IIWXXV

INTERNET IDENTITY WORKSHOP 25

ENDORSED BY HISTORY

Book of Proceedings

www.internetidentityworkshop.com

Collected & Compiled by
SIMONE POUTNIK, HEIDI N SAUL AND JACOB WINDLEY

Notes in this book can also be found online at
http://iiw.idcommons.net/IIW_25_Notes

Photo credit #IIW @Nobantu

October 17, 18 & 19, 2017
Computer History Museum ~ Mountain View, CA

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

Phil Windley
@windley

Kaliya Young
@identitywoman

Doc Searls
@DSearls

Co-Founders of the Internet Identity Workshop

Contents

About IIW

The Internet Identity Workshop (IIW) was founded in the fall of 2005 by Phil Windley, Doc Searls and Kaliya Hamlin. 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 past 12 years at IIW.

The event is now in its 13th year and is Co-produced by Kaliya Hamlin, Phil Windley and Heidi Nobantu Saul. IIWXXVI (#26) will be April 3 -5 , 2018 in Mountain View, California at the Computer History Museum. Please join us to learn and innovate with others!

IIWXXV Sponsors

IIW Events would not be possible without the community that gathers or the sponsors that make the gathering feasible.

If you are interested in becoming a sponsor or know of anyone who might be please contact Phil Windley at Phil@windley.org for event and Sponsorship information.

Upcoming IIW Events in Mountain View California

IIWXXV #26 April 3 - 5, 2018
IIWXXVI #27 October 23 - 25, 2018

Opening Discussion Question "Table Talk"

Pick a technology emerging or maturing in the IIW Community and answer the following:

- **What ethical problems does this technology cause? For whom?**
- **What questions should we be considering as the technology develops?**

Tables of 10 people each, both long time IIW Community members and first timers to IIW, discussed these questions and shared one of the technologies and questions with the entire group.

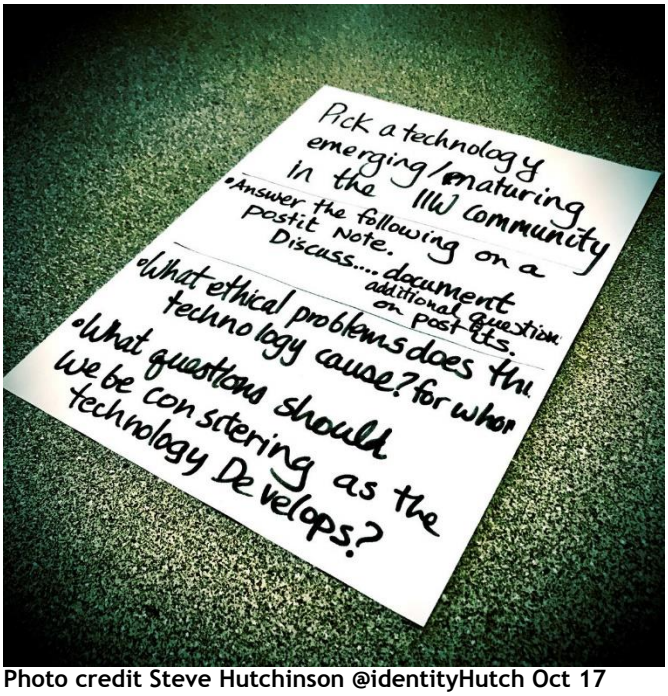


Photo credit Steve Hutchinson @identityHutch Oct 17
Starting my day at #IIW XXV with a 'table talk' about #AI. Lucky to have super smart people in my group.

Sacrifice of Autonomy for Trusted Identity

Need more review of ethical frameworks for identity with new solutions – covering anonymity to formal Government ID.
Dangers and Benefits across different societies
How do we make this easy enough?

Single Point of Control

What are they doing with the data?
Whose identities are being served?

Data Immutability

How to have the right to be forgotten within context of identity on a public layer?

Identity vs Anonymity

Identity and Culture

Is Spirit Related to Identity?
To what extent should Tech based Identity be free? Frictionless Accessibility

Quantum Computing

Is it ethical to build solutions on PKI (or DPKI) knowing that they are likely to be broken?

Self-Sovereign Identity

Will self-sovereign identity W I D E N the digital divide?

Sovereign Identity & Zero Knowledge Transactions

Enables appropriate privacy, e.g between doctor and patient
Allows validation of claims, e.g. vaccinations
BUT – causes issues at the meta level, e.g. The social good of investigating cost/benefit of treatments within patient groups. Or, how can a police department verify a potential new hire hasn't been fired 'for cause' without alerting the officer's current employer they are looking.

Ethical Issue Related to Autonomy both for Machine Learning and Blockchain

Highlights / Themes

Ownership of Data
The ability of users to understand how and why their data is valuable
What is the 'help' button for modern, distributed ID systems?
How do we create incentives for users to care about their data?

Universal Login

Data privacy - Who authorizes it? (Private co's wanting to be universal login provider)
Silos don't want to lose control
Smaller companies dong innovative things for identity but the challenge is how to get that widely accepted
How do you create self sovereign identity but

General Topic - 'Ownership and control of your Data'

Want digital services BUT now there is no personal legal accountability for use or misuse of data.
May lead to scary outcomes – AI

Data / Personal Data

Personal legal accountability
Lack of transparency on reuse

Data Immutability

How to have the right to be forgotten with/in the context of identity on the public ledger

Photo Credit: Julian Ranger @rangerj Oct 17

25th Internet Identity Workshop (#IIW) under way in Mountain View @digime proud to be one of the sponsors - learn & innovate with others

IIW 25 Session Topics / Agenda Creation

Photo credit
Sean Bohan @seanbohan
The calm before the #IIW storm

~ Before ~

Tuesday October 17, 2017

Session 1
1B/ 101 Introduction to OAuth2
1C/ DHS S&T IDM Program's R&D
1F/ DIF Technical/Recap and Roadmap Discussion
1G/ App Auth Q & A RFC 8292 BCP 212
1H/ Blockchain Democracy

Session 2
2A/ Self-Sovereign Identity #
2B/ 101 Introduction to OpenID Connect
2C/ Is Your Data Legal? Meaningful (oxymoron?) Consent
2D/ 'Fixing' The Consumer IOT/Smart Home User Experience
2E/ 6 Degrees of Identity Freedom
2F/ DIF Did's In-Depth (w/Review of Contentious Bits)
2G/ Token Binding for Cookies – OpenID Command OAuth
2H/ Intro to Hyperledger "So you think you need a Blockchain…"

Session 3
3A/ Mutual OAuth Distributed OAuth
3B 101 All Things UMA (user managed access)
3C/ Concerned About Centralized Authority? Let's Make It Participatory
3D/ Implications for the End User of How You Design A Blockchain For Digital Identity
3F/ Aadhaar
3G/ Information Sharing Agreements (ISA) – First Party Terms That YOU & I Proffer: V2.0 of the Commercial Web
3I/ The Big, Big Picture = Identity Money Topology – A Conversation – (did this happen twice?)
3J/ Identity Agents: It's not just what you know, it is what you can DO – Personal Data Stores—Extensible API'

Session 4
4A/RISC – Working Session
4B/ 101 NIST – Digital Identity Guidelines '101'
4C/ Blockchain Security & Privacy R&D Lessons Learned and Gaps
4D/ Fixing Social Security Numbers = Blockchain, Good Identity, Don't Break Existing SW
4F/ Functional Idenity
4G/ Public Blockchains AND – Private UMA) User Managed Access
4H/ Open ID Connect CIBA Explained
4I/ Identity Concepts Around The World

Session 5
5A/Public Blockchain Addresses FOR User-Centered Digital Signatures
5B/ 101 Introduction to DID's, Verifiable Claims and Blockchains
5E/ Blockchain Interop Chameleon Nodes?
5F/ HOLOCHAIN P2P Apps Without the Blockchains Problems for Scale, Speed, Cost & Governance
5G/ Next Gen Phishing (all your OTP belongs to us)
5H/ Yubikey Usability Study – Results for lab + longitudinal study
5I/ IDPro = Help Build Next Gen of ID Professionals

Photo Credit Doc Searls - @DSearls

~ During ~

Wednesday October 18, 2017

Session 1
1A/ Intro to Sovrin
1B/ Two Short Talks on Capabilities
1C/ Distributed ID System Patterns with Distributed Systems
1D/ DIF – Universal Resolver + Universal Teistrar (DID's across blockchains)
1G/ Minute Money? A new currency based on A NEW PARADIGM – Time AS Money
1H/ DNS Based OpenID Connect Discovery

Session 2
2A/ Triple-blind Brokered Identity Federation
2B/ First Party World: People in charge via GDPR by 25 May 2018 – Calling Lawyers & Geeks
2C/Ecosystem Map – Explore Where Could It Go – Insight Treasure Hunt
2D/ Estonian ID Cards Internet Voting
2G/ DIF Identity Hubs Deep Dive & Spec Feedback
2H/ NO Identity – ID As A Collection of Verifiable Claims
2I/ Gender and Diversity in the Valley – A Listening Circle to talk about all the stuff

Session 3
3A/ Group Privacy
3B/ Building Community for SOVRIN and Hyperledger Indy
3C/Dgital ID in Cities – Use Cases and Pilots
3E/ How 'Private Sharing' Breaks the See-Saw or Do More With Data, Not Less or Thank You GDPR
3G/Intro to Cryptocurrencies, Tokens, Token Distribution Events, and Tokennomies #ICOs
3H/ Where Is My Personal AI?
3I/Verified Organizations – Bootstrapping a Self-Sovereign Identity Ecosystem via Government Services for Organizations
3J/Proofing + Assurance Combo – ID Proofing & Standards for Identity Assurance Across Systems ?
3K/Intuition Session Including Ego Identity to Field Identity

Session 4
4A/OIDF RISC Working Session
4B/ Identity For All
4F/ Decentralized Identity, OAuth, OpenID and How They Can Fit Together
4G/ Know Everything About a Customer, But Know Nothing – How intentional amnesia can be good for Security & Privacy
4H/ Science of Persuasive Communication
4I/ Mental Models of Identity
4J/How The GDPR Is Making Me TRACK MORE

Session 5
5A/ OpenID Working Group: Fast Fed Intro and Discussion
5B/ Identity Smart Contracts on Ethereum
5C/ MANIFOLD – A Self Sovereign Internet of Things Platform #Picos
5D/ Fluid Boundaries of SELF and implications for self-sovereign identity
5F/ Reputation as a Primal Use Case for Data Intensive Applications of Decentralized Identifiers
5G/ Distributed Token Validity – A Different Approach To Local Govt
5H/ Digital Identity of K-12
5J/ OIDF RISC Working Session

Photo credit Prabath Siriwardena @prabath Oct 17 #IIW XXV today's sessions

~ After ~

Photo credit COMRADITY @comardity Oct 17 #iiw the unconference Agenda

Thursday October 19, 2017

Session 1
1A/ A Bank/Telco Use Case Exploration – Working Session to Go Through Project Details
1C/ Lost Identity – Post Disaster Recovery (Nor Cal Fire, Puerto Rico)
1G/ Bringing It Together – DID + What We Already Have = How Do They Work Together
1H/ Autonomous Agents & Identity Delegation (JHV Research Project)

Session 2
2A/ Alexa Identity – What Would You Want?
2F/ The GS1 Identity System
2G/ Indieweb.org
2H/ Sovrin Ecosystem
2I/ 500 Years of Identity & How Does Nature Do Identity?
2K/ Intuition Part II

Session 3
3A/ Rat Hole (Round #3) OIDF RISC UG
3C/ Signatures and Selective Disclosure (show me the math)
3D/ Networks v. Ecosystems & Identity
3F/ Accountability vs. Safety in Permissioned Decision Systems
3G/ What Should Large NGO Organizations Be Doing to Help? What Role Should We Play in This Ecosystem?
3H/Discussion on Constrained Devices and OAuth2/OpenID Conn – Including JCOR!
3K/ Fashion Wearables IOT DEMO ~ 360 Fashion Network www.360FASH.com

Session 4
4A/DKMS – Key Recovery Summit: Biometric Recovery, Cold Storage, Social Recovery
4C/Using DIDs to Bootstrap Scondary Communications Channels and Move to New/Different Protocols
4F/ The Human O/S Defending Privacy by Understanding I.T. Forces and Managing Human Nature

Session 5
5F/ Reputation II – Data Intensive Applications Using DID's
5G/ How Many Blockchain Tokens Will There Be?
5H/ Diversity In Digital Identity
5J/ Identity + Reputation, Enabling New Business Model for Open Source Projects

Tuesday October 17

Introduction to OAuth2 (101 Session)

Tuesday 1B
Convener: Justin R.
Notes-taker(s): Anik

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

OAUTH

The presenter has written a book on OAuth2. 39oauth2 OAuth2 in action.

A lot of OAuth out there right now.
What is OAuth?

- An Authentication method
- Token instead of actual credentials.
-

OAuth, acc to the spec, "authorization framework.." (Take from notes)

Letting 3rd party app get access on behalf on someone.
-not an authentication protocol

It's a delegation protocol. Giving an app the permission to act on one's behalf.

Traditional OAuth:
Resource Owner (RO). — has access to —> Protected resource (PR).

OAuth was designed for http.

(Client app)
RO ——> CA ——> PR

<u>One way</u>: to give CA, the actual credential
- no way for PR to identify who is asking for it.
- no way for access control (read only)
- only way to remove access is to change password
+ simple to build
- credentials given to CA can be used maliciously.

<u>Second way</u>: In the enterprise world, a thing was described as "Client Key" . It hasn't taken any consent from the user. No way for the PR to confirm it came from user.

<u>Third way</u>:

Special passwords to be given to CA.
+ nice and limited
+ access control is better

- usability sucks (user can't remember all the passwords)

Example study: Google Subversion

Fourth way:

Fix usability
A new component: T (Authorization Server) to manage credentials, knows who we are, what we are delegating, who we are we delegating to. A special password called: Auth token.

OAuth uses http a lot, we need to know how http works. Http includes a lot of specialized info embedded into it, but people don't speak http. So we need a thing called front channel communication. It works when a client (browser) wants to talk to AS. And As redirects the browser to C through to PR.

Downsides: Browser can leak info, we don't have any control on it. OAuth tackles it by saying, Browser can do only specific thing at specific time.

When we are doing Auth flow. Traditionally all parties were web servers.

Front channel redirect:

ClientId, Scope (a bag of strings that gets passed around., defined by API)
We can start a session between User and AS, which warrants a login. AS knows who the user is, who the client is, what the request is (scope)
But still AS, can ask Client C wants access to PR, should we allow that?

Answer to whether one has used OAuth: is almost always yes.

Q : What's Scope?
A: Any resources which will identify AS to the PR can be called a scope. In practice, each individual resource has a different scope.

Now User can confirm that she wanted to allow access, can have better access control.

Delegation is not completely independent of security, its a subset of it.

AS handles a major part of complexity of the protocol. Earlier a lot of complexity was supposed to be in C. But C only care about security only when it comes in their way. They all want it, but only to do what they actually want to.

Now, Browser knows which client to talk to. AS knows what scope the client is supposed to have. Even if a C is allowed to get that scope, user may still deny it

Q: How is the client id protected?
A: Its public.

Q: Can I use someone else's client Id?
A: Yes, we don't know what prevents us yet to come in this session.

AS takes in RO, C, PR and generates an Authorization code (AC) which is a random string.

