we disagree on how we get there and somewhat on how it should be implemented

Life Scope.io Digital Self (AI, HUB, DB, DID, SSI)

Thursday 12I
Convener: Liam Broza
Notes-taker(s): Liam Broza

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

Link to the original notes provided by Liam:
https://www.dropbox.com/sh/nog9lwofd6ztkym/AABX2TXj3aUKl6GY6w3HssQ1a?dl=0

This session continued from the first LifeScope talk. (Thursday Session 11B)

- Went over alternative technologies to be reviewed in implementing LifeScope. (AI, HUB, DB, DID, SSI)
- Screening of the LifeScope "war room" commercial
- Went over AI plans and LifeScope Capture.
- Went through a long discussion of the emerging Human Digital Twin industry and how this affects IIW, SSI, and current data politics.
- Continued into a deep architectural discussion of LifeScope and solicited aid from the community.

If you are interested in contributing to LifeScope.io, please reach out to liam@lifescope.io

Censorship Resistance & Permissioned Ledgers Survivability Analysis

Thursday 13A
Convener: Sam Smith & Phil Windley
Notes-taker(s): Sam Smith

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

Link from Sam:
https://github.com/SmithSamuelM/Papers/blob/master/presentations/CensorshipResistance_IIW_2019_B.pdf

ID4 Africa: Exploring Possibilities for How SSI Communities & Companies Show Up At The Event & Surrounding Weekends (Morocco June 2-4, 2020)

Thursday 13F
Convener: Kaliya Young
Notes-taker(s): Kristina Yasuda

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

Context: Kalya went to ID4Africa and got inspired to organized a SSI related event at a next conference is Marrakech http://www.id4africa.com/

- Abbreviation: CRVS - Civil registration and verification service
- Background
  - Difference in mental models: our (IIW) perspective – I have a digital self and I control it vs World Bank – digitizing records
  - Dedication: Data protection officers brought to ID4Africa for free
- SDG 16.9 give everyone a legal / digital ID – need to be finished in several years
  - Motivation in Africa: Intention to learn as fast as we can and start implementing = pressure
  - Dilemma: have to be delivering a service to scale this
- Doc's previous conversation with the WB after explaining SSI:
  - Their answer: Funding is there, but if we continue doing it in a conventional way, we will get nowhere
  - "we're going to help governments not to make a mistake" – help African governments to get 'centralized' databases correct
- Need databases to be talking to each other
- Kalya had 'decentralized' identity meet-up @ ID4Africa
  - Problem found: cannot onboard RPs fast enough
- Feedback from Youth in Africa: "Africa is decentralized anyway"

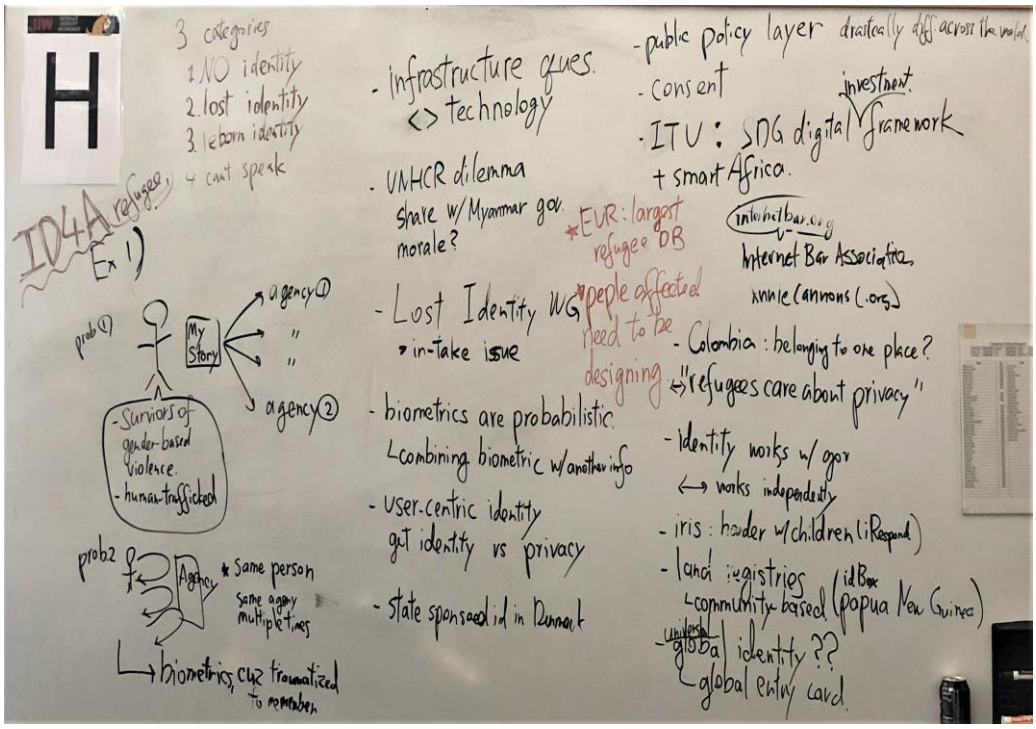
Discussion

- How is collab across the countries done? – parties do not even talk to each other today
- Need: Education material
  - Brussels Sciences & Society felt like victims
  - How do we talk about identity to a 'normal person'? to policy makers?
- Who defined Africa? Egypt, Libia not included
  - Do not have capacity or already advanced?
  - Smart Africa is similar
- Bringing together start-ups working on Digital ID. Problems faced by a participant doing business in Africa (Uganda)
  - Explaining that they are not competing with others
  - Explaining it to the governments, how they can meet the deadline by 2030 /the concept itself -> need to be at the conference itself
- ITU – Digital Roadmap
- What problems does Digital identity solves for the governments
  - Honeypot problem increases risk for them?

- Foreign investment – early adopters private sector (ts1, WorkDay)
- Data protection problem tied into (eIDAS)

- Need to be selling as a scalable thing: once you issue, you can talk to anyone who issue these credentials (We are selling it all wrong now)
- All these architecture assumes connectivity
  - Chain of keys/credentials that can be read offline
  - SSI offline?
- Satellites! Relativity – 2 co-founders, founding of 3D printed rockets
  - 2021 rockets a year – will be carrying micro satellites who are building those up for communication services. Space version of google satellites – low orbit satellites
  - At least 5G level communications?
  - Connectivity goes away in 7-10 years away?
- Do not build another one – connect those systems,
  - Interoperability not just technical, but also legal, trust framework
  - Gov as certifiers?
- Survivability of a regime change…
  - Leverage the NGOs networks who have expertise in this domain
- Leverage Japanese
- Reach out to ITU (international telecommunications union)

- Founder of Diwala – skills data points in Uganda
- Close digital divide
- Chinese surveillance system
- JICA got funding to do digital identity in Africa (Rwanda)



Verifiable Credentials for Digital Provenance? + Deepfakes Part 3: What Part of the Identity Stack?