User talked to As -> AS gives back a AC (front chanel redirect) -> User talks to Client and passes the AC -> C talks to AS (which only allows particular AC to particular clients)

AC is not enough on its own. There is a client secret (CS) given to C which needs to authenticate to AS. Which, in addition to AC, makes sure AS authorizes the call). CS is not known to the user.

Now AS replies back with an access token (T) back to C, which it passes to PR to show access. It is opaque to the client, so the client never gets to know what permissions were provided (it hopes it got what it asked for)

In all cases, Client is completely dumb. They will always say AuthToken doesn't work in all failed cases (Not enough permission, token expired etc)

Criticism : AS is a single point of failure.
Defense: Its ok to have one secure single point of failure than having multiple places to make things wrong.

Through Open Auth, Client never gets to know anything about the user. It can do so through other additional info.

Optimizations:

1. What if client is running inside the browser. Now "implicit flow" comes not picture, now no need of a Client secret. Its less secure, it beats cookies in security, but is susceptive to various attacks.
2. API key can be used in applications directly. Instead of user's password apps can use API keys

DHS S&T IdM Program's R&D, Goals & Overview

Tuesday 1C
Convener: Anil John
Notes-taker(s): Heather Vescent

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

Interested in "What is the role of government in the identity ecosystem?"

The more choices in the environment, the more in the competitive environment.
Identifying the market failures, mitigating to fix it and make sure enough work to have a competitive environment going forward.
Act as a trusted agent/resource for solving government identity problems.

An R&D organization - 1 to 5 years out. Not interested in solving current problems, or addressing market problems that can be corrected by the market.
Problem driven research organization.

Stakeholder needs: large buckets that we say we need
Not a lot of work in the adapt area. having systems and capabilities that operate under duress, when they have been compromised, etc. e.g. that have product/technology resiliency.

A practical model for digital identity and privacy
Digital Identity Model: sign in, verified person, consent and authorization, trusted digital identity, trusted and standardized infrastructure.

It's important to know what you don't want to do. So this outlines the bounds of the work at DHS S&T.

Can this pain be solved using current technology (what is in the ecosystem)? Solved by warm introduction, but not funded. Interested in the current state of technology to map and give a warm introduction.

More involved where the current technology can not solve the problem. In these cases, I am more of a VC.

Private Sector engagement:
Technology awareness
Talent sourcing
Transition partnership

Leveraging the private sector.
R&D Valley of Death - where a MVP but it is not enough to be market viable. Needs to be productized.
Second valley of death - have a product, have a company, but don't have a good customer. So you can't get funding. Iterate, validate or pivot.

Multi-track.
Fund multiple projects that are solving the same problems. This supports multiple diverse solutions and a competitive marketplace.

Question about Open Source. If there is a community around the open source, then sure, but if not already in place, concerns.

Prefer agile iterative development to waterfall. I want to see iterations as it is developed.

Success is, the customer need is addressed.

Quarrel - bridge btw FIDO and certificates
NFC for Pax - a secure channel over NFC, next step is to apply to bluetooth model.
Interest in non-carbon based lifeforms. e.g. spoofing.
IOT, security, blockchain projects. Key management system. funding a decentralized key management system. flexible ledgers. data that is validated as true and right, to be able to stand up in court. counter fraud and anomaly detection.

Decentralized Identity Foundation (DIF) technical/org recap & roadmap discussion … followed by DIDs in depth (with review of contentious bits)

Tuesday 1F & 2F
Convener: David Buchner followed by Drummond Reed
Notes-taker(s): Scott Mace

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

Daniel Buchner on Decentralized Identity Foundation

Done quite a bit of work in the five months since founded.

Engineering-driven organization, not like a SDO like W3C.

Instead, focusing on developer tools, interoperable specs and implementations.

The goal is to pave the cow paths of decentralized identity.

Right now it's disparate, a lot of interest, but people want to pick one of these systems, not hitch wagon to something that won't work with anything else in the future.

Full disclosure I work at Microsoft.

The ecosystem building is the goal with DIF.

If you're a contributor, just sign an agreement saying code will be Apache 2, W3C agreement, Creative Commons.

We've added 20 new members. Microsoft helped envision this but we have other competitors, such as an blockchain. IBM. Also Hyperledger. Not like we don't talk to each other, but there is competition in the market. Both have now joined DIF. A signal to the market that we may be competing, but we are agreeing there should be a shared vision for this thing. Inherently, no one owns decentralized identity. For this segment of blockchain-based ID systems, we have to align.

Identified 4 key deliverables.

- Decentralized identifiers
- Universal resolver, a DID might be rooted in one system or another is still resolvable.
- Universal registrar, a separate server. Modules to create DIDs on various systems.
- Identity hubs. DID-based personal data stores. Not a blockchain type system.

Marcus … landed an actual implementation of the Universal Resolver. Something you can use today to resolve DIDs today. Truly one thing as an oracle to find DID information.

Roadmap

What do we want to target in next six months. To show the market they can trust the tech.

By 1/1/18, land core properties and features of the DID spec. A few contentious bits.

3/1/18, universal resolver in two major languages; 1 already is Java. with client libraries for all mobile environments. And support for 3+ DIOD drivers.

4/15/18: Identity hubs, reference implementation

Show it 5/14/18 at Consensus main stage in New York. Presentation and demo showing the interoperable layers working together.

We want at least 3 DID methods being used between two entities and a user, to issue/verify attestations that drive a real world use case.

We want you to submit 1 page with desire for inclusion in this demo. And what resources you are willing to allocate.

Want to participate? Commit key dev resources. Help produce the demo and manage execution on the demo.

Q: DIF have an opinion on user experience?

A: We're trying not to do that. We're not trying to build a product. Making sure underlying fundamental bits are there, table stakes. A reference implementation.

Q: This is all new stuff. If there's no exemplar usage scenarios, how do you know functionally it is what the market needs?

A: We've worked on use case scenarios. Some data we keep; lots we're willing to share. I.e. one type of claim may be something a bank has a big need for. At the same time, we're also building low level enough stuff, we're not excluding new use cases.

Q: Part of Indy?

A: DIF is its own thing under the Joint Developer Foundation. We are technically a nonprofit LLC under JDF.

Q: What kinds of identity are you thinking of? IoT devices? AIs? No assumptions whatsoever?

A: More than half skew toward human identity. We would help they support devices and objects.

Q: What are you resolving to?

A: Go to the Universal Registrar server package. Creates decentralized identifiers. Each driver corresponds to a method that corresponds to a chain. It has its own way of inspecting the chain and coming up with the answers; here are the keys. You can challenge them. We want to encourage lots of systems, Etherium 745, standardish way on Etherium to do DID, if that gets accepted. Finding data off-chain. Drivers. I.e. replace ICANN or other centralized naming systems. The resolver is what you would run. DID document, control document has service pointers in it. It's a way you can find IDs, challenge them using keys that are there, find where data resides.

Q: SOBs?

A: We look at the community, says I'm SOB. Who has the most adoption. We will sign a bundle that SOB is this driver. It's market adoption, not an international standard.

Q: What is wrong with the ICANN approach?

A: If they don't like your blog, you're gone. To have your identity turned off, we're talking about claims that could get you into hospitals. I think it's a human right.

Q: Denial of service concerns.

A: There's a way to do qualitative assessments based on attestations. You can run trust scoring. If it's all empty shell identities. To discern who's real and who's not.

Q: A list of not just use cases but also abuse cases. A detailed threat analysis.

A: That's something we want to do. Verifying the methods.

Q: Right now we have the concept of levels of assurance and auditors. Seems to me like different methods are going to possibly need different levels of assurance or auditability practices. What's the scope of DIF relative to this ability to meet the requirements of regulatory agencies?

A: DIF doesn't want to be involved in that analysis. We might encourage constraints. Such as proof of stake. We are not going to say we're only going to accept this or that. We might keep a log of good feedback to play into your DID acceptable scenarios.

Q: Dive in more on the identity hub. Related, is it assumed all identity hubs are in a public access as opposed to private? The name resolvers resolve to public things?

A: I'll show you an actual diagram of how they map together. May have multiple hubs for redundancy's sake.

Q: Are claims part of the identity hubs?

A: They're not super smart. They're untrusted. The likelihood is they can't issue claims, sign keys. If a government wanted to attest that someone was 25 years old, that DID, they would sign an attestation with their DID, now you have an object, go to the resolver, get both DIDs and the keys related to them and check the objects to see the signatures are tied the way they claim to be.

Q: Can the identity hubs run code?

A: I don't think scaled implementations would run it; it's a large attack surface. Go to Spideroak, secure storage, boutique hub providers.

Q: This could end up being a complicated mess for users.

A: What proof points are you looking for?

Q: What will the reference implementation be able to do?

A: Some storage, facilitate some messaging. You might want to present someone a document. Sign with your DID. How? You need an endpoint where you look it up.

Q: Scalable to billions of identities? Hubs, local stores?

A: No different than Dropbox on your phone or OneDrive on your phone. Microsoft may have much replicated.

Q: Why not use Dropbox?

A: It's more about the API and the permissioning flow, having the hub resolve and check the ID request. Acclimating piece of storage.

Q: Dropbox, I can provision a piece of data.

A: Dropbox owns your data.

Adrian Gropper: Public blockchains, private UMA.

A: Many economic reasons why large companies would give away free account, like they give away free storage or email. High traffic users would have to pay. You're still syncing to your own devices. I will have all my claims on phone. I might want large volume going to the cloud. It's for availability and scale.

Q: What is the value add of your switching, the first two boxes. If I have co-equal providers (i.e. email) different APIs, you've provided a way to smooth over that.

A: Yes we need to speak the same data language. Find me everyone in the world who wants to offer me a red car to buy. I need to be able to ask the same question. The hub says lets not create new APIs. Let's make the API not 1 to 1. Say you're Craigslist. We could recreate Craigslist.

Q: Craigslist doesn't need all that stuff.

A: I think the world will find it's very challenging for them in the next 10 years. It's a crawler.

Q: All the different personal data store providers, there could still be leakage of identity across platforms. We want storage to retain anonymity. We're building this on top of an imperfect backplane.

A: Why we're not creating a new API. The data is the schema. It's deterministic. We're saying reuse the APIs the world is already giving us.

Q: Email hacking scenarios. If they hack your email they own you. This creates appropriate segregation. An inflection point, figure out what is critical mass.

NOON SESSION CONVENED BY DRUMMOND REED

We define specific DID method: Defines structure & method of generation for the method-specific identifier. Globally unique among other method names.

DID method specs … IPIB not IPDB

Not all of those are blockchains.

Globally centralized key value store.

Each DID method will define its own access control.

Agents - do key management to establish trust, verifiable claims exchange

A method of implementing GDPR

Revocation is method specific.

This is a JSON alternative to Web ID (& SoLiD?)

GDPR authorities considering this workable.

Working with OASIS on key management protocols.

Q: How do you avoid name collisions in methods?

A (Buchner): Attestation, DIF believes you should link these two.

Drummond: A method that doesn't have a community behind it won't be viable. You're starting the Web of trust with communities.

Q: We don't have an example at scale yet.

Q: I have an example. Well-known ports.

Q: The registry came first.

A: We've developed a template for ID methods.

Q: Letters vs. numbers.

A: The goal is to provide a list of well-known services. And ways to create cryptographic proof.

App Auth RFC8292 BCP212 Q&A

Tuesday 1G
Convener: William D. & John
Notes-taker(s): Sarah Squire

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

Cookie theft and man-in-the-middle attacks are a big problem, and we'd like to solve them.

Currently token biding is implemented in Chrome, Edge, and IE. It's on by default in Redstone 2. Microsoft added it at the OS level, so IE inherited it because IE uses Windows' TCP.

Mozilla is looking at it.

Protocol flow:
User agent (UA) generates a key pair
SP is scoped by ETLD+1 (the top level domain and whatever string comes before that)

The UA key pair signs an HTTP header which sends mutually negotiated exported key material (EKM) to the SP, which can include the public key
SP creates a signed token with the public key of the device so you don't need to maintain the state at the server
Then when you receive a cookie that contains stuff that you signed, you can tell that it's not being replayed by a different browser.
This binding lasts until you remove the cookies for a particular site.

Question: When SP writes a cookie for the HTTP header, what is it signing?
Answer: It's signing the cookie, and putting the opaque value of the public key in the cookie

In the case of an IdP and RP using an OAuth flow, an RP can ask the user agent to provide its token binding ID to the IdP. In that case, the UA would sign over the EKM using both the IdP's token binding ID and the RP's token binding ID. Then it can create a token with proof-of-possession (a token that is only considered valid if it is presented by someone who can prove they have control of the private key associated with the public key in the token).

In the case of FIDO, the FIDO challenge response would include the token binding ID. The FIDO authentication server can then verify that it's using the right TLS channel and initiate a proof-of-possession challenge.

Q: Can you do it withe a PIV card?
A: No, all you get with that is mutual TLS to the user agent.

There are flaws in channel ID. Channel ID uses exported key material, so it's vulnerable to a number of TLS attacks. The FIDO specs still say channel binding, but they are subject to whatever the browser supports, so effectively, they're using the EKM flow.

Token binding is in the last stages of review before it becomes and RFC in the IETF.

Q: What about network hardware implementations?
A: Nginx and Facebook have implemented it. Layer 7 working on it. There is an apache module. There are complexities with Java that Oracle hasn't fixed. Java doesn't implement the latest version of TLS. You can implement it through a reverse proxy, and the working group is working on a standard for that. If you're doing load balancing, you have to do that anyway because that's where it terminates.

Blockchain Democracy

Tuesday 1H
Convener: Dave Sandford
Notes-taker(s): Dave Sandford

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

Slide Deck has been copied and pasted in:

Blockchain Democracy

Can a blockchain platform be designed to support
Enlightenment era goals for democracy?
"Code is Law" Lawrence Lessig

State of democracy – threats and opportunity

- Behavioral science is being effectively leveraged to manipulate people to act in ways that may not be in their own best interest.
- Political polarization akin to tribalism – so that the determination to support 'our tribe' and oppose 'the other tribe' can be more important than what the tribe stands for or does. These tribes can act against the good of the tribe, nations, or the world without necessarily losing followers.
- Well-funded shadowy organizations are trying to use machine learning algorithms, bots and disinformation to effect political processes. Unchecked their effectiveness is likely to increase.
- In one sense it should be scary, as in a call to action. In the other sense if we were to react to it out of fear – that would guarantee a bad decision making process.
- Trump has demolished the 'Overton window', so all sorts of new things are possible

Blockchain Cambrian Explosion

- World changing 'positive sum games' are continuing to be created and evolved on blockchain related platforms. Intersection of machine learning and blockchain could be a lot of autonomy.
- Fat protocol thesis suggests that distributed autonomous algorithms and protocols will create value, produce multi-sided networks and support machine learning and crowds
- World telemetry - Any state in the world (e.g. IoT) that can be measured and transmitted can either be: written onto an immutable ledger or be an event within a smart contract state machine.
- This evolution is very early in the process – both with:
  - ❑ new platform algorithms (proof of work, proof of state, sharding, Spectre, Ghost, Plasma, etc.) and
  - ❑ new applications and services, app token, where ICO value = new service (ERC20 token std, swarm, whisper, golem, ENS, augur, uport …)
- Which of these 'organisms' do we most want to survive and thrive? What vulnerabilities and exploits are likely to be spawned within this ecosystem and are we smart enough to build in the appropriate corresponding 'immune system' response mechanisms?

Talk about democracy in blockchain space

- Scalable consensus algorithms (may or may not help speed convergence of human consensus processes – more on that later)
- "How to build a democracy on the blockchain" is a tutorial for a type of democratic smart contract on Ethereum (https://www.ethereum.org/dao)
- Prediction markets support responsible governance (related to Robin Hansen's 'Futarchy: Vote Values, But Bet Beliefs' (http://mason.gmu.edu/~rhanson/futarchy.html)
- 'DAOs, Democracy and Governance' by Ralph Merkle (http://merkle.com/papers/DAOdemocracyDraft.pdf)

Note: Need to be very careful on which functions are automated and which are not, however a Decentralized Autonomous Organization (DAO) can be designed to follow rules, exist as long as it provides valuable services, can use it's own crypto and pay money, execute contracts and CAN be made radically transparent

Toward a New Enlightenment

"To make a better future, you have to believe in a better future" Ted Nordhaus

Democracy as an enlightenment era experiment that worked best when viewed as an experiment and to the extent it embraced these values:

1. Democracy – Government derives its power from the consent of the governed. That some form of decision making by the people – perhaps some of it by proxy - could move us in the direction of the utilitarian ideal of greater good for the greater number.
2. Science – Evidence over ideology, in support of democracy, universal opportunity, prosperity. Science may be the only dogma that is self correcting.
3. Universal Opportunity – That every human gains rights reflected in legal decisions. I argue for the goal of 'universal opportunity' as a counterpoint to identity politics. John Rawl's veil of ignorance thought experiment "you do not know who you are, and will not know who you are, until after the laws are passed. Yet, you are expected to pass laws that will benefit you." may be a valuable litmus test.

Note: Lots of other enlightenment ideas and their evolution are critical to democracy (e.g. Cesare Beccaria writings on criminal justice) but I chose these three

Ethical Effective Opportunities

- There are a lot of undiscovered possibilities at the upper right quadrant of ethical and effective
- Open immutable ledger is the blockchain mechanisms closest to a free press
- What kind of code should be law? It should be under version control and hashes of changes written to an immutable ledger. Automatic sunset if it doesn't come within a defined margin of pre-stated measurable goals (or other Internet bake-off similar process)
- Application of deliberate practice – purposeful, focused and systematic
- Whether it is teaching ourselves or teaching our machines, faster incremental feedback, always refining definition of the goal as well as the quality of the error signal

Kohlberg's stages of moral development

	View of Persons	Social Perspective Lvl
6	Sees how human fallibility and frailty are impacted by communication	Mutual respect as a universal principle
5	Recognize that contracts will allow persons to increase welfare of both	Contractual perspective
4	Able to see abstract normative systems	Social systems perspective
3	Recognize good and bad intentions	Social relationships perspective
2	Sees that a) others have goals and preferences, b) either conform to or deviate from norms	Instrumental egoism
1	No VOP: only self & norm are recognized	Blind egoism

Voter Empowerment 'DemosCoin' Design Constraints

- Require agreement to act in accordance with these 3 'first principle' beliefs to become a voter, these principles should be more important than scaling
- One person/One vote
  - ❑Means no bots voting
  - ❑No cases where one person is voting multiple times with different personas
- This implies enough centralization to maintain and manage a central eligible voters list and it's associated lifecycle
- System design resilient to hacking, collusion, and other adverse system effects (new threats – DAO, machine learning, bots; old threats anti-democratic humans (e.g. Kekistanis))
- Rapidly evolvable design in response to voter will
- Transparency, privacy and auditability granularly applied by specific technical mechanisms as appropriate

Voting Technology Requirements (cont'd)

- Try to avoid tyranny of majority, higher level of consensus is always preferable to a simple majority
- Pseudonyms should be reasonably protected, however since they will be compromised and people can make them public, any voter should be able to trade-in pseudonymous keys for a new pair
- Transparency by design - voting results should be a public record and a person should be able to verify their own pseudonymous vote as well as the tallies
- Voting system public data should be immutably public, voting system private data should be hard to compromise
- Telemetry should be designed to validate, audit and provide forensics for events and should write to both immutable private and public chains
- Critical code may need to be evaluated with formal methods (e.g. TLA+, SCADE)

Evolvable design in the laboratory of ideas

- DevOps style vote/referendum to 'social contract' code deployment pipeline
- Faster and shorter feedback loops for all segments of the pipeline
- More, smaller and faster experiments, fail fast, A/B testing
- Multiple democracies – competing and cooperating, but most importantly learning from each other
- All code and documents should be both human and machine readable
- At every stage of this vulnerabilities have to be assessed. Threat assessment should include the platform(s) can be attacked by anti-democratic, anti-science and/or anti-equal-opportunity forces
- Countermeasures?
  - Truth bots that identify themselves as bots and point to evidentiary sources
  - Machine learning watching for anomalies

Democracy as a platform for what

- First of all 'dog fooding' – using the platform voting/consensus method to decide new features for the platform (somewhat meta)
- Democratic process – Continuously evolving mix of wet logic (human), dry logic (smart contract automation)
- Transparency > distributed ledger, Security/privacy > encryption and Auditing > zero knowledge proofs
- Exploring process alternatives – What decisions need votes? How to ensure all decisions and work driven by the common good? Votes might not be binary, multi-armed bandit
- Top of the greater good lifecycle - research into what works:
  - Voter driven (and funded?) research
  - Data science platform, support for SciPy, voter driven and funded
  - Machine learning
- Bottom of that lifecycle – Implementing things that research and evidence shows will improve greatest good for the greatest number

Correctly Empowered Crowdsourcing

- At a minimum topic forums with moderators to support the values of democracy, science and equal opportunity
- Ideally a sort of legislative process – allowing decisions to be made by those who self-select as understanding and caring about the issue at hand
- The primary characteristic of great teams is psychological safety, forums should strive for that – as well as the perverse joy when evidence invalidates ones own preconceived beliefs
- In general, forums should be publicly readable, but only postable to by voters – thus creating incentive for people to become voters
- Reputation metrics (aka Karma) might provide value, but should be approached carefully to avoid non-egalitarian perceptions or reality

Blockchain Architectural Principles

- Decentralization performance trade-off. Different chains have different processing overhead, use the lowest you need for the function required (i.e. public is expensive)
- Processing and services should be 'paid for' by or as close to the protocol layer as possible, particularly for expensive highly redundant processing
- If processing (smart contracts) or writing does not have an explicit functional need to be on chain – it should not be
- Trust engineering – always looking to increase the Nash equilibrium within the overall system and looking for threats that could lower it
  - Autonomous, open source, transparent trust at low processing cost preferred
  - Cost of maintaining and recovering trust can be lowered by good design
- Both public and private immutability are required
- ZKP/ZKSNARK – may be needed for auditing
- Contracts should not be subject to interpretation and self-verifiable contracts are preferable to human verification
- Contracts are only as trustable as their data sources or 'oracles'

Money and Funding – Some ideas

- Most successful blockchain platforms build services that pay for their operations and maintenance at the protocol layer – need to continue to look for funding models like that in the greater good space
- It might cost a reasonable recurring tax to become a voter
- DemosCoin – App token to invest in democracy and the common good? 'Gas' pays for implementation of common good initiatives – a more accountable charity model perhaps
- Funds spent as the voters decide, presumably mostly to create code and run it
- Tax democracy platform revenue generating automata
- As passive and/or automated income is created on the platform, this could go to DemosCoin holders and/or tax is lowered and eventually, slow ramp into UBI for voters

A Few of Many Open Questions

- What parts of the democratic process are critical for humans to be involved and which parts are better once they are automated?
- Lots of alternative voting, polling, and consensus models that need to be evaluated for their effectiveness in improving the quality of decision making?
- When should the need to converge on decisions quickly be more important than following an open, egalitarian process that might be slower?
- How important is voter pseudonymity? How easy is it to protect?
- And anything else related to theory of democracy or implementation of it in a 'code is law' world.

Introduction to OpenID Connect (101 Session)

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

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

Notes posted as the last bullet item at: http://self-issued.info/?p=1738

Is Your Data Legal? Meaningful (oxymoron?) Consent

Tuesday 2C
Convener: John Wunderlich
Notes-taker(s): Sean Bohan

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

Purpose - give the IIW community a breakdown of GDPR, it's impact on the EU AND outside the EU

Notes:

- IAPP Primer on GDPR:
  - https://iapp.org/news/a/the-gdpr-in-20-minutes/
- General Data Privacy Regulation - EU personal data regs
- 75% of most companies use of personal data will be illegal
  - What does this mean for the information economy?
- Under GDPR May 25, 2018 is the big day where the regulation AND consequences go into effect
  - $20MM OR 4% of global revenue if an organization doesn't comply
- For EU citizens, whether they live in the EU or are travelling
  - might also apply to citizens of other countries living/visiting in the EU
- If you process personal data on someone in EU or an EU citizen you are required to comply
- There are some who believe the law isn't well defined enough
- Expanded definition of Personally Identifiable Information (PII)
  - Info about or in circumstances could be about a person
- Really important - Article 6: Lawfulness of Processing
  - Reasons/Rules why a company *could* process your data lawfully
  - See graphics, but the lawfulness includes:
    - Consent from the user
    - Contractual Obligations
    - Legal Obligation
    - Protect a Person
    - In the public interest
    - legitimate interest of the controller

- For any reasonable enterprise, the last choice of lawful processing is CONSENT
- Most will want to use this as a checklist
- Consent receipts
- 2018 - YEAR OF THE BIG DATA FLUSH
- No profiling clause is critical to advertising
- Solving problems with auditability
- Rights for Privacy under GDPR
- Right to be forgotten, erasure, mobility
- Can't use arcane rules to lock data in
- No great technical issues with GDPR - lots of compliance issues
- Resistance isn't technical - it is cultural and commercial
- Is "information sharing agreement" a term of art?
- In GDPR Consent must be "free and informed"
- Consent receipt - there is a spec from Kantara
    - Human-readable, JSON format
    - New WG @ Kantara: Consent Best Practices
- There are those just waiting to file lawsuits over this once the law is in effect
- Pretty good chance no one who take an ethical and informed approach to personal data will get in trouble
- Lots of privacy law based on "fair information practices"
- Article 29 Working Group
- Data Protection Impact Assessments
- Data Controllers vs. Data Processors
- Will users face "consent fatigue"?
- There are UX problems and there isn't UX research on how users will react/impact new GDPR requirements
- MEF Trust Study: https://mobileecosystemforum.com/programmes/consumer-trust/global-consumer-trust-survey-2017
    - Rise of the reluctant sharer
- "17-25 year olds don't care about privacy" has been proven wrong
- Social Graph Data is very valuable
- Are governmental orgs / departments exempt? Maybe
- 1 rule for all of EU
- GDPR may enable businesses to do more with less data
- "Will issue X be covered under GDPR?"
    - ASSUME YES

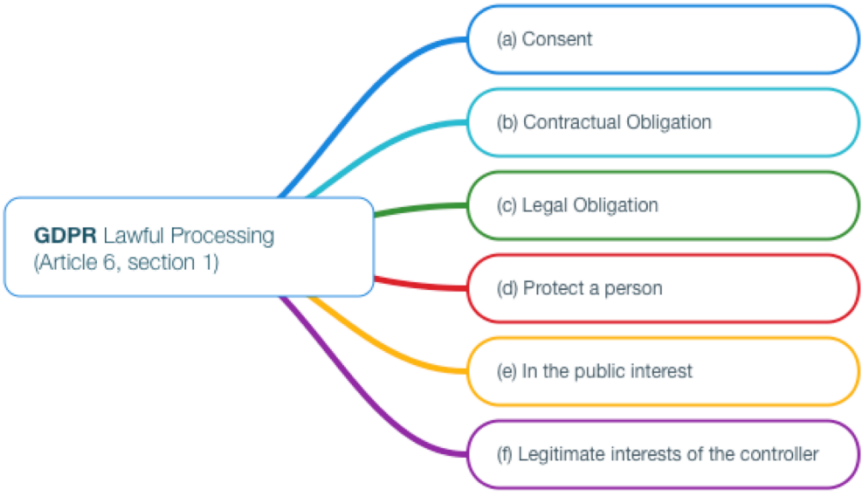
Article 6
Lawfulness of processing

1. **Processing shall be lawful only if and to the extent that at least one of the following applies:**
   - a) **the data subject has given consent to the processing of his or her personal data for one or more specific purposes;**
   - b) **processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;**
   - c) **processing is necessary for compliance with a legal obligation to which the controller is subject;**
   - d) **processing is necessary in order to protect the vital interests of the data subject or of another natural person;**
   - e) **processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;**
   - f) **processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.**

- **Point (f) of the first subparagraph shall not apply to processing carried out by public authorities in the performance of their tasks.**

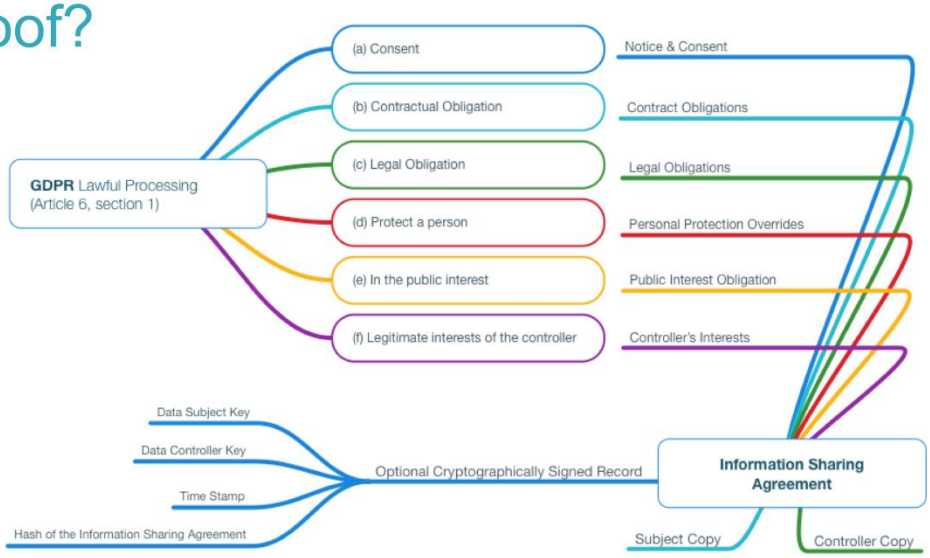
JLINC LABS

Lawful Processing



JLINC LABS

Proof?