Thursday 13G
Convener: Sarah Allen & Kathryn Harrison
Notes-taker(s): Sarah Allen

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

Two Digital Provenance Use Cases presented:

Scenario (A)

In order to refinance a loan, there is a complex network of actors who review multiple inputs to assess the creditworthiness of the investment.
Actors

1. Homeowner- Owns the home and is submitting a request for refinancing.
2. Bank- Organization which owns the loan
3. Loan processor Pete- 3rd party organization working on behalf of bank to assess if house meets code requirements to get loan

Objects

1. Loan application
2. House photos- Pete takes photos to validate that the house meet the criteria for the loan
3. Loan evaluation- qualitative commentary and photo evidence

Flow
Homeowner-->Loan Application-->Bank--> Loan Processor Pete-->Photos taken by Pete-->Loan application

How do you know that the content in the photos is authentic?
Example-- to pass the loan criteria need a carbon monoxide detector but homeowner doesn't have one. But Pete is incented to get the loans approved and finished so he pull a detector out of his pocket, plugs it in and takes a picture.
Or he photoshops it?

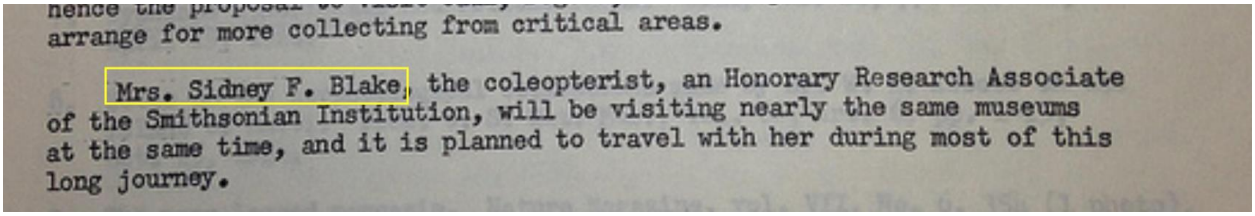
Scenario (B)

Can we connect digital records such that the provenance of knowledge can be traced in order to streamline the research process? For a use case, we can look at a focused research questions that was answered in digital archives with multiple searches and expert research analysis
(via Smithsonian Collections Blog)

Doris Cochran was a herpetologist who collected over 3,000 frog specimens from Brazil in her career. Her 1962-1963 travelogue documents Doris Cochran's National Science Foundation funded

trip to visit museums in South America and collect frog specimens. In 2013, Smithsonian Institution created an online Transcription Center where volunteers could transcribe historic documents. One volunteer questioned whether the catalog meta-data was correct. The writer of the travelog mentioned a travel companion "Doris" -- was this book written by another scientist?

Working with archivists and researchers at the Smithsonian Institution Archives, we discovered the original NSF research proposal which mentions Mrs. Sydney Blake.


arrange for more collecting from critical areas.

Mrs. Sidney F. Blake, the coleopterist, an Honorary Research Associate of the Smithsonian Institution, will be visiting nearly the same museums at the same time, and it is planned to travel with her during most of this long journey.

1. Archivist Annie -- takes papers from Doris Cohran's office, catalogs them for the physical archives and creates digital records (Finding Aid)

2. Digitizer Don -- creates digital image from the field notebook, giving it an independent digital record (ID: SIA RU007151) with reference to the collection of papers.

3. Researcher Ric -- documents NSF grant proposal with reference to Mrs. Sydney Blake

4. Researcher Ellen -- determines that Mrs. Sydney Blake is the "Doris" mentioned in the field notebook.

The group decided to focus on Scenario A because participants believe it to be simpler.

Actors

- Home owner "Wendall" (excluded to simplify scenario)
- Loan processor "Pete"
- Bank

Pete is issued a credential that he is qualified to inspect the home.

When Pete inspects the home, he uses his credential to issue a claim.

What credentials do they need to perform the role? What is the chain of events?

Verifiable Credentials issues to humans / real-world entities

1. Bank asserts that Pete is authorized to take photos for the loan documents
    - issuer: bank
    - subject: Pete
    - holder: Pete's Photography Co. (could be Pete)
    - claim:

Possible option: Bank provides Pete a digital camera >

2. Bank asserts that Pete is authorized to take photos for the loan documents
    - issuer: bank
    - subject: Pete
    - holder: Pete's Photography Co. (could be Pete)
    - claim:

Possible option: Bank provides Pete a digital camera >

Transactions

2. Pete takes photo and generates a report. (This report is a verifiable credential.)
    - issuer: Pete
    - subject: <house or photo (could be two subjects)>
    - holder: Pete's Photography Co. (could be Pete)
    - claim:

3. Pete provides the report to the bank. The bank can verify the report (VC) to ensure that it was created by the entity that was authorized by the bank.

Open questions

- ontology for the issuer/subject/holder fields need to be determined
- what happens in real world / real time? what are the digital parallels?
- what are the implications of this? does it reduce / increase trust in informal systems?

https://github.com/ultrasaurus/digital-provenance

Generic MFA Token Recovery: The Good, The Bad & The Ugly

Thursday 13H
Convener: Niels Van Dijk
Notes-taker(s): Nick Roy & Niels Van Dijk

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

Notes from Nick Roy:

Currently implementing webauthn for a number of IdP products
Webauthn is easy
Key recovery is hard

In the old password reset scenario, you still had a database of email addresses.
For second factor recovery, or primary authn factor recovery, sending an email is a bad practice

Force people to register more than one second factor, use the spare for recovery
- Works well assuming the strenghth of both is comparable
- Could be expensive
- Crank up the pain until they do what you want - break SSO, etc.
- The recovery factor must be of the same type - something you have == something you have

Print out sufficiently high entropy recovery code (could encode this in the seed quest game)
- Must be single use

- Having too many recovery methods adds risk

Lock the user's account when they recover via email, so the "real" user has a chance to react if it's an attempted take-over

Dead-man's switch - account recovery keys kept by others (trusted third party/social key recovery) become active only after account inactivity

Key sharding - n of m
- Have to gamify it / make it fun
- Shard it / immediately distribute. Then if you need to use it, you have to recover a bunch of those

Use part of what the org knows about you to recover (basically KBA)
- Enterprise, send reset token to your manager
- Ask questions about things that are in your email, your social network, that that org knows
- You can't claim that it's two-factor if you're using KBA to recover the second factor
- Open to social engineering
- Incentivizes phishing

Use of a guardian to do key recovery
- Everyone who you pick as your "buddies" have to be enrolled in the second factor

Physically go to a place to get your identity re-proofed

- Or via video
- Doing this in southeast asia for Grab (prevent drivers sharing accounts)

Biometrics as one of the factors minimize the risk?
- Something you are is something that can be stolen from you
- Performance of the sensors isn't as good as other authentictors

Key scoping/beyondcorp/webauthn
- Protecting different things with different keys
- Separation of duties
- Not really recovery of keys
- Parallellized keys for every interaction?
- There should be no master key - you can regenerate from your other keys

Need to solve for the masses/for the cost
- Making bettter security posturing decisions to protect the 90% - "good enough"
- Student population - 10,000 people and up.
- Need a good/cheap/easy way to do this.

Managing a single private key doesn't fit into a normal consumer mindset
- Is having multiple keys really helpful?
- Technically yes, but people are lazy.
- Continously updated key material updated as you pair devices, all your devices have secure enclaves. Back to n of m.

Biometric
- Require pin and password
- Then need backup for pin and password
- Use email
- Lots of people, for example in SE asia, don't have email - use a fake email address

Writing a recovery secret on a piece of paper is airgapped, simple, pretty fool-proof
- Unfortunately it's not verifiable by the system that the person wrote it down, wrote it down correctly.
- Falls through to the helpdesk

Using a government or other authority as the guardian
- Could be used as part of the identity proofing process
- Assumes you could strongly proof everyone, which you can't/is a privacy problem

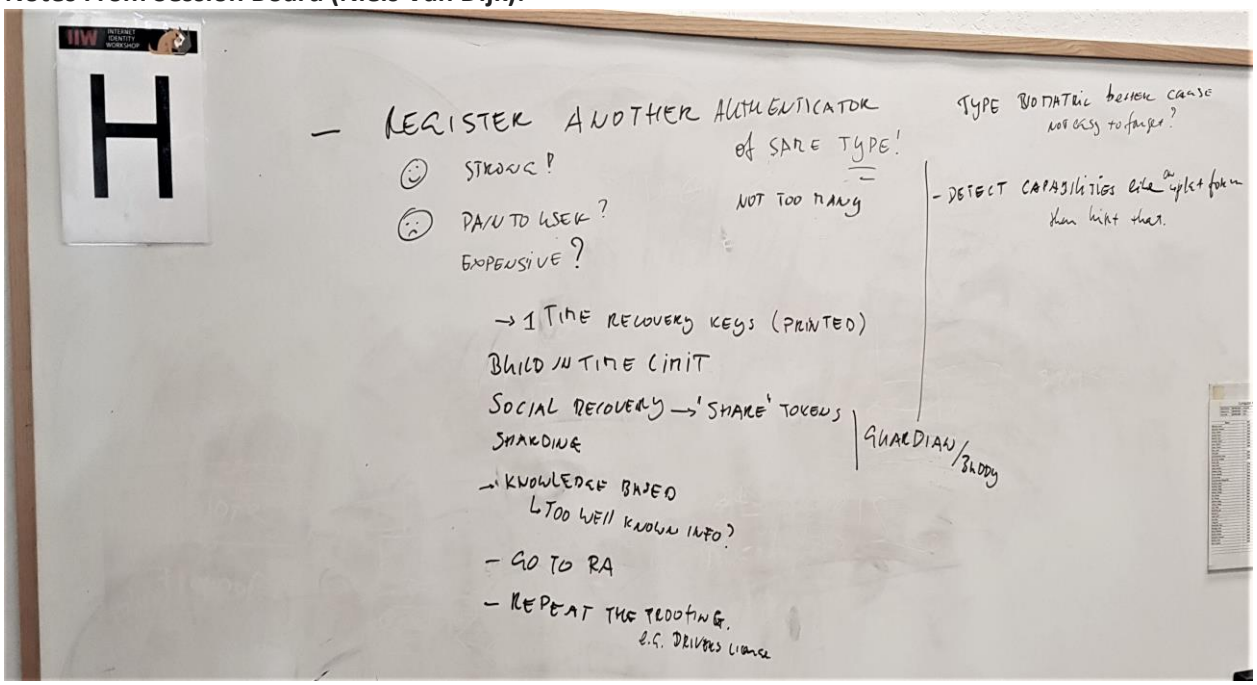
User-friendly scenarios?
- Gamification
- In Webauthn, experimenting with logging in with Android, have a platform authenticator, platform can offer to helpfully enroll another token (its enclave) for you. Be 'helpful' / offer to do nice things for the user.

Situational authentication/behavioral authentication
- Useful for adding extra facts to the session
- Great for triggering step-up, but not useful for recovery

In a multifactor situation, what happens when someone forgets their password?
- Can't have a backup password, they're more likely to have forgotten it
- Have to break the rule in that case
- You could require two physical authenticators and send a notice to the user, something like that
- Sometimes it boils down to a help-desk problem

No reason you couldn't design a recovery flow where you get a temporary password, use that, and have to use U2F as basically the primary factor and then you reset your password.

Notes From Session Board (Niels Van Dijk):



Claims Vis-à-Vis Scopes in OAuth & OpenID

Thursday 14A
Convener: Travis Spencer, Curity
Notes-taker(s): Travis Spencer

Tags for the session - technology discussed/ideas considered:

oauth, scopes, openid, oidc, openid connect, claims, scope

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

In this talk, Travis lead a discussion about his and his team's learnings about the relationship of claims and scopes. He stated that "scopes are a group of claims". He showed how the precedence for this is set in OpenID Connect (OIDC), and suggested that the idea be extended to plain OAuth. This would allow for arbitration scopes to be created that contain various claims.