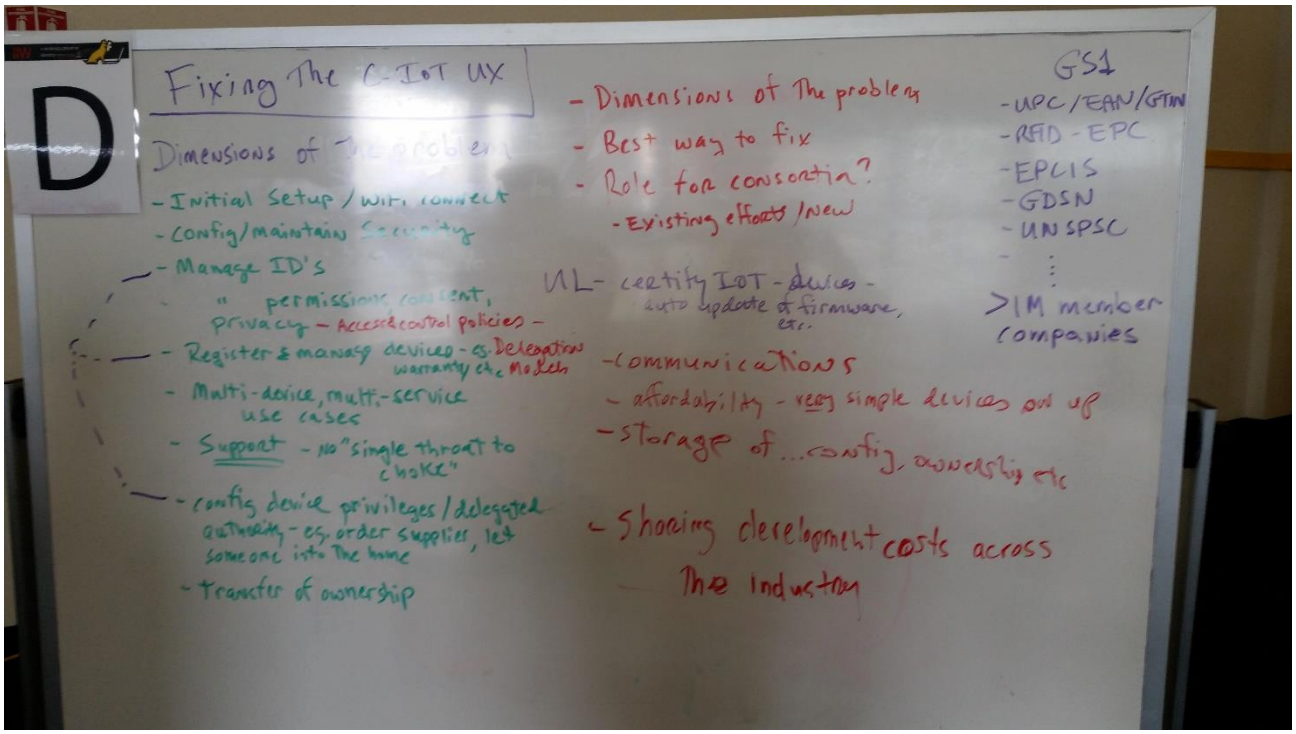


JLINC LABS

'Fixing' The Consumer IOT/Smart Home User Experience

Tuesday 2D
Convener: Bill McBeath
Notes-taker(s): Bill McBeath

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



Six Degrees of Freedom

Tuesday 2E
Convener: Darrell O'Donell
Notes-taker(s): Darrell O'Donell

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

I hosted a session at IIW 25 yesterday covering off Tim Bouma's "Digital Identity: Six Degrees of Freedom" (source: https://medium.com/@trbouma/digital-identity-six-degrees-of-freedom-4dbccbd8cd5)

- Freedom of **Credential**—I should have the ability to use whatever credential (login, etc.) that ensures that I am in control.

- Freedom of **Identity Data**—I should have the ability to decide what identity information to use to identify myself.
- Freedom of **Authorities**—I should have the ability to choose which authorities (or lack thereof) I require to vouch for me on my behalf.
- Freedom of **Disclosure**—I should be able to decide which identity information (or subset of information) I give to others.
- Freedom of **Consent**—I should be able to decide how and when my identity information can be used, including the ability to fully revoke its use, if so be.
- Freedom from **Control**—I should have full agency over the decisions relating to the above in the identity system I choose to use.

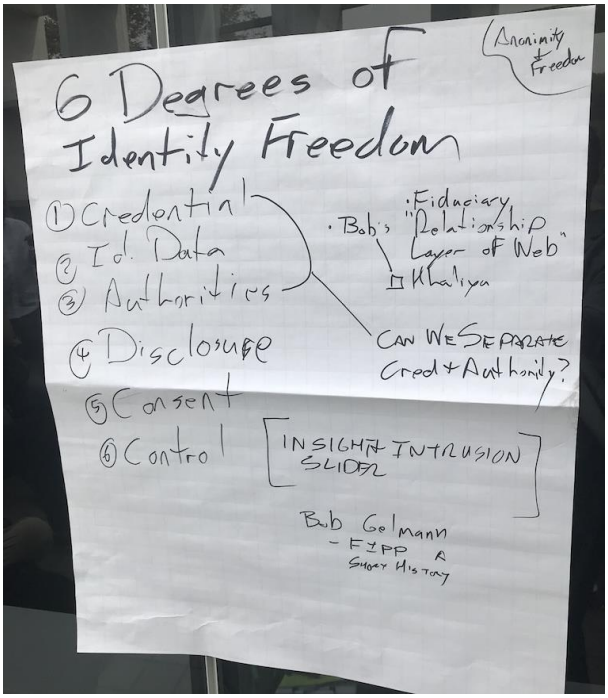
Tim closes with the idea that I likely won't have total freedom on all of these dimensions. The point of this is that there is a conscious starting point created.

My premise for the discussion was that there is a continuum in each dimension. Depending on my use case I may have the freedoms I want but likely not in all dimensions.

Example: I am paying cash for lunch at a taco truck. I have most of the freedoms under my control, but if a purchase is in USD, my Freedom of Authority has been picked for me - and I need to be ok with that or walk from the transaction (no taco for me).

Some further reading was recommended during the fairly well attended session:
- Reference to a "Relationship Layer of Web" document that I can't find.
- Bob Gellman's short history of FIPP. https://bobgellman.com/rg-docs/rg-FIPshistory.pdf

We bounced through multiple use cases and the 6 degrees concept held up quite well other than some relatively fine, and partly pedantic, disagreement. For my use Tim's 6 Degrees are a great starting point.



The use cases that we floated ranged:
- Making a purchase from Amazon of something like a book. In theory very little freedom is lost here - Identity Data is currently constrained but that may be a relic of how things have always been done. Amazon creates the Credential.
- Making a purchase from a vendor of a food product. There are needs to potentially share more information here in the event that there is an urgent need to contact the end user (e.g. food contamination issue).
- Creating a bank account on a simple KYC basis.

Further I wanted to understand if the dimensions withstood debate. They did.

Darrell @darrello
darrell.odonnell@continuumloop.com

Token Binding for Cookies – OpenID Command OAuth

Tuesday 2G
Convener: John B
Notes-taker(s): Sarah Squire

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

Cookie theft and man-in-the-middle attacks are a big problem, and we'd like to solve them.

Currently token biding is implemented in Chrome, Edge, and IE. It's on by default in Redstone 2. Microsoft added it at the OS level, so IE inherited it because IE uses Windows' TCP.

Mozilla is looking at it.

Protocol flow:
User agent (UA) generates a key pair
SP is scoped by ETLD+1 (the top level domain and whatever string comes before that)
The UA key pair signs an HTTP header which sends mutually negotiated exported key material (EKM) to the SP, which can include the public key
SP creates a signed token with the public key of the device so you don't need to maintain the state at the server
Then when you receive a cookie that contains stuff that you signed, you can tell that it's not being replayed by a different browser.
This binding lasts until you remove the cookies for a particular site.

Question: When SP writes a cookie for the HTTP header, what is it signing?
Answer: It's signing the cookie, and putting the opaque value of the public key in the cookie

In the case of an IdP and RP using an OAuth flow, an RP can ask the user agent to provide its token binding ID to the IdP. In that case, the UA would sign over the EKM using both the IdP's token binding ID and the RP's token binding ID. Then it can create a token with proof-of-possession (a token that is only considered valid if it is presented by someone who can prove they have control of the private key associated with the public key in the token).

In the case of FIDO, the FIDO challenge response would include the token binding ID. The FIDO authentication server can then verify that it's using the right TLS channel and initiate a proof-of-possession challenge.

Q: Can you do it withe a PIV card?
A: No, all you get with that is mutual TLS to the user agent.

There are flaws in channel ID. Channel ID uses exported key material, so it's vulnerable to a number of TLS attacks. The FIDO specs still say channel binding, but they are subject to whatever the browser supports, so effectively, they're using the EKM flow.

Token binding is in the last stages of review before it becomes and RFC in the IETF.

Q: What about network hardware implementations?

A: Nginx and Facebook have implemented it. Layer 7 working on it. There is an apache module. There are complexities with Java that Oracle hasn't fixed. Java doesn't implement the latest version of TLS. You can implement it through a reverse proxy, and the working group is working on a standard for that. If you're doing load balancing, you have to do that anyway because that's where it terminates.

Implications for the End User of How You Design a Blockchain for Digital Identity

Tuesday 3D
Convenor: Cara LaPointre
Note taker: Lara Fishbane

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

What are the decisions you make in building a blockchain that have implications for the end user?
Never put PII data on a blockchain, even if it's encrypted
You can put a hash of the PII
Hashes are immune to quantum attacks
Cannot erase anything you put on the blockchain
Chance of protecting it
Hash can verify that it's correct

How can the end user have access to the data?
Whole point of the blockchain is to make it immutable and accessible

What are ways that if you do have the data, is there any way to still make it transparent?
Can be reflected to them on a UI
Log into system, a lot of standardized ways
Person needs login credentials
Disaster relief mechanism

What information you need
Make sure that the end user gets the money
PII on the blockchain or link to it? Who are the nodes?
Does not allowing leakage

Do you even use a blockchain?
The distinction with a vulnerable population is that they might need to give data to access services.
In a disaster situation, you don't have any choice.
What information specifically goes in there? How do you choose authenticators or validators?
Decentralized authority / infrastructure

Blockchain technologies in marginalized communities
The access problem is actually very important. If I am the doctor, I can override certain rights that people usually have. What I need to rule out is how this happens.

Record what's been done. When has a doctor overridden your rights?
If you've decided that blockchain is it, then you need to decide which blockchain is it?
You have to make that decision too. Whoever is making the policy needs to have information about what types of blockchains there are.
Need to have person who understands security. Will a quantum computer break everything?
A system that looks at everyone. Literature or illiterate. System with trust built into it.
Identity to be documented, need trust protocol. Can't even have agency. Has to have trust protocol.

Are there certain identifiers that would be more beneficial than others?
Not actually helpful if everyone has the same name. These are cultural questions. A lot of our thinking about what identity is -- states and identities for people co-arose. Taking identity to places where people aren't related to the state.
Biometrics seem useful here.
Aren't we putting too much identity information into one place?
Are biometrics able to be put on a blockchain?

What does the person need to prove that they own it? Don't put public key, just put the hash of the public key?

What do people physically need to prove they own it? Private key.

Mechanism to recover private keys? A service to do it. Service doesn't have to work in a second.

Authenticate in a second.

Key recovery → split into different places

iRespond is trying to support people

Individual has agency over record?

What exactly is in your digital identity universe? You choose what you want to transact out. Need to think about all these ways you want to

What is the minimum amount of identity?

Are there things that are easier to ensure?

Blockchain that sits on top of the situation that suits the conditions.

Concern to the emergency team.

→ Think about a few kind of templates or overruling logic

Opting out is possibly all a matter or transparency. Ruling out through regulation.

Implementation matters. If we use a service, we assume it's private.

Same principle applies.

Public blockchain is anonymous. Decentralize for better transparency.

Public/private blockchain scenarios. Cut through different applications.

Probably not a bad idea. Recording somewhere.

There are some pieces of heathcare information that aren't anyone's business.

Understanding blockchain options. How do they apply?

How do you decide who the nodes are and what access they might have?
How does that affect the end user?

Will all the nodes have universal accessibility?

If you have a private blockchain and permissioned nodes, can everyone see all the information in it? The whole point of decentralized is that you touch what you can see. Pretty much the whole concept is that you decide.

In general, it's very difficult to see anything. The actual data isn't really on the blockchain.

Technical decisions for the person you're hiring and it's much better not to do that.

Give it to contractor? Let them build a road. If you don't want data to be seen, don't put it on a blockchain.

Give tools to policymakers.

What you need to do is get an expert to go out and evaluate these things

Need to have a competition so you can go out and shoot down other people's ideas

How do you protect the privacy of the end user is a good question, but it's too early to ask more detailed questions. Can't design a system. It's too early.

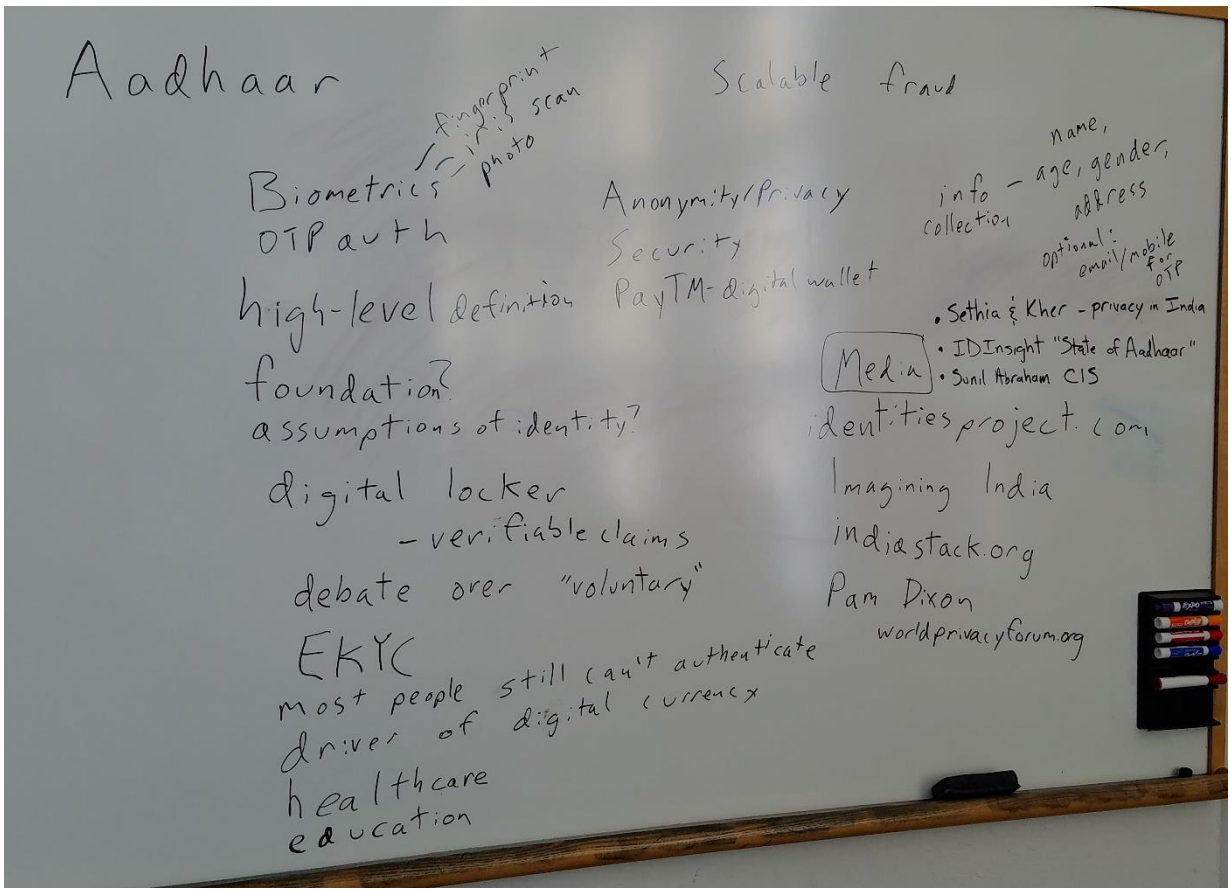
Who has access, interactions, move the data, encryption?

If a quantum computer was invented and became easily accessible, what does it do to your design?

Aadhaar

Tuesday 3F
Convener: Sarah K Squire
Notes-taker(s): Sarah K Squire

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



Information Sharing Agreements ISA - First Party terms that you and I prefer V 2.0 of the commercial web

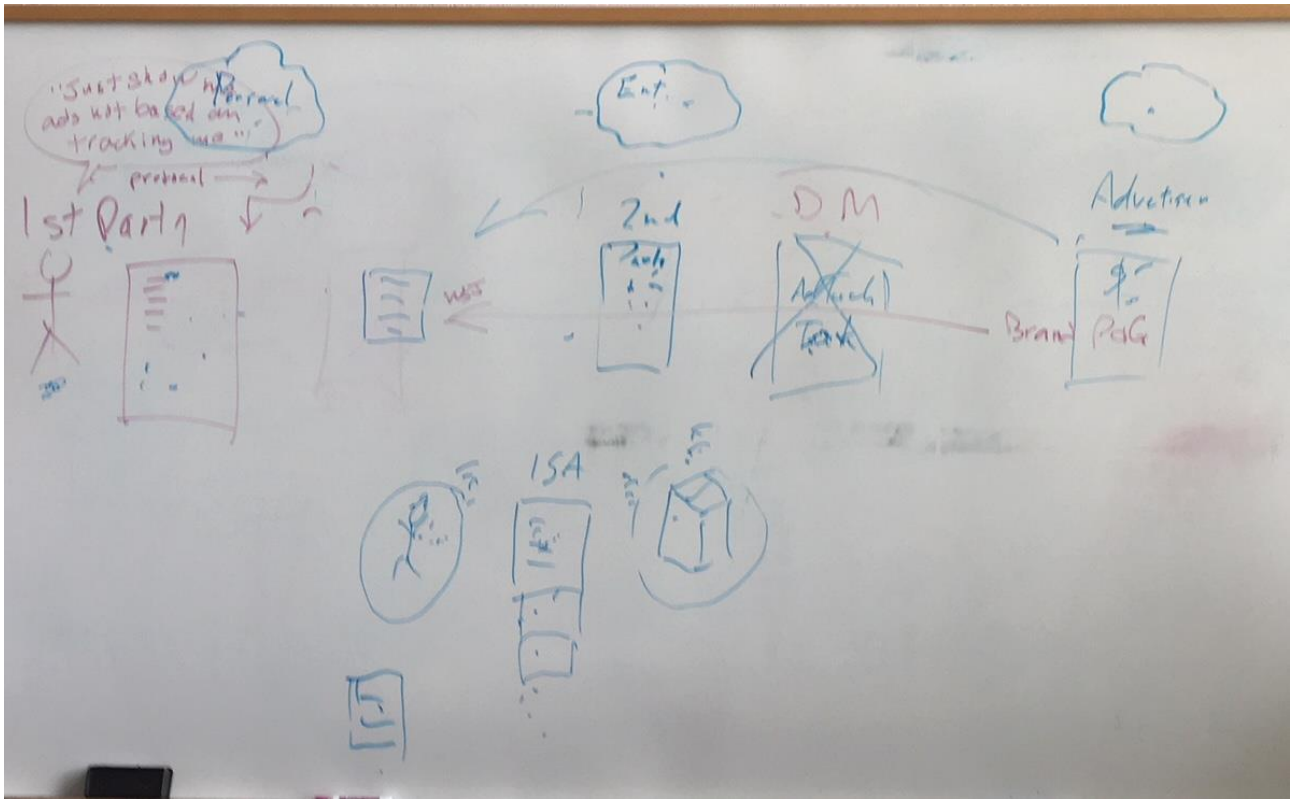
Tuesday 3G
Convener: Doc & Jim Fournier
Notes-taker(s): Jim Fournier

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

Doc asserted the customer should be able to set their own terms, for example "no stalking" under GDPR, ideally in a browser.

Jim introduced the concept of an Information Sharing Agreement (ISA), a human, machine, and lawyer, readable agreement written in JSON-LD that can be automated using JLINC to achieve GDPR personal data control compliance and ultimately intent-casting for VRM.

Discussion ensued, among lawyers and others including input from Mary who has already been working on similar efforts from the legal side at Kantara.



Big, Big Picture Identity Money Topology - A Conversation

Tuesday 3I
Convener: Trey Tomeny
Notes-taker(s): Trey Tomeny

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

In this session, we discussed a big idea proposed that might solve the problems of identity, money and privacy.

It involves simultaneous bottom up and top down approaches. From the bottom up, all people with access to a device and at least an intermittent connection can participate in the world's economy by creating "Minute Money".

Minute Money is using time directly as money. Money has always represented stored work and the work that consistently has positive externalities is education. A Minute of Money, "Meny" is earned when a user has verifiably focused full attention on a learning activity. This Meny currency can be earned by all, but only those, the young and the poor, whose alternative uses of time are compensated at low rates, will have the incentive to devote time to creating the currency.

This currency should be inherently stable on the long term, as the portion of one's lifetime devoted to creating it should stabilize as large numbers are involved in the system. To prevent generational inflation, the widely dispersed currency created by each individual is withdrawn from the system upon the individual's death.

To create Meny, users log in with an Internet Guardian site and select an app to work in. The app may involve a wide variety of learning tasks, and each app must be approved by the League of Internet Guardians. The League is a competitively cooperative organization. Each Internet Guardian is a self selected individual leading perhaps an enterprise of which he or she is ultimately responsible.

The League represents the top down component of this plan, but it is comprised of Internet Guardians who have risen from the bottom up. The Internet Guardians are all competing, constantly, to be the most trusted entity in the world. Internet Guardians have the incentive to become the largest and potentially most well compensated organizations in the world, as not only does money creation happen there, but they have numerous revenue opportunities as their user base expands.

To join a particular League of Guardians, individual Guardians must be allowed into the League by existing Guardians. The whole process may start with the simultaneous start up of two or three Guardian enterprises, by individuals of sufficient stature to have already earned trust in the communities they wish to serve.

The creation of Minute Money will start with an individual Guardian finding sponsors who are willing to pay people, in an existing currency, to learn specific material. Two possible use cases are churches, desiring people to read sacred texts, and companies with worker shortages, desiring a low cost way to train and perhaps to keep workers in compliance regimes. These sponsored payments set a floor price for Meny, but soon Meny, when understood as a currency, will float alongside other world currencies, and have an intrinsic market based value.

The fundamental principle of value behind Meny is that work was verifiably done to create it, and that it is maintained by real people leading enterprises that they are personally responsible for, and that the whole system operates in parallel to any and all existing currencies and government imposed systems.

Freedom from "men with guns" aka government intervention is achieved by not requiring the use of any government resource, and running the League and Internet Guardians with no physical assets. Internet Guardians and the League will be operated as individuals each use devices to communicate and authorize transactions in the cloud, with not fixed physical presence anywhere. Those with the most transparent operations will likely evolve to be the most trusted, and therefore the most remunerative for their operators. Users will enjoy the benefit of constant and consistent online identity provision by the Guardian they select. A trust breach by a Guardian will likely be the end of that Guardian.

When the entire system is up and running, being excluded from joining any League will be the ultimate penalty for any individual. Being a client of a League member, mutually selected by the individual and a Guardian, becomes essentially citizenship in the new online world. If your past behavior makes you ineligible to be associated with any Guardian, in any League, life will be very primitive and difficult, as it essentially "kills", for at least a time, your online life, until you can re-establish yourself as trustworthy, and likely specialty Guardians will arise to help in those circumstances.

This session, which was a multi-hour conversation, will be followed up with today by more specific conversations about Minute Money, Internet Guardians, and the implications of being fundamentally identifiable, biometrically, in all public places.

OIDF RISC Working Sessions (T - TH)

Tuesday 4A, Wednesday 4A & 5J, Thursday 3A
Convener: Annabelle Backman and Marius S
Notes-taker(s): Annabelle Backman

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

The following notes are for all four OIDF RISC working group sessions across all three days of IIW #25:

SET Subject

Ways to Identify a Subject

Base URI for subject type: http://schemas.openid.net/secevent/risc/**subject-type/**

- iss and sub only

```
{
 "risc_subject": {
   "type": "http://schemas.openid.net/secevent/risc/subject-type/iss-sub",
   "iss": "https://idp.example.com/",
   "sub": "123abc",
 }
 ...
}
```

- email only

```
{
 "risc_subject": {
   "type": "http://schemas.openid.net/secevent/risc/subject-type/email",
   "email": "foo@example.com",
 }
 ...
}
```

- phone number only

```
{
 "risc_subject": {
   "type": "http://schemas.openid.net/secevent/risc/subject-type/phone_number",
   "phone_number": "+99-123-456-7890",
 }
 ...
}
```

- email hash only

```
{
 "risc_subject": {
   "type": "http://schemas.openid.net/secevent/risc/subject-type/email_hash",
   "email_hash": "xyz",
   "hash_alg": "CRC",
 }
```

```
  ...
}
```

- phone number hash only

```
{
 "risc_subject": {
   "type": "http://schemas.openid.net/secevent/risc/subject-type/phone_number_hash",
   "phone_number_hash": "xyz",
   "hash_alg": "CRC",
 }
 ...
}
```

- iss + sub and email and phone number merged

```
{
 "risc_subject": {
   "type": "http://schemas.openid.net/secevent/risc/subject-type/id-token",
   "iss": "https://idp.example.com/",
   "sub": "123abc",
   "email": "foo@example.com",
   "phone_number": "+99-123-456-7890",
 }
 ...
}
```

- iss + sub and email and phone number as array

```
{
 "risc_subject": [
   {
     "type": "http://schemas.openid.net/secevent/risc/subject-type/iss-sub",
     "iss": "https://idp.example.com/",
     "sub": "123abc",
   },
   {
     "type": "http://schemas.openid.net/secevent/risc/subject-type/email",
     "email": "foo@example.com",
   },
   {
     "type": "http://schemas.openid.net/secevent/risc/subject-type/phone_number",
     "phone_number": "+99-123-456-7890",
   },
 ]
 ...
}
```

- iss + sub and email and phone number as map elements

```
{
 "risc_subject": {
      "http://schemas.openid.net/secevent/risc/subject-type/iss-sub": {
           "iss": "https://idp.example.com/",
             "sub": "123abc",
```

```
        },
        "http://schemas.openid.net/secevent/risc/subject-type/email":
{
             "email": "foo@example.com",
        },
        "http://schemas.openid.net/secevent/risc/subject-
type/phone_number": {
             "phone_number": "+99-123-456-7890",
        },
  }
  ...
}
```

- risc_subject and optional risc_subject_alt

```
{
 "risc_subject": {
   "type": "http://schemas.openid.net/secevent/risc/subject-
type/iss-sub",
   "iss": "https://idp.example.com/",
   "sub": "123abc",
 },
 "risc_subject_alt": [
   {
     "type": "http://schemas.openid.net/secevent/risc/subject-
type/email",
     "email": "foo@example.com",
   },
   {
     "type": "http://schemas.openid.net/secevent/risc/subject-
type/phone",
     "phone": "+99-123-456-7890",
   },
   ...
 ],
 ...
}
```

We will use risc_subject (single object) and risc_subject_alt (optional array) to represent subjects in SETs.

Nested Subject

```
{
 "iss": "https://idp.example.com",
 "risc_subject": {
   "type": "http://schemas.openid.net/secevent/risc/subject-type/id-token",
   "iss": "https://tr.example.com/",
   "sub": "7375626A656374",
   "phone_number": "+99-123-456-7890",
 }
 ...
}
```

Top Level

Allowed if no iss conflict.

Implied subject type:
"type": "http://schemas.openid.net/secevent/risc/subject-type/id-token"

```
{
 "iss": "https://idp.example.com",
 "sub": "7375626A656374",
 "email": "foo@example.com",
 ...
}
```

Single vs. Multiple Events

- RISC only needs one event per SET. Unknown attributes within an event body MUST be ignored.
- Three use cases for multiple events presented and discarded:
    - **Extensions:** Event extensions will define new attributes directly within the event body. Anyone implementing a proprietary extension will be responsible for avoiding collisions for themselves.
    - **Aliases**: For migration purposes, a transmitter can send the same event twice, under both the old and new name.
    - **Related Events**: The SET transaction ID can be used to relate multiple events together, even if they are in different SETs. This behavior is necessary even if multiple events per SET are supported, as there is no guarantee that related events will be transmitted together.
    - Instead of a single risc_subject array, RISC will use two claims in the SET, risc_subject and risc_subject_alt:

Required Subject Types

- Stream config API will have a subject_types array, identifying which subject types are to be used within SETs transmitted on the stream.
    - Meaning is unclear. Does [iss+sub, email] mean all events have both? Would [iss+sub] mean that Amazon always gets iss+sub even though we enroll using email?
- Implementers MAY allow receivers to edit the subject_types array to remove subject types that they do not want to receive in SETs.
- In order to indicate to callers whether all requested changes were supported and accepted, stream config update responses will indicate one of the following:
    - The entire change was accepted.
    - The entire change was rejected.
    - Some of the change was accepted, but one or more requested changes were rejected due to not being supported by the implementation.

NIST – Digital Identity Guidelines (101 Session)

Tuesday 4B
Convener: Sarah Squire
Notes-taker(s): Colin Jaccino

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

Levels of Assurance
Restrictions on use of SMS for 2FA
Password Policies Vectors of Trust
Password and MFA Guidance

Want to divorce identity from security and authentication

What is authentication

- a way we determine that a person is the same as the last time we saw them (not who they say they are)

Types of threats:

- unintentional account compromise
- snooping by known relation
- bots - don't have access to your device, but may be able to brute force or reverse hashes
- nefarious third parties by stealing identity
- state actors - well-resourced nefarious parties
- hacktivists - often with political motives

Levels of assurance

- 1 -
- 2
- 3 -

- 4 - Very high confidence
  - Strong cryptographic authentication
  - strong man-in-the-middle resistance
  - no bearer tokens
  - account owner has physically appeared and a government-issued photo-identifaction document has been verified

NIST Digital Identity Guidelines - Act III

- Changed guidelines from 1 dimensional to three
- Identity Assurance (1,2,3)
  - L1 - Pseudonymous
  - L2 - Remote or in-person identity proffing
  - L3 - In-person identity proofing with biometric collection for the purpose of non-repudiation
- Authenticator (1,2,3)

    - L1 - Single-factor authentication
    - L2 - Two-factor authentication
    - L3 - Two-factor auth with cryptographic device and verifier impersonation resistance
- Federation (1,2,3)
    - L1 - Signed bearer assertion
    - L2 - Signed and encrypted bearer assertion
    - L3 - Signed and encrypted holder-of-key assertion
        - A method of federation in which the client trusts the identity provider AND trusts (validated) that the person using the client is the correct person (the holder of key)

Secretary of State would be
ID assurance level 3
Auth assurance level 3
Federation assurance level 2

MFA Guidance
Knowledge-based authentication (KBA) is banned

- bad security
- bad usability

One-time password over SMS is restricted

- Public switched telephone network has extensive vulnerabilities
- SMS can be sniffed
- Easy to socially engineer phone number porting/device replacement

Password Policy Guidance
DON'T

- Special character requirements (allow them, not require them)
- Forced rotation

DO

- Allow ridiculously long passwords
- Accept spaces and special characters
- Compare to breach corpus
    - haveibeenpwned.com?

NIST 800-63-3???

Usability is key to security.

Look Up: UAF, U2F. Fido

IDPro.org
Identity bootcamp - 1 day conference before Gartner's identity conference

https://www.rsaconference.com/videos/measuring-authentication-nist-800-63-and-vectors-of-trust

Additional Notes from Anik

Election in Iran happened after 5 months election of Obama, the contestant who was mainly hated, esp in youth, won. The govt. blocked websites that gave out the information against the candidate.

We want to know its the same person,
Idea is to divorce identity

What is authentication? Why do we measure it?