To justify this somewhat novel and controversial idea, he explained what claims are: A statement asserted by some entity about another (the subject). These are only believable and acceptable if the asserting parting is trusted. He then explained what attributes are and that these are inputs to claims. They only become claims when an asserting party asserts them. A claim can be made up of many attributes and the values can be transformed into various types of objects (Boolean values, numbers, string, or complex objects).

When a scope is a group of claims, the administrator of the OP/AS need only configure scopes since a claim will always be in at least one scope. Claims are mapped into a "sink" on a per client basis.

A "sink" of claims are various places where claims end up. These include an ID token and user info as defined by OIDC. They can also be mapped to an access token or an access token only for a certain API / RS.

There are many sources for claims. The obvious one are data sources, but others exist. Travis listed a few including authentication attributes, static text, etc.

Users / RO consent to scopes (if it is an empty group) but typically the claims in the scope.

Claims input / output are defined for all OIDC flows (code, implicit, and hybrid). Input is done using the claims request parameter using its defined query language. This is needed for all other message exchanges with the OP/AS (like on token exchange, refresh, introspect, etc.).

In a claims-based system, the need for scopes goes away. Until the system is totally claims-based, however, access control can continue to be done on scopes (which are less expressive). If the client or RS is claims-aware, it can make more fine-grained access control by looking at the claim names and/or claim values.

Pico Agents for Communication Follow-Up

Thursday 14E
Convener: Bruce Conrad
Notes-taker(s): Bruce Conrad

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

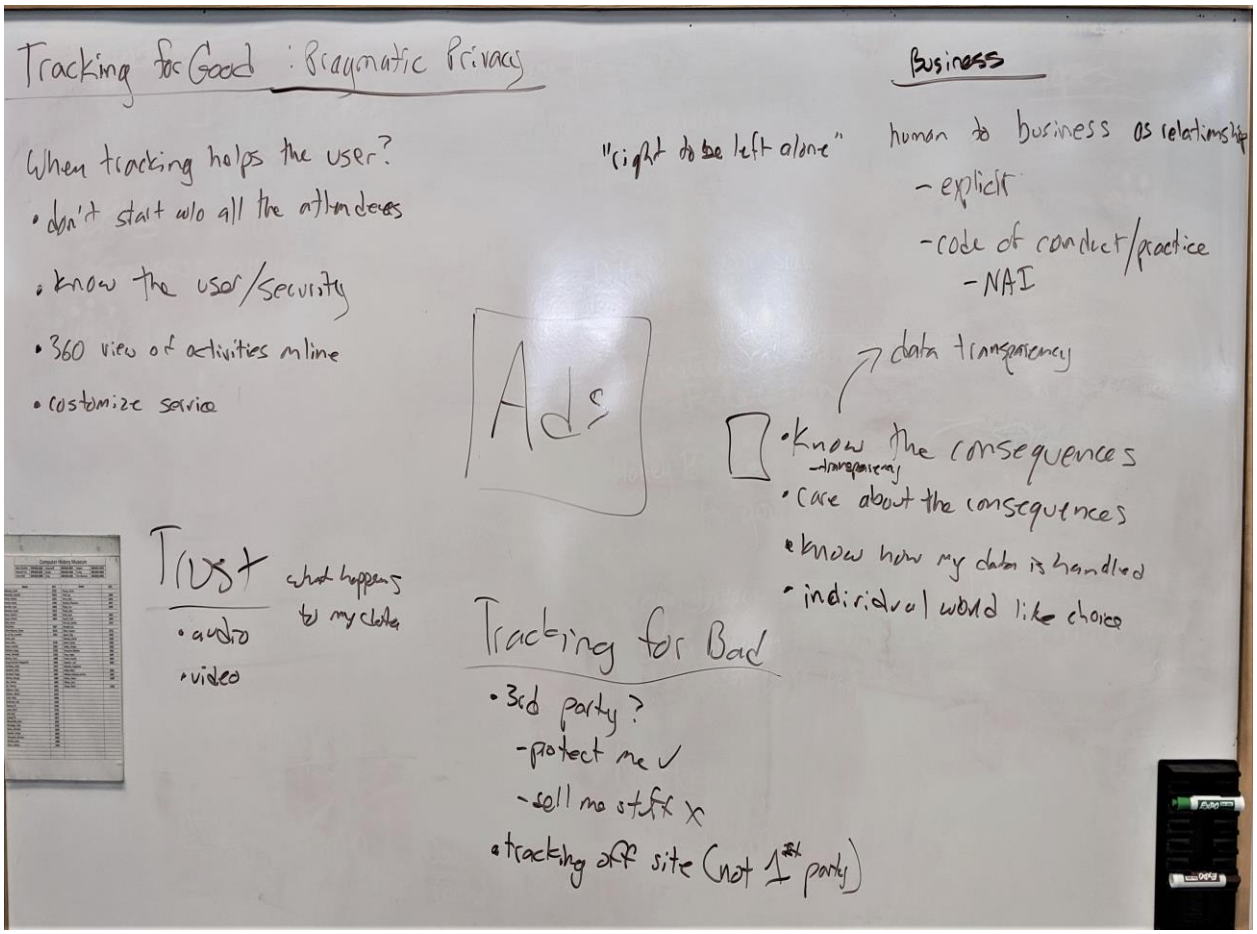
This was intended as a continuation of session 11J but ended up being a one-on-one with Ram and myself, where we discussed all things pico.

I learned some useful things about what happens with private keys when a pico is transferred from one owner to the next.

Tracking For Good: Pragmatic Privacy

Thursday 14F
Convener: George Fletcher
Notes-taker(s): George Fletcher

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



Product Roundtable: Bridging Tech & Business Connect And Sahre Challenges & Resources

Thursday 14H
Convener: Margo Johnson & Luke McIntyre
Notes-taker(s): Paul Tinson

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

Product Round Table
The volume of people interested in this session is indicating that the time is right for the product and marketing people to start taking a bigger stake in this technology.
Lead by Luke and Margo
Resources:

- uniresolver
- Figma - Design Tools
- The noun projects
- whimsical
- iconjar
- product board
- Cascade Strategy

Working Groups

- DID UX (sovrin)
- other

How do we bridge the tech into product realities and start a continuing roundtable forum? Need to bring together the like people into a group like DIF for product and market story.
What are the markets?

Needs:
Definitions about terms from a market and consumer point so it is useful and understandable.
So consistent industry terms and consistent consumer terms. Does it matter that we may have variation?
Clear adoption story for enterprises is critical.
How to help the customer understand what the value of this is, why should i change from a stack that mostly works.
Show the problem that your existing technology stack cant solve that this technology does.
Have formal ways for product people to collect and share the needs and problems of the customers. Start the customer-centric work.
Customer personas are needed, they will help define the thinking about what segment you are targeting.
What is the driving principle that drives the conversation to even begin?

Pricing Models:
pricing models are useful, and we should not try to re-invent that as well as the tech. That is working well for some people.

Advice:
mapping cost to business benefit.
Quantify the benefit in terms of something tangible
UX and CX is critical
Avoid vendor lock-in

Working Well:
Using the language of added value, new value props, new business models.
Reducing infrastructure costs and complexity
Ethical monetization of data that enables conversation at scale.
Relating to the customer's domain-specific eco-system helps bring them on board

Who are the buyers:
Cost Savings:
UX ... Design Ecosystem:
Question:

- User managed keys
- Spectrum of users
- Simplicity
- Choice
- Understand responsibility/cryptography

Adoption curve and strategy, are there parallels with existing paradigms.
Targeting enterprises and empower them to drive them to their customer bases.
New employee onboarding, vendor onboarding etc
Mental metaphor model
How does consumer protection fit into this model, who is the authority that consumers can tie back to for a sense of certainty?

Terminology: The Plan

Thursday 15A
Convener: Drummond Reed, Daniel Hardman, John Jordan, Joe Andrieu (remotely)
Notes-taker(s): Sarah Allen

Tags for the session - technology discussed/ideas considered:
SSI, Decentralize Identity, Terminology

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

IIW started as a mailing list around user-centric identity.
People were talking past each other, until we get to shared understanding and shared language

shared understanding - I understand what you mean even if we are using different words
shared language - shared terms

Eugene Kim - specialized in collaboration, way to successful collaboration is to identify small goals and make them happen

Paul ??? led community through process of creating a lexicon

Lexicon on the identity commons
NSTIC references it

Alice / Bob ==> ??? ==> Persistence of an attribute about Alice

SSI didn't emerge until around 5 years ago
Decentralized identity, User-centric identity, SSI largely describe the same thing

Sovrin Foundation needed to create policies, founding docs, etc., so they needed a glossary

https://sovrin.org/library/glossary/

July 2017 - Sovrin Glossary v1 - 102 terms - all legal agreements used these terms
~50% of the terms were refined or replaced

March 2019 - Sovrin Glossary v2 - 248 terms

What about NIST Taxonomic Approach to Blockchain identity?
https://csrc.nist.gov/publications/detail/white-paper/2019/07/09/a-taxonomic-approach-to-understanding-emerging-blockchain-idms/draft

Functional Identity paper by Joe Andrieu. Joe joined meeting via zoom and gave an overview of this paper. The paper asks for people to think about Identity functionally, rather than political, cultural, psychological. Let's talk about how we use it. (Part of that was rejection of ISO standard that said that identity was a set of attributes associated with an individual)

> "Identity is how we recognize, remember and respond to specific people and things" — seems to work cross-culturally and cross-contextually

We operationalize identity in a number of ways. This definition seems to work well for how we need to use identity. The paper also introduced 10 terms, which also seemed to help.
http://bit.ly/FunctionalIdentityPrimer

Not being too prescriptive. Let's not run things in parallel that are really the same and not arbitrarily different just because of terminology.

One of the 7 laws of identity, "unified user experience" — regardless of terminology, we all have a shared experience of driving a car. It's a safety concern that we have consistent user experience in driving cars. Same for identity space.

What is the audience?

- Need to have words for the people who use the software
- Also, policy vs. software developers

Is this even about identity? Should we instead focus on ue cases

When sovereign states use “identity” badly, they end up harming marginalized peoples. It ends up turning into an oppressive statement like “we are giving you an identity” or “we are defining your identity”

How we use words amongst ourselves affects how we talk outside our community? For example, the “stack” we created was helpful in organizing how we work with each other.

Audiences

1. Developers / Architects
2. Product designers
3. UX designers
4. Policy writers / regulators / lawyers / legislators
5. “End Users” (useful to refer to different, specific groups of end users)
6. Investors
7. Journalists
8. Customers
9. Analysts
10. Standards groups

Terms are valuable for developing a market for the solutions people are building

There are a number of terms that are well-used within the identity space — would be great to clarify if anything is different for SSI or just a clarification.

What do you think about moving the glossary into a repo?

What is the scope of this? There are so many glossaries out there. What is the scope of this?

Min scope - Developers + Policy writers

Sources

- SGFWG
- MyData
- GDPR
- Standards Groups
- NIST

Maybe it needs to live somewhere that is not affiliated with a single group (e.g. IIW, identity commons) [Note: these suggestions are affiliated with their own group.]

To be continued, after closing circle.

Cards Against Identity

Thursday 15B
Convener: Justin Richer
Notes-taker(s): Justin Richer

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

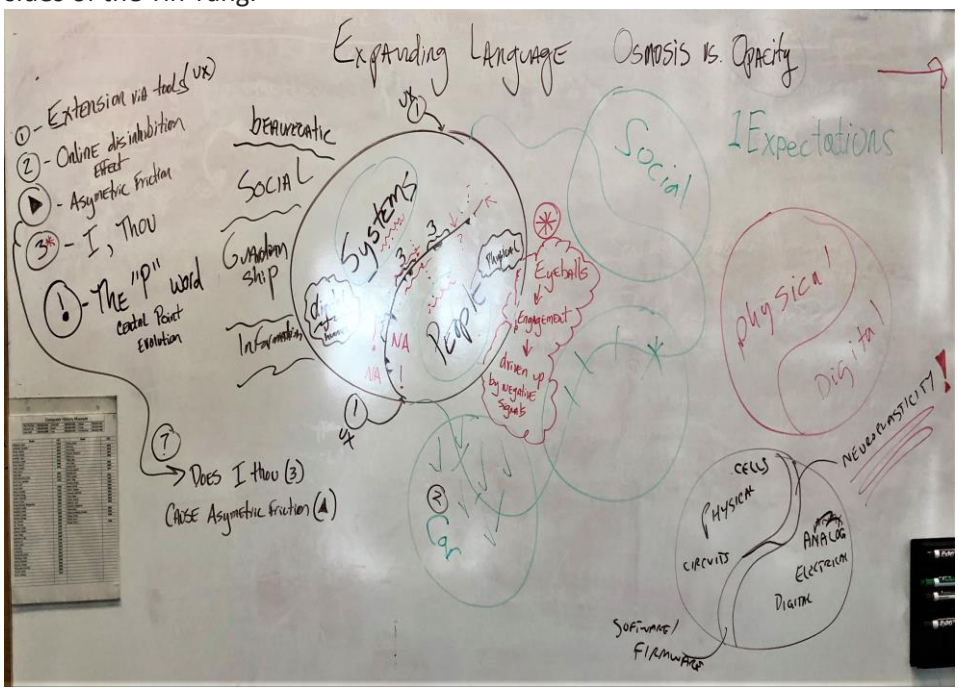
Links from Justin:
(these url's are the contents of the notes, I'm not saying the notes are hosted here)
http://cardsagainstidentity.herokuapp.com/
https://bspk.io/games/cards/