We make standards in size.. it will be difficult if everyone is measuring in their own scales.
It means making sure that a person or thing is the same person that we last saw. (IMP: Which is diff from them being who they say they are). Whistleblowers can securely authenticate without revealing their identity.

Types of vulnerability

1. Accidental loss
2. Snooping (access to device)
3. Bouts
4. Financial fraudsters (wire money, fraud open credit)
5. State actors (people with a lot of resources)
6. Hackers (usually political motives)

Levels of Assurance.
LoA-1 to 4
LoA4 : Strong cryptographic authentication
String main middle resistance
No bearer tokens
Account owner has physically appeared with a govt identity

NIST digital identity guidelines Act III. 800-63-3
Instead of huge paper trail application this provides for online

3 dimensional assurance levels

Identity AL1	Authenticator AOL 1.	Federation AL1
Pseudonymous	1-factor	signed bearer
Identity AL2:	Auth AOL 2	Fed AL2
remote or unperson proofing	2 factor	signed and encrypting
Identity AL3	Auth AOL 3	Fed AL3
		Signed and encrypted and holder-of key assertion

Password MFA guidance

Knowledge Based Authentication is banned
- Bad security, usability

OTP over SMS is restricted
- Public switched telephone n/w has vulnerabilities

- SMS can be sniffed
- Easy to socially engineer

Password policy guidelines

No special character requirements
No forced rotation
Allow ridiculously long passwords
Accept spaces & special characters (don't require them)
Compare to breach corpus. (Already compromised passwords, also most common passwords)

Q: We know what we said what not to do (don't use OTP SMS), what should we do?
A: The list of guidelines are coming in soon.

Fixing Social Security Numbers

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

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

The slide deck that was presented during this session has been copied and pasted below.

The SSN problem

When your SSN is stolen, what do you do?

Problem: Replacement costs money

- Users should not bear the cost
  - Suggest that when your SSN is tolen, the company that let it get out bear thte cost of replacement
  - Replacement should cost LESS than identity protection
    - Win/Win for everyone
  - Replacement should be MORE secure than the SSN was

Problem: Whatever we replace it with needs to be *incremental*

- Too much stuff uses your SSN as either a unique indicator of identity or a authenticator
- Whatever we replace it with needs to continue to work with "non-stolen SSNs"

Problem: How to Establish identity in a strong way after it is fixed

- Usually Public / Private key
- Quantum Encryption problem

How to re-establish identity in a non-repudiable way if identity lost/stolen

- If biometric based
  - Problems of storage
  - Problems of spoofing
- Who has authority to change it?
- How can proof of change (and authority to change it) be maintained
  - Quantum Computing problems

Potential solution

- When your SSN is stolen, the company pays for you to
  1) Get strongly identified (perhaps as done for Passport at the post office?)
  2) Issued a digital private key
  3) Get the hash of the public key stored on a blockchain along with your SSN
     - User's name is NOT listed on the blockchain.
     - Hash is used to prevent mass quantum attacks
  4) Law passed that requires verification of ownership of the SSN if the SSN is on the blockchain, using the public key.
  5) SSN can still be used as an identifier / pointer / userid in older software

How does a user prove ownership of private key?

- Token without a password (?), but with a button for use
  - Needs to be EASY for a user to use
    - Note that SSNs are NOT commonly used today
      - Getting a new credit card
      - Getting a new bank account
      - Allowing access to financial information (new phone account…)
  - MUCH more secure than current solutions
    - *We don't have to be perfect, just better*
    - Private keys are not put together in large databases – hackers can only get them one at a time.

How to recover identity when lost/stolen/broken token

- Same way we do with passports?
- Government controlled database (hash stored on blockchain?)
- New research needed?

Quantum Insecurity

- Keep a "Quantum Emergency" hash of a public key on the blockchain, used to endorse a new quantum secure key, once it comes out.
- As long as the public key is never used, except for that purpose, this provides a "race condition" that can be used to endorse a new quantum key.
- Signature over quantum key is first provided and extended onto blockchain. Upon being added to the blockchain, the public key is sent.

Functional Identity

Tuesday 4F
Convener: Joe Andrieu
Notes-taker(s): Joe Andrieu

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

The base document is at http://bit.ly/functionalidentityprimer

What emerged today:

1. Add discussion of subjective notion of identity (humans and ICTs)

2. Add Context, which includes source

3. Remove derived attributes. All attributes are derived.

Public Blockchains and Private UMA

Tuesday 4G
Convener: Adrian Gropper
Notes-taker(s): Scott Mace

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

Adrian draws a stack:

- User at top
- Mobile device
- Agent
- DID (decentralized distributed ID)

One model for how to create an agent is something called UMA, User Managed Access, been worked on for about 8 years.

What this agent does is when somebody like a doctor (Bob) wants to have access to something about patient Alice, the lab creates a resource, has an API. Alice might be completely anonymous or pseudonymous. Healthcare allows for that. Bob is the requesting party. The directory may or may not exist. Bob gets the idea there's something about Alice that the lab has. The HIE is the agent. The lab could be anything that has personal information about you. As a servicer to you Alice, I'm going to register this result. Bob figures out sometime later that Alice has a test result and goes there. The resource says yeah I have a test result but I can't give it to you. You have to go to Alice's agent. First,

Bob brings a context. This is what we're calling the self-sovereign stack. Bob is bringing a context and bringing credentials. He will bring his medical license. And the agent will be autonomous. I will claim the most interesting aspect of the agent is in terms of AI and machine learning without it being owned by anybody. When the agent looks at the context and the credentials, the agent returns an access token to Bob. Taken by Bob's client to the lab. The lab gives the resource to Bob's client. Based on a theory called the object capabilities model. Can't use access control lists to just give Bob the answer. Why the mobile? This is where the biometrics live or things that behave like the biometrics. What makes it convenient and practical for Alice as a person to control their agent and the DID. UMA lives in this layer (agent) where everything is private. Maybe running in a closet in my house. Agent is not online all the time. It can be lost. You might want to have multiple agents. It's a practical issue, not a philosophical one.

Q: Will there be companies running agents in people's closets?

A: We hope so. Two issues. How do we get the world to play by these rules? Not in the nature of manufacturers, service providers, even doctors to give users control. How about the design of the stack? How do we give the labs or manufacturers, drug companies, primary service providers (not data brokers) potential? Second problem, how do we make it cost effective for everybody to be able to run their agent in a self-sovereign way without having to compromise by having a data broker seeing or monetizing my data. There are two camps. Slowly the world is shifting. Two years ago, there was no blockchain and all federation. In healthcare, federation does not work and has never worked. Healthcare is provided by everything from a VA hospital to a nursing home or a doctor that's semi-legal in a poor neighborhood. You cannot have effective federations around identity in healthcare. So what's been happening at IIW, people are paying more attention to self-sovereign identity. It doesnt mean you can't use federation, but it means you don't need to use federation. Alice can decide to whitelist federated IDPs. If Bob says I don't have any ID but I have my Gmail address. HIE of One says oh that's fine. There are certain things I will trust Google as an identity provider to do. Sutter Health is an identity provider.

Alan H. Karp: Patients love this. My choice was doctors see my medical records or not. With a token I give the guy doing my X-ray a subset of my record.

Adrian: With standard HIEs you have either an opt-in or opt-out agreement. None of them are wildly successful. You're basically opting in to a certain set of policies. Imagine an HIE opt-in agreement.

Alan: Think of them as your Google privacy settings.

Adrian: In the case of psych info, whether Alice has control over that info is a debatable point. Is identity what I assert, or what others say about me?

Q: As people get older they designate a health agent. They can be guardians.

Adrian: Yes I've oversimplified by not dealing with guardianship. Delegation with attenuation.

Alan: If Bob gets a credential from Alice to see the lab report, can he give a subscope token for someone else, like a nurse.

Q: Never made it to RFC. There's token chaining. The more UMA approach is for Bob to redelegate rights for someone else to get a token.

Adrian: In this stack, and the protocols associated with it, the lowest level is by definition public. No

one is proposing private DID systems yet. Would be a corner case. DID documents may be IPFS or in the blockchain directly. Everything above it needs to be private. One of the reasons that drives this whole philosophy is the increasing importance of machine learning and AI. The only place that has access to your policies. I don't have to declare if I'm a Democrat or a Republican to anyone. How do we create a gig economy for physicians. Credentialing. Prescriptions. Secure transactions. Reputation. Some matching function. In general, the first two of those are handled by the standards we have today. The reputation piece is very squishy. Matchmaking is just out of scope.

OpenID Connect CIBA explained

Tuesday 4H
Convener: Bradley & Hjelm
Notes-taker(s): Bjorn Hjelm

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

Session Summary

- Presented an overview of the OpenID Connect Client Initiated Backchannel Authentication specification.
- Discussed the use cases that the specification addresses and steps.
- Discussed some of the technical design assumptions and trade-offs.

Slides available on SlideShare: https://www.slideshare.net/secret/6cbyLHVEZCAApq

Identity Concepts Around the World

Tuesday 4I
Convener: Pelle Braendgaard
Notes-taker(s): Tom Brown

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

Most everything we talk about is U.S. or E.U.
Didn't see the applicability of digital identity in developing nations
We have mobile phones, ATM cards

Agent banking
Every 15 days is payday in Nicaragua, Central America

Empeso - usd to pay for bus in Nicaragua although many people find it annoying and prefer cash
China - no gov identity system but corporations provide de-facto identity
People like to display status, so it would help if you could make identity card fashionable in that way
People in Kenya wanted affordable makeup, without the duty markup, with aspirations of becoming more modern
Trust in the sense of reliability: my brakes work or else the stock price of the car company goes down

Tribal trust systems...
Somali Hawala system - strong identity model for payment. you belong to family that belongs to clan
Can send cheap instantaneous money to anywhere there are Somalis
Their KYC is not something you can document. It's about reliability and knowledge
FATF - Financial Action Task Force
What is the least common denominator of interoperability of these systems around the world?
Hernando de Soto - Mystery of Capital
doingbusiness.org (world bank)
The reason transactions need identity is because FATF
Unless we're talking about credit, KYC's value is questionable
DIF - decentralized identity foundation (Sovrin, Uport, Microsoft, etc)
DID - kind of like a url for an individual
Transferrable statements can take trust statements from your local region to another region

Introduction to DID's, Verifiable Claims and Blockchains (101 Session)

Tuesday 5B
Convener: Drummond Reed
Notes-taker(s): Colin Jaccino

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

A brief overview of Decentralized Identifiers, Verifiable Claims, and the Sovrin Public Permissioned Ledger

The work was initially driven by Web Payments work at the w3c, also in the verifiable claims subgroup.

Verifiable claims are essentially your ID card, credit card, etc.
If someone controls your claim, then it's not yours. It's not necessarily portable.

DID is decentralized identifier.
Self-sovereign identifier is another term to refer to the same, but with an emphasis on owner control.

DID can be used with any form of decentralized network, not just blockchains.

How do you do privacy-respecting identity on a publicly readable blockchain.

Sovrin Identity proposed publishing only public information. The private information handled by agents off the blockchain.

Self-soverign identity is…

Lifetime portable digital identify for any person, organization, or thing that does not depend on any centralized authority and can never be taken away.

"Show me a globally resolvable identity that you have that cannot be taken away from you?"

This is only possible with…
Decentralized Identifiers (DIDs): a new type of globally resolvable, cryptographically-verifiable identifier registered directly on a distributed ledger.

Breakthrough: we use standard URN syntax for the DID syntax
URN syntax (RFC 8141)
urn:uuid:ae84-d5c2-9fb785ea-72ccd34
Scheme, Namespace, Namespace-specific Identifier

DID syntax:
did:sov:3k99dg356wdcj5gf2k9bw8kfg7a
Scheme, Method, Method-specific identifier
Method-specific identifier: generated as defined by the particular DID method specification

Initial DID Method Specs

Sovrin did:sov:
Bitcoin Reference did:btcr
Ethereum uPort did:uport:
Veres One did:v1:
IPFS did:ipid:
IPDB did:ipdb:

{ "Key": "Value" }

{ "DID": "DID Doc" }
Decentralized Identifier
DID Document (JSON-LD == JSON Link Data)
JSON Link Data provides a means to reference an RDF Ontology, enabling validation and interpretation of the document.

The six primary elements of a DID doc.
1. DID (i.e., the JSON-LD is self-describing)

2. List of public keys (for the owner)

    - This is the answer to public key infrastructure and the problems of adoption. Now you can locate the public key of an identified party.

3. List of service endpoints (for interaction)
    - service endpoints will probably evolve into a standard set of endpoints
4. Access control branch (for key mgmt)
    - Information required to ensure that only an authorized party can make updates to the DID doc
5. Timestamps (for audit history)
6. Signature (for integrity)

Decentralized Identity Stack"

- Identity Owners
- Identity owners need not be humans.
- Edge Layer
- Edge Agent
- Service pointers may point to these
- Edge Wallet
- Cloud Layer
- Cloud Agent
- Service pointers may point to these
- Encrypted P2P verifiable claims exchange
- Cloud Wallet
- DID Layer
- If the economics of the DID Layer are set up correctly, one could have a different DID for every relationship. By having a different DID per relationship, it may be possible to avoid correlating relationships, undesired association.
- DIDs can be mapped into legacy systems.

Nothing about the parties described in the decentralized identity stack that *requires self-sovereign identity*. But the idea is this kind of architecture would support this model for identity.

HOLOCHAIN P2P Apps Without the Blockchain's Problems for Scale, Speed, Cost & Governance

Tuesday 5F
Convener: Matt S.
Notes-taker(s): Heather Vescent

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

Holochain is an alternate to blockchains.

How we do distributed data integrity - holochain.
releasing alpha on friday
It's open source

Why
1. users in control
2. no dependence on 3rd party
3. works the way users expect
4. maximize adaptive capacity

Humans need new ways to organize themselves. We need more adaptive models.

How
Each application has its own holochain.
Take the best parts of blockchain and bit torrent.

Shared validation rules - agreeing on the rules
Hash chains (one for each user)
Distributed hash table (for each application)

A separate chain for each user. you have your own log of your own activity on my device. each application has its own holochain, which means you have your own chain for each application for each user.

Every holochain has 3 parts
1. application code
2. local hash chain (an append-only tamper resistance log o the users own actions)
3. shared storage (a distributed hash table for only the content in the app)

q: does the hash table have history? do I get to add data and pass it along?
a: you would be able to sign it, but not able to alter the stuff I have signed.

In a distributed system, there is no absolute ordering of events. One person could receive things in a different order from someone else?

Example: peer to peer message
1. Installation (on your divide in your local source chain:

1: add application code as first entry: application code lets other know you are using the same app.

Q: versioning?
A: there is no versioning: we are running identical code.

Q: so you have your own runtime execution?
A: yes.

2. Generate keys and add as 2nd entry: keys enable others to
a. route content (hash is an address)
b. send encrypted messages
c. verified signature

Sending a message
1. write message
2. validate new data (sanity check
3. store data in new chain
4. signs in chain
5. store DHT

Expect users to also be hosts

....

Q: Can we have backups of source chains?
A: yes

I'm finding the best path, by queuing the nodes around me, until I find the best path, and then I send the message.

this is a routing protocol, with a stable network in it. time transient.

Benefits
Consensus on rules not data
Fast (Blockchains go slow and are expensive)
Cheap
Scales well

User centric
Application bridging
Identity bridging
Adaptable

analogy: humans speaking english, each have a knowledge of english (although they are not running the exact same source code so there might be misunderstood).

Holographic storage, to adapt to the new things to propagate through the system.
This leads to adaptive capacity.