Expanding Language: Systems & People - Osmosis & Opaqueness

Thursday 15F
Convener: Jeff Orgel
Notes-taker(s): Jeff Orgel

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

Reviewed the membrane between systems and people and the efficacy, or lack thereof, between to two sides of the Yin Yang.



Sidetree DID: ion+did:elem Roadmap & Dev

Thursday 15H
Convener: Orie Steele
Notes-taker(s): Guillaume Dardelet

Tags for the session - technology discussed/ideas considered:

Sidetree, Element, Ion, Scaling, DID

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

In this session, we discussed the Sidetree protocol as a solution for scaling DIDs and the two main implementations:

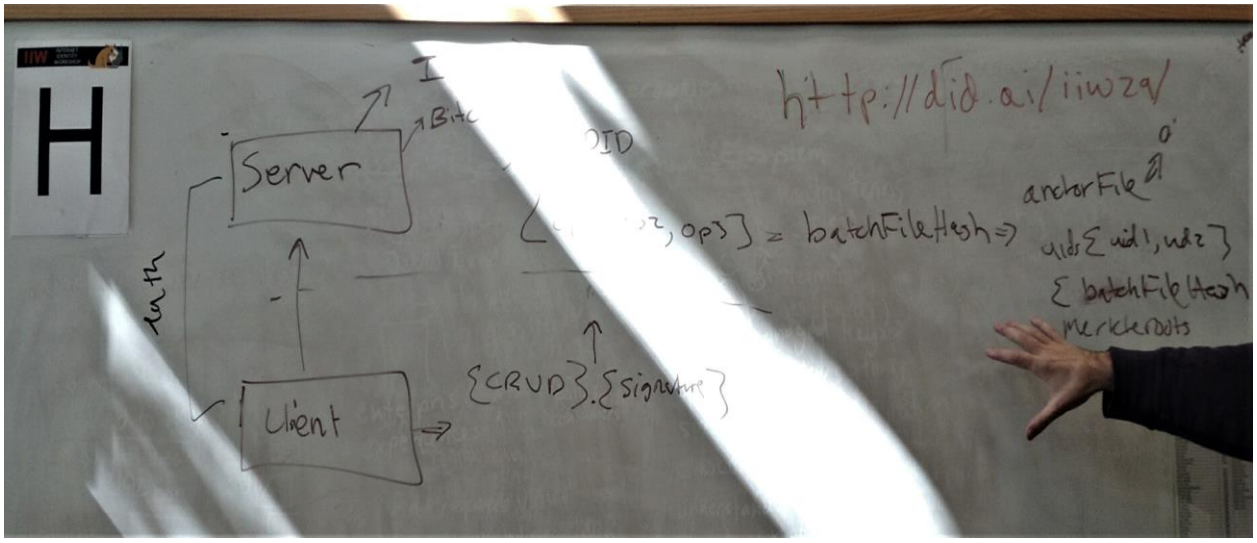
- Element (which uses Ethereum as a ledger)
- Ion (which uses Bitcoin as a ledger)

The main points that were addressed were:

- How Sidetree batches DID operations
- How resolving a DID works
- Key differences between the Ethereum implementation and the Bitcoin implementation

Resources:

- https://did.ai/iiw29
- https://github.com/decentralized-identity/sidetree/blob/master/docs/protocol.md
- https://github.com/decentralized-identity/element
- https://github.com/decentralized-identity/ion



Building A Business Around Identity In Education – From A Colombian Perspective

Thursday 15J
Convener: Sabastian Farfan & Danny Suarez
Notes-taker(s): Sabastian Farfan

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

Write-up from Sabastian Farfan; https://link.medium.com/QVjFZfmww0

It was a pleasure being a part of the 29 version of the internet identity workshop held in Mountain View, California this week and to have the opportunity to share my experience from a Colombian point of view.

Unfortunately when it comes to identity i know that my country, Colombia, is known for mostly three thing: Beautiful women (like Shakira and Sofia Vergara), making the world greatest coffee and for drugs (thank you Narcos for this).

We as Colombians are trying to break this stereotypies because we are hard-working people and we want to make an impact in world economy. For example, I don't know if you know, but the first unicorn in Latin America is from Brazil called Nubank a fintech founded by David Vélez a Colombian entrepreneur. And the second unicorn, is a delivery company called Rappi an app were you can order whatever you want in any part of Colombia, but besides being a delivery service, what they really do is collect the hugest number of data sell it to big companies.

We are eager to take part in world economy and we are ready to take a big step. The problem is that the idea of digital identity is unknown in Colombia.

Our main concern, in terms of internet, is for people to have access to it. About 23.8 million of Colombians don't have access to internet and this is one of the biggest challenges the country has. That segment of the population concentrate in remote regions and in the main cities they concentrate in the lower-income society, the technology is simply not there. Comparing to the states, 76% of the population have access to the internet.

¿Did you know about the Facebook initiative about giving internet access to everyone? In 2014 Facebook had this initiative where they wanted to give internet for all calling the project internet.org. Colombia was the first Latin American country to receive the app by the hand of a big telecommunications company called TIGO. This didn't worked because of many reasons involving internet neutrality and fair competition. They only had access to 16 web pages including Facebook of course.

Now let's talk about the blockchain legislation, if you have a wallet with 4 Bitcoins, today the Bitcoin is at 14 dollars and the end of the month that Bitcoin increases it's value to 10,000 dollars ¿do I have to pay taxes by this occasional money valuation? Ok, in Colombia i was in a criptocurrency conference and a lawyer talked about this subject, and he said that our legislation is way behind because we don't know yet how we can handle this front the taxable part and, I mean, governments are always looking for a way to have more tax collection and improving and improving the country's revenue system. But corruption is a disease in my country so things tend to happen really slow.