Micro apps and meta applications - create custom UI that works for you.

Version control: ? how do you get people to migrate apps all at once
should be able to bridge platforms

Clutter: peer to peer twitter

Current model is the app developer is a dictator model

DPKI - building another application that is a distributed public key infrastructure. Interested in talking to people to set up identity servers. social key revocation.

Ambition: we think the world works better when individuals get to pick the way their apps work. We want to get people used to this user centric way. This is different from network centric blockchain.

Larger context: CEPTR: out of the meta-currency: interoperable communication systems that mimic biology communication, building social coherence and social risk. Ceptr.

Pcubed - protocol for pluggable protocols.

YubiKey Usability Study

Tuesday 5H
Convener: Kent Seamons
Notes-taker(s): Kent Seamons

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

In this session, Kent Seamons presented results from two recent user studies of YubiKey - a laboratory study and a longitudinal study.

Study 1 focused on the setup phase. Participants set up a YubiKey on Google, Facebook, and Windows 10. The majority of users were able to set up Google easily using a Wizard. Less than half succeed with Facebook and Windows 10. Overall, the usability of the setup phase was low.

Study 2 focused on daily use, and participants were given a YubiKey for one month to use to login to Google, Facebook, and Windows 10. In general, users liked their experience and gave it high usability scores. Some users indicated they preferred the YubiKey to SMS two-factor authentication (2FA). Some users disliked the small form factor of the Nano.

We finished by talking about future user study plans that broaden the scope to include all types of 2FA (SMS, TOTP, push notifications, hardware tokens, and OTP). Suggestions were made to incorporate mobile-phone only applications and command line 2FA.

Contact Kent Seamons at seamons@cs.byu.edu for more information about the studies. A research paper is forthcoming.

IDPro: The Organization for Identity Professionals

Tuesday 5I
Convener: Sarah K Squire, Steve "Hutch" Hutchinson
Notes-taker(s): Steve "Hutch" Hutchinson

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

Where is Identity in our organizations?

- Is it merged with security? Is it part of the larger IT organization? Do you end up sending identity experts to the four corners of the organization and infuse it without knowhow? My guess is a bit of all of these. There's no one "standard" place for identity to be located on organizational charts
- With the rise of the value of identity within in business systems, identity professionals are in high demand. But we still struggle to grow in terms of prominence when it comes to executive mindshare. Or prominence with policy makers. Or even when trying to grow communities like this one.
- We do hear a lot about security and privacy. They are the peanut butter & jelly in today's world but they have their limitations. GDPR is a good example of this.
    - For certain, there are obvious security requirements in GDPR: encryption in motion, encryption at rest, have a security program. Those are definitely security requirements
    - There are also easily understood privacy requirements: privacy by design, privacy by default, know who your Data Protection Officer is. It's great and important stuff.
    - But there's also requirements in GDPR like "Do Not Process," "Right to Rectification," and all of the "Consent" stuff. The default tools available to Security and Privacy cannot do these. Because these are identity requirements. Only the tools in the stable of identity professionals have these capabilities. This is our workshop.

- In order to provide a stable base for all of our enterprises to rest upon, not only do we need security & privacy but we need to add identity to that as well
    - Identity is the human interface for security. Without identity, you have a lot of boring logs without context, and that diminishes their value
    - Identity is the operational arm of privacy. How else do we grant access to data? How do we monitor it? That's us.
    - Security and Privacy give us the requirements and we make it real. We are the fabric by which their needs are instantiated in the enterprise

- Security and Privacy give us the requirements and we make it real. We are the fabric by which their needs are instantiated in the enterprise

Identity industry lacked a professional organization

- We're not always the "go to" source in the enterprise to get these answers. Our voice isn't always heard when some of these decisions are being made about how to tackle large-scale problems like GDPR
- We face these challenges, in large part, because, unlike our peers in Security & Privacy, we have not had an advocate to be the entire industry's voice. We didn't have an advocate for the profession and the practice and the discipline of identity management
- In that sense the Identity industry was a collection of professionals without a profession

How did you learn identity management?

- It's a difficult practice to learn because there's no established curriculum so most of us gained our knowledge by first learning a particular vendor product and then backing into the art
- Let's ask the question a little differently … how long did it take you to learn? How long does it take to train someone in your enterprise? You get a bright, smart kid right out of school and you put them into identity. And you do what? What is the curriculum? A couple of blog posts? Some Twitter handles?
- You've really got to *want* to build new identity professionals because the resources required are enormous

How do we grow this industry?

- All of these things restrict the growth of this industry. How do we change that?
- How do we grow the industry in terms of prominence among executive mindshare?
- How do we grow the industry in terms of prominence among policy makers?
- Last year, Ian Glazer had these same questions kicking around in the back of his head and in the spring of 2016, he sat down to discuss this situation with Allan Foster and Robin Wilton from the Kantara Initiative who, as it turns out, were also noodling on the problem
- Kantara agreed to host a discussion group which was launched in May 2016 at the EIC in Munich and at the CIS the following month in New Orleans. Within the first three months, we had over 400 professionals sign the pledge. Over 100 of those signed up to begin the actual work on a code of practice and body of knowledge
- All of this led to June 17th of this year when we announced the formation of IDPro, a fully incorporated 501c6 non-profit organization of, by, and for identity professionals

What is IDPro?

- Three things we're focused on from a program level:
    - Membership
    - Code of Practice
- Body of Knowledge

- The development of the above three are in support of the eventual development of a certification

Membership

- Individual Memberships
    - We currently have over 150 fully-paid individual members
    - Individuals can join from https://idpro.org/join/
- Corporate Members
    - We also have ~ 15 fully-paid corporate sponsors
        - Including Oracle, Radiant Logic, Ping Identity, SailPoint, GIGYA, ADP
    - We have another dozen corporations pending legal/paperwork
- Organizational Partners
    - FIDO Alliance, Women In Identity
        - Event Partners
    - First one is Identiverse

Code of Practice

- If we're going to be a profession and formalize this, we need to have a code of practice. And we've been hard at work creating one that incorporates ideas around professionalism, personal integrity, and onward continuous skills development

Body of Knowledge

- But I also asked you earlier "how did you learn this?" One of the trickiest parts is finding a curriculum to give a new identity professional … or for yourself because you just inherited Customer Identity Management, and you don't really know what it is.
- So we've been working on developing a taxonomy for identity management. Because if you take two identity professionals and put them in a room together and ask them to define one term, they'll come back with four definitions. We've got to make it easier to pass through this forest of knowledge and learn … not just debate the definitions

Certifications

- Building that body of knowledge is all in support of getting to certifications
- In talking to companies and professionals across the globe about certifications, the most important thing to any of them is that a certification has to be neutral. They cannot be specific to a product but instead address a discipline: "This is how you do access certification"

- Certifications have to be applicable, which means we need to keep them contemporary. We need to be addressing the practices that are important today that practitioners are responsible for and performing in their normal line of work.
- And finally, a certification needs to be meaningful. It has to have teeth. We don't want this to be a paper mill, we want it to represent that you really know your stuff.

Member Services

- A monthly newsletter that includes best practices of things to do in your world. Original editorial content targeted specifically towards our membership. There is already an established team under Andy Hindle creating and collecting content as well as establishing a publishing calendar
- A daily news clipping service. There's a lot going on in our industry and it's really, really hard to keep track of everything
- Digital forums that can bring practitioners together for discussion on current issues or even for those seeking help from other experts. This is one fo the most important things we can do. At identity conferences across the globe, some of the most popular sessions have been case studies. People talking about what they have done in their own enterprise.
- And meetups, like this one. How do we physically get together in one place? It's great to go to a conference and be surrounded by identity gurus from across the globe. But not everyone gets to go to those conferences. So how do we do something locally?

Wednesday October 18

Intro to Sovrin

Wednesday 1A
Convener: Phil Windley
Notes-taker(s): Phil Windley

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

Link to Intro to Sovrin slide deck:
https://drive.google.com/open?id=0B_luqCyRPBXjWVMtZmROVkd2UkJ6Yi1FcUlpUlB1N2l4Mjg0

Two Short Talks on Capabilities

Wednesday 1B
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:

http://habitatchronicles.com

Tags for the session - technology discussed/ideas considered:
#Capabilities #Distributed Capabilities #Access Control

Video Recording is here:
Part 1: https://youtu.be/yKFpCazwy6o
Part 2: https://youtu.be/XQWY9_BcSGI

Summary: Alan Karp "The anti-identity guy"

TALK 1: Access Control for IoT
Capabilities as tokens that prove authorization
Our current mechanisms don't support the modes of sharing that we rely upon in the physical form.

Six Aspects of Sharing
Dynamic, Attenuated, Chained, composable, cross domain, accountable

Capability Tokens avoid problems related to these that traditional Access Control Lists don't solve.

TALK 2: Unforgeable Distributed Capabilities
A capability is a:
Transferrable
Unforgeable
Permission
To use the thing it designates.

Permission is not sufficient for security analysis.
MAY vs CAN
Authority is about the set of things that can happen.

Distinction between
Knowledge Grants Permission and
Knowledge Grants Authority

A distributed authority is unforgeable is there an no KGP bits even if there are KGA bits.

Distributed ID System Patterns with Distributed Systems

Wednesday 1C
Convener: Dave Sanford
Notes-taker(s): Colin Jaccino

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

This conversation opened with a discussion of topics and technologies relating to distributed ledger-based identity systems. The conversation then moved to the continuum of freedom and control in human systems, and the similarity, or potential risk, human freedom has on the degree of control or independence inherent in digital knowledge systems on which we depend.

A number of questions emerged in the conversation:

1 – Will we eventually become so dependent on these systems that we cannot change them, even if there are problems with them?

2 – Will we enable strong non-repudiation in a way that has negative consequences for humanity? For example, in a punitive, self-destructive, or genocidal society, will these systems enable greater human harm?

3 – Have we assessed the potential negative outcomes of the introduction of strong, objective state and knowledge systems? Are we building safeguards into these new technologies?

Distributed ID:

-> Anonymous

-> Anon-Verified

-> Pseudonymous

-> Real Name

——> Sovereign ID

Distributed System

- Open, Permissioned, Private
- Fat Protocols
- Protocols that include a component that includes the payment for the use of the protocols
- Zero Knowledge
- - Consensus Algorithms
- Validate & Choose
- State == Truth

Continuum of autonomy for Human and Machine systems

<————————————————————————————————————>

Full Consensus Local Consensus Truly Decentralized Static

Human

Totalitarianism or Better Regional Autonomy ————————

Machine

Blockchain to rule them all ————— All nodes maintain state. no consensus

DIF – Universal Resolver + Universal Registrar (DID's across blockchains)

App Auth RFC8292 BCP212 Q&A

Wednesday 1D
Convener: Markus Sabadello
Notes-taker(s): Markus Sabadello

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

Several communities are making progress on specifying "methods" such as **btcr**, **sov**, etc. for Decentralized Identifiers (DIDs) in different blockchains, DLTs, and other decentralized storage systems.

The Decentralized Identity Foundation (DIF - http://identity.foundation/) is now working on a "Universal Resolver" that can resolve DIDs to their DID Documents in a unified way, by exposing an abstract interface that is implemented by a "driver" for each DID method.

The Universal Resolver can be deployed as a web service, and drivers can be implemented as docker containers. For some DID methods such as **btcr** and **sov**, a driver has to go through a number of steps to dynamically assemble the DID Document. In other cases such as **v1** and **ipid**, the DID method actually stores the DID Document that can be returned by the Universal Resolver directly.

Right now, preliminary drivers exist for **btcr**, **sov**, **ipid**, **uport**, **ipid**.

Corresponding to the Universal Resolver, there will also be a Universal Registrar that can cover registration (and updates, and revocation) of identifiers, using a similar architecture involving an abstract interface and a set of drivers. Depending on the method, this may require the user to take certain action (e.g. send funds to a Bitcoin address, or contact a Sovrin trust anchor).

- https://github.com/decentralized-identity/universal-resolver/
- https://github.com/WebOfTrustInfo/rebooting-the-web-of-trust-fall2017/tree/master/draft-documents/UniversalResolver

DNS BASED Open ID Connect Discovery

Wednesday 1H
Convener: Marcos Sanz (on video conference from Germany) & Mike Schwarz
Notes-taker(s): Mike Schwartz

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

Discussed draft created by Marcos Sanz, which can be found here:
https://www.ietf.org/id/draft-sanz-openid-dns-discovery-00.txt

PRO's:

1. DNS is already in use for discovery, while Webfinger is used only for OpenID Connect.
2. DNS is probably more secure then a web service

CON's

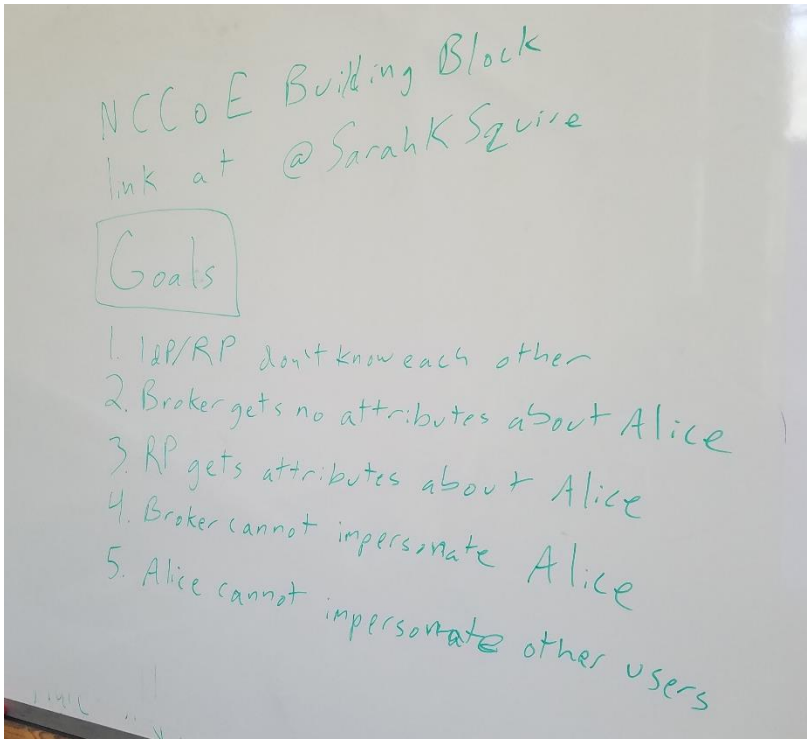
1. RP developers will have to support both methods, because some IDP's may support one or the other.
2. RP developers will need a DNS client library to resolve discovery, versus using a 100% web tools.
3. Webfinger can handle more complex discovery rules, especially where email is at the top level, but there may be a number of underlying OpenID Providers. For example, let's say there are OP's at us.corp.com, emea.corp.com, and china.corp.com. But... all email for users is at ___@corp.com for simplicity. DNS might struggle to implement the business logic for this scenario.
4. Oversimplifying a little... in some large enterprise environments, coordination with the "DNS department" adds some complexity to a rollout where OpenID Connect is primarily an operational concern of the "web department"

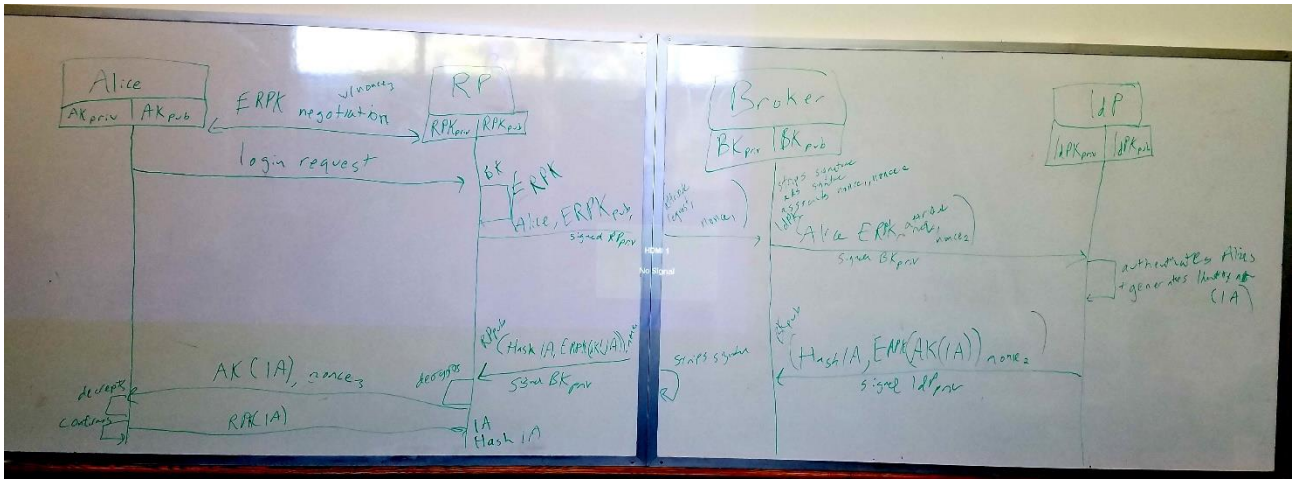
Although there was a fair amount of skepticism, there did seem to be a case for supporting this, as it would be sufficient in the vast number of cases, and management of a one-off discovery service is not ideal for organizations.