However, they are about 7 companies that are emerging in the blockchain ecosystem in Colombia. And the more the better, because they incentive fair competition and the most import thing they educate people in the use of their digital identity, but ¿How do you talk about identity to a normal person?
Self Sovereign Identity is a beautiful market because when a competitor closes a deal or does well with a client, it helps the others because it creates trust in the system. The market is really big and we are just starting to explore it. The only problem i see is that Colombian universities and companies want to create a closed network and in the future ¿Would we be able to create interoperability between all the networks?

I'm going to tell you a little anecdote that I had. In 2015 i graduated with a double bachelor degree in Business Administration and Design form the best university in my country, University of Los Andes, and I wanted to do a master's degree in London Business School. For the application to the program i had to send my certificates to the university and for doing that I had to three things:

1. Go to the university and ask for the documents, for this they took about 2 weeks.
2. Then I had to go to a place called a registry and add a stamp to the documents (you know, just to make sure that I wasn't making this all up) I manage to make this in a day
3. Then I had to go to the delivery company to send this documents to the university.

The first time i did this, the delivery company lost my documents, they simply didn't knew where they went. The second time, i went to the registry they put the stamps wrong so i had to go back (a third time) to the university and ask them for the documents. In all this time, the university in London didn't get the documents and i had to apply all over again. So I postponed this and start working in the health sector.

Being aware of digital identity in the world and knowing Colombia is not part of it, we created Xertify to meet this goal, a company that issues digital credentials for students. At the beginning we started going to the big universities, to the government and all this big institutions that just didn't listened to us, they saw as a small project with no much importance. This is because the universities have long bureaucratic processes that make hard for decisions to be made.

¿How long do you think it takes to close a deal with a university? approximately 12 months, because you talk to them at the beginning of the year, when they are planning their budget for next year, and meanwhile you try a demo and continue tu manage the client. We had to review our business model, because when you go to the market you will meet many things that you think are right but are actually wrong like ¿how are we charging for this? ¿Is better to sell packages or a monthly subscription? For

example, one big university turn us down because our business model at the time was for packages of 200–3000 certificates and they were issuing approximately 10,000 documents a month.

When you are an entrepreneur you have to deal with rejection all the time and this is beautiful because is a learning process that few can handle. After this we found a big language institution that wanted to issue digital credentials, it took 7 months to close the deal but we found that in this time of non-formal education system the bureaucratic process is not that long, decisions are made fast and implementation was easy. They are a lot of non formal education institutions and they want to differentiate with each other.

In Colombia the concept of digital identity is unknown yet we started to sell this idea of self sovereign identity and empowering students to hold their data but universities really don't care about any of this, they just want to make the process easier and to save money. Funny thing that we found also is that people or students don't really care about digital identity, they just want their life to be easier.

Demo Hour

IIWXXVIII #29
Community Sharing / DEMO LIST
Wednesday Oct. 2, 2019 1:30 - 2:30
http://iiw.idcommons.net/IIW_29_Demo_Hour

Thanks to our Demo Hour Sponsor HYPERLEDGER

1. **Gluu Gateway:** Mike Schwartz
   URL: https://gluu.org/docs/gg/ Gluu Gateway is an HTTP proxy to control access to web sites and API's using OAuth or UMA access tokens. Use cases include centralized policy management, stepped-up authentication, or explicit user consent. You can manage policies in the Gluu Server or an external policy server.
2. **SeLF by esatus AG:** Carsten Eichhoefer and Christopher Hempel
   URL: https://self-ssi.com/en SeLF transforms SSI credential-based access rules into authentication and authorization objects that can be synchronized and used by conventional technologies like SAML or LDAP.
3. **Transmute ID:** Karyl Fowler & Margo Johnson
   URL: https://www.transmute.industries/transmute-id Transmute ID brings decentralized identities and verifiable credentials into traceable multi-party business transactions integrated with major storage and identity access management tools. Scalable DIDs are possible with Element – the Sidetree protocol on top of Ethereum and IPFS.
4. **yes.com:** Torsten Lodderstedt
   URL: https://www.yes.com/ yes® introduces a scheme that enables bank customers to use their online banking accounts for conducting various digital transactions, such as login, registration, identification, payment and signing, with Relying Parties. Use of bank-verified KYC data in conjunction with online banking multi-factor authentication allows to address use cases up to eIDAS trust level substantial.
5. **ConsenSys: Ivan, the not so terrible:** Wayne Chang
   URL: http://www.ivanidentity.com/ (to be launched in September) Ivan stands for Identity Verification Attestation Network. Ivan is software that allows you to create and share real-world identities for people, places, and things and map their interrelationships.
6. **Vivvo - DID Authentication and Wallet Recovery:** Lucas Tétreault and Jamie Jamieson
   URL: https://www.vivvo.com/citizenone-eeze/ A quick demo of Vivvo's mobile DID/VC wallet. Create a wallet, use it to authenticate, and recover your wallet if you lose your phone.
7. **GÉANT project/ "eduGAIN: Global Identity Federation in Research and Education":** Niels van Dijk (SURF) **URL:** https://edugain.org/ This demo will showcase the current state of eduGAIN, an Identity federation in Research and Education in use across more then 63 countries. I will briefly discuss its reach, discuss some of the technical background and showcase some of the services that it enables.

8. **Workday Credentials:** Bjorn Hamel
   URL: https://credentials.workday.com/ Workday Credentials is a decentralized, standards-compliant platform for Issuing, Holding and Verifying credentials. We will be doing a short demo of all these capabilities.

9. **Duo Mobile and Partner Program Opportunities:** Leya Leydiker
   URL: https://duo.com At Duo, we combine security expertise with a user-centered philosophy to provide two-factor authentication, endpoint remediation and secure single sign-on tools for the modern era. Partner with us to connect and collaborate with Duo customers, resellers and developers.

10. **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 (128 bit cryptographic seed used to generate key). Designed to be simple and fun. Instead of memorizing your seed, you memorize actions in the game to recover your seed. After learning the actions, simply play the game to recover your seed. That's it. This complements other methods of key (seed) recovery as it is self-contained. This is a mnemonic capable of learning and recalling 128 bits of entropy.

11. **ISO 18013-5 Mobile Driver's License from GET Group NA:** David Kelts
    URL: https://getgroupna.com/media-center/resources/mobile-id-resources/ Mobile Driver's Licenses and Mobile ID Cards are being standardized now and should be in production during 2020. Learn how you can accept an mDL and the different modes of interaction supported by the ISO 18013-5 standard.

12. **Pico Labs - Manifold -- Manage All Your Things:** Bruce Conrad
    URL: manifold.picolabs.io A demo of the "Safe and Mine" application in Manifold to help when you lose one of your things. Also a give-away of tags that you can physically attach to your things.

13. **IBM Decentralized Identity Offerings:** Milan Patel
    URL: https://docs.info.verify-creds.com/explore/interactive_guide/ Interactive experience that showcases IBM Decentralized Identity offerings and an end to end experience of credential lifecycle management - issue, hold, and verify built using Hyperledger protocols. https://docs.info.verify-creds.com/explore/interactive_guide/

14. **Universal DID Registration and Resolution:** Markus Sabadello
    URL: https://uniresolver.io/ Interoperability on the DID layer is becoming more and more important. Let's look at some existing tools that can help!

15. **Wireline D-Suite demo:** Pete Rowley, Chris Waclawek, Karissa McKelvey
    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.

16. **Streetcred ID:** Michael Boyd, Tomislav Markovski, Riley Hughes
    URL: https://demo.streetcred.id **(not active yet. Will be by IIW)** Experience Streetcred's API in action. Our demo will show you how to setup your organization to issue a verifiable credential to your user's digital wallet within 5 minutes.

17. **Kiva. Biometric eKYC checks via Hyperledger Indy:** Horacio Nunes, Camillo Parra
    URL: https://www.kiva.org/protocol Kiva Protocol is using blockchain to provide microfinance access to communities that have traditionally been considered too poor or rural to serve. In this demo, we will demonstrate Hyperledger Indy's ability to provide eKYC checks to financially underserved populations.

18. **Self-Sovereign Biometric Credentials:** John Callahan, Chief Technology Officer / Veridium
URL: https://app.box.com/s/53xvyvqbj236v8vplxc65ppvg9rwjma2 The process for secure collection of fingerprint-based credentials that could be used in several countries currently requiring fingerprint-based KYC/AML checks for identity verification in which only the end-user holds the actual biometric information.

19. **TAG's Real-ITs Emoji Project and To Air Gap or Not To Air Gap IIW.28 Survey Results:** Jeff Orgel
URL: Link up at the table for the Reveal - "Facing" Your Self. Also presenting results from "To Air Gap or Not to Air Gap" survey of IIW.28

20. **HearRo, Inc is the company and our product is also called HearRo:** Vic Cooper
URL: https://www.hearro.com HearRo uses SSI to create unique, trusted connections that enable effortless communication. Built for enterprise call centers, using HearRo means no id questions, no waiting on hold, no starting over.

21. **Spaceman ID - SMS SSI agents:** Dev Bharel and Alexis Falquier
URL: spaceman.id Showcasing a new method of creating and maintaining an agent through SMS controlled cloud hosted wallets. See how a user using only text messages can connect with our API in order to create a sovrin agent. This agent can connect with other agents, receive credentials, and fulfill proof requests.

22. **Blockstack PBC:** Jude Nelson **URL:** https://blockstack.org Free and instant sign-up and authentication in a Blockstack's decentralized identity system.

23. **Xertify:** Sebastian Farfan
URL: https://xertify.co/ Xertify is a network were people and institutions can exchange trusty information using blockchain technology. We build a digital wallet for users so they can hold all their verified information and share it if they want. We build a solution that helps the process of issuing documents easier & faster.

24. **Where did my password go? Yubico:** Chris Streeks and John Fontana
URL: https://yubico.com _____ This is where your password used to be. Visit us to see where it went.

25. **IdRamp - Self Sovereign Identity the Enterprise and Beyond**: Mike Vesey
URL: idramp.com/ledger Learn how practical Interoperability with enterprise infrastructure enables adoption of decentralized identity.

The IIWXXIX Demo List can also be found here
http://iiw.idcommons.net/IIW_29_Demo_Hour

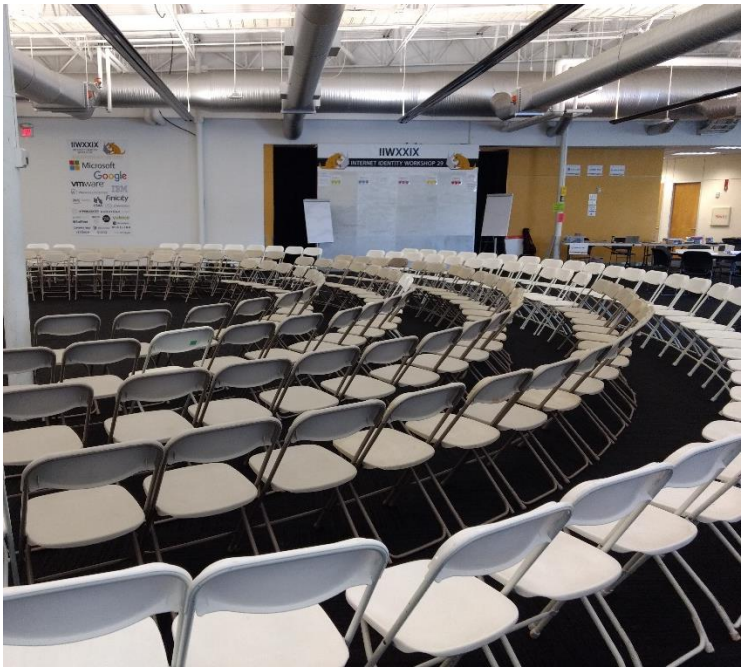
IIWXXIX #29 Photo Albums by Doc Searls

Check out Doc's FABULOUS candid photos of IIWXXIX @dsearls

Day 1: https://www.flickr.com/photos/docsearls/albums/72157711202277777

Day 2: https://www.flickr.com/photos/docsearls/albums/72157711408057691

Day 3: https://www.flickr.com/photos/docsearls/albums/72157711421249337



See you
April 28 - 30, 2020

for
IIWXXX

The 30th
Internet Identity
Workshop!

REGISTER HERE
https://iiw30.eventbrite.com

www.InternetIdentityWorkshop.com