Triple-blind Brokered Identity Federation

Wednesday 2A
Convener: Sarah K Squire
Notes-taker(s): Sarah K Squire

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





First Party World: People in charge via GDPR by 25 May 2018 – Calling Lawyers & Geeks

Wednesday 2B
Convener: Doc Searls
Notes-taker(s): Scott Mace

Paul Baran's models of the Internet: Centralized, decentralized, distributed, independent.

But every different Internet node is an independent entity. David Reed works with Customer Commons. End to end in system design. Put all the intelligence at the ends of the network. All the middle does is route. It puts everybody in a position of independence.

Cicero talked about what's more strongly guarded than a man's own home. It's his castle.

Every one of those nodes is a castle. When we go to a Web site, we're not traveling anywhere. We're actually requesting a file. Netscape 1994 invented cookies to maintain state.

Contracts. I'm not a lawyer but I hang out at a law school. An agreement made by any two parties. That's a contract. There can be a third party but that's all law contemplates. The third party is inherently neutral. Always someone proffering the terms and someone agreeing to terms.

In the everyday world, we have a set of understandings, but in the internet world we've only had 22 years of that. For the Web, we chose an architecture called client/server. You always go to the server. World looks like this. Display Lumascape. This is the ad tech business. You the consumer are being followed by ad networks who plant cookies on you. He's done a good job of saying who's involved.

The GDPR comes along to protect consumers. You will owe up to 4% of your global revenue if we find you in violation of that.

The three entities they have: the data subject, data controller (could be any party in here, including Oath). The spirit of GDPR says you'll not only collect info about people but you owe it back to them if you collect it because it's there data. Starting in 2013, McKinsey and IBM started talking about the term big data. Now Microsoft, Oracle, SAP, Accenture, Deloitte. Now if you look up GDPR, who are the top advertisers. IBM, Deloitte. We have one small simple solution in getting compliance. A couple days ago, what happened. There are approaches to the GDPR that start with the individual. If you agree to my terms, you're in compliance with the GDPR. The third component is the processor.

Here's the auspicious thing that happened. Having Twitter conversation with the guy who invented Lumascape. He said you're being childish. Then he comes out with this two days ago. [Plays video]

In a world where ads target, one regulator took a stand to invoke privacy regulations. Notice consumers have changed to people. That's a big change. GDPR coming May 2018. An ecosystem has to adjust to a first party world. We won that argue. Will you be ready? Credits: Jason Kint, runs Digital Content Next, new name for Online Publishers Association. Now getting religion. He helped Terence Kawaja come up with this.

Q: Jason Kint is telling publishers Facebook and Google are not their friends. Margrethe Vestager. She's the one who says you're a trust, we're going to bust you.

Doc: This came out yesterday: The day after tomorrow, when adblockers and GDPR kill all adtech and

martech. Full of quotes from Doc. This is the book I wrote 5 years ago - The Intention Economy: When customers take charge. We're there now.

Q: Have you talked to Timothy Wu about this?

Doc: Yes and no. He wrote a great book about advertising. So Customer Commons is basically a complete knockoff of Creative Commons. Created at Berkman Center. The whole idea is the First Party terms that we can assert can live in a place that a browser or app can point to. The terms can be invoked and can be infinite. We will make them complicated. We can do intentcasting, where we can do the advertising. In a secure way, they're shared with what in marketing is called a qualified lead. An exchange and a negotiation can take place. Intentcasting and all those ceremonies, take the entire adtech and martech, annual conference with 5,000 entity Lumascape. Martech needs customer tech on your side. Let's make sure it's one kind of customer tech that talks to anybody, rather than the way CRM works now. We want it in the world by next May 25. It won't work across the board but it will be a proof of concept. Spoken to people at Conde Nast and Wired, the Guardian. I think we can make this happen.

Term: #NoStalking. The person is saying, just show me ads not based on tracking me. There is probably a more succinct way of putting it. On the other side is a publisher. Behind that is advertising or advertisers in general. Was part of a major advertiser until the early 1990s. The way advertising worked for the longest time, the advertiser had an agency. Through it they placed an ad. That ad sponsored the publisher. There was no mystery in it. You know the ad came from that company. That was called sponsorship. Ad tech said we're tracking eyeballs. Walt Mossberg starts Re:Code, is on stage with a big ad tech guy. You're going to advertise with us right? Ad tech guy says we'll find your readers and look for the cheapest place. Your eyeballs got followed to Breitbart. It's called into the world an endless variety of content. All we're doing is saying we're only interested in supporting you. Ad blocking is saying no to all of advertising. This brings sponsorship back. So what we need right now, there's human readable, lawyer readable [legalese] and the third is machine readable. We need a little help with lawyer readable. Students at Harvard are helping. How are these terms being proffered? Are you using the DNT field? W3C is mired in not coming up with a definition for DNT. Looking for a browser person to help. So looking for geek help and lawyer help.

Q: I can help with the DNT thing. Active standards work on user-granted exceptions to express exceptions. A fairly simplistic response the server can give back. The W3C standard should be published imminently. There is a UX to put in front of the consumer all the consents they need.

Doc: Concer. We're trying to turn this thing around.

Q: This is browser vendors developing this for display in browsers. It's browser-vendor centric. Intention is the three great browsers will commit to develop this if industry commits to accept it. Last time, Microsoft did this thing...this time could happen by May.

Q: DNT had no teeth. GDPR is a meat grinder. With DNT, if I went to a site that didn't respect that, there wasn't feedback. If we wait for standards it's going to be a while.

Q: Browser vendors are somewhat neutral territory, different world view. I work for Oath. Publishers like Jason Kint have their own problems. All this consent stuff lands on that. The publisher owns the media and offers it for sale. They're worried about the UX for their site or what the browser vendors will do in front of them to control access to their site. The IAB has a proposal, not circulated yet, daisy chain or daisy bit. What Doc is proposing. A set of permissions or bits which will go against all 880 participants in the IAB universe, consumers will consent to use of their data. I.e. stalking, analytics. 4-6 bits for each entity named in the Lumascape. What we're being asked to do in ad tech trade is to

choose a preferential one. One thing I would love to get out of this is where you all would like it to happen. Do we want browser centric, publisher centric?

Doc: I am an attorney for the individual. I've been paid twice by the IAB to tell them what to do. Especially re ad blocking. IAB says it's about the ad blocking companies rather than what people want to do.

Q: Digi.Me, what we do. Profile them on device, none of their data leaves their device but you can ask them how has your shopping at McDonald's changed in the last three months. Others are doing similar stuff. You need a summary of that. Get them to opt in. The beauty of it is if you go to the individuals, you will get orders of magnitude better information than from all the tracking.

Doc: The only thing until May 25 is show me ads not based on tracking me.

Q: No interest based advertising?

Doc: Let me talk about interest based advertising. Here's advertising. It went to a publisher and sponsored that publisher. That was all it did. There was another thing first called direct mail, then direct marketing. When the Web came along, it said DM is going to be advertising. It looks exactly like advertising. We've redefined advertising. It's only direct marketing. Madison Avenue fell asleep, direct marketing ate its brain and woke up as an alien replica of itself. I'm proposing, simple, narrow, are you so deep into this that you can't do this (no interest advertising).

Q [Wendell]: Yes. The 3x multiplier, out of Harvard Business School, IAB sponsored, if we can answer how to make more money using that method, we are all ears.

Doc: The concept I want to prove this is still possible.

Q: What Digi.Me and JLink are doing, putting the user in control doesn't address some of the issues. Doesn't address the free and informed consent in the GDPR.

Q: Stalking is because there is no ability to ask automatically an individual for their interests. That's advertising's dream. What's wrong with that?

Doc: The only thing wrong with it is it's not in my plan.

Q: You need a signal off to the publisher that says here's the user's data and what the user wants to do that. The IAB can say here's what I'm allowed to do with the data.

Q: If you read these privacy notices, you will get a term, interest based advertising. What it says is do you consent to have ads delivered against your profile based on your interests gathered. Content targeting, AdSense. Technographic targeting. Geographic targeting. No stalking, not a term of art in the industry.

Doc: I don't like the term no stalking right now. Since Harvey Weinstein we have to lose it. The problem is targeting. My friends at Ad Block Plus, say it's all about acceptable ads. It blurs the whole thing. What I want to support is publishers who want to see an ad in the Wall Street Journal. A trillion dollars has been spent on ad tech but not a single brand has been made by it.

Q: We're testing if one of Jason Kidd's clients can make money off the no stalking tag.

Q: If you say no stalking equals no interest based advertising...your problem, is this no stalking but do

what you like downstream, or are you saying no stalking and no interest based advertising? They're separate things.

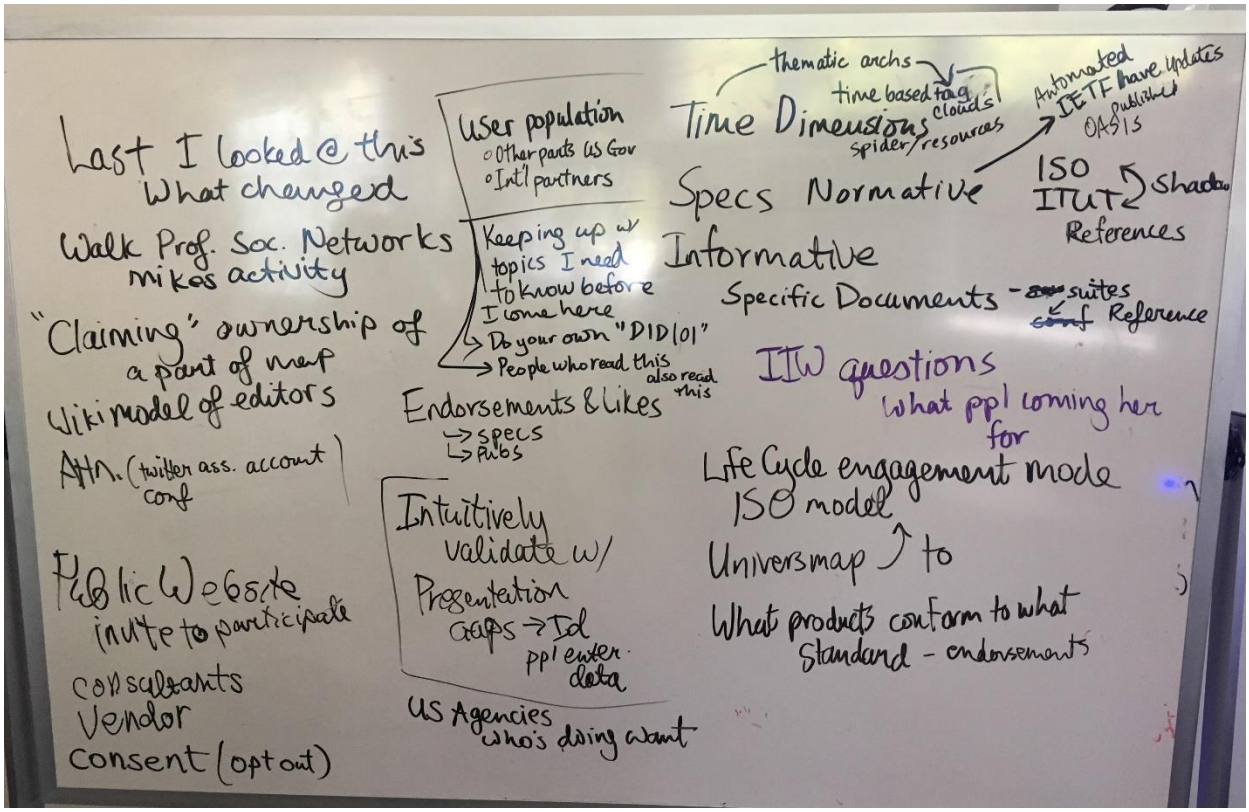
Doc: Everyone in the direct marketing world, all of Google and FB, advertising is basically interest based.

Q: Ad choices, you go into their system, don't work for the next site. All the agency is on their side.

Ecosystem Map – Explore Where Could It Go – Insight Treasure Hunt

Wednesday 2C
Convener: Kaliya
Notes-taker(s): Colin Jaccino

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



Estonian ID Cards Internet Voting

Wednesday 2D
Convener: Kaur Virunurm & Martin Paljak
Notes-taker(s): Kaur Virunurm

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

Pdf presentation available here:
https://drive.google.com/open?id=0B_luqCyRPBXjQlZRMlVPWUtPX3RMal9FZWNHUzNkU0RzN3NF

Group Privacy

Wednesday 3A
Convener: Justin Richer
Notes-taker(s): Danielle Johnson

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

Group Privacy… what does that mean?... A group discussion on what this could possibly be

- Small hop link
- Differential Privacy

Privacy
- We are building tech systems such that they ask for permission ahead of time

Group Privacy (also a book by Dr. Taylor)
- How do privacy and consent change when talking about more than one person? My privacy vs my privacy in this group

Define Privacy
- What group?
- What are the groups?
- What type of setting are we trying to protect

Consensus/Group Control over security that involves us knowing what privacy/protection settings exist

Ex: Someone consents to be tagged in a photo on Facebook, but asks that the location is not included. While the person taking the photo has recently shared their location (but does not specify it in the picture itself)

Now the person who asked for the location not to be shared in the person's photo can be pinned to a location by someone who sees the photographer's recent location sharing.

One on one comfortability vs group settings where one person is less private and breaks down the whole privacy level (only as strong as your weakest link… or less secure/private in this case)

Vegas Rules: Just don't talk about it (informal rule which is known, but has no written specifications)
Chatham Rules: Formal set of rules, written down and easy to follow… as long as you read them and know them

Socionormative vs technological privacy (what we are trying to solve)

Two individual consents that neither could send individually, but in a group setting, they can suddenly communicate to each other. What needs to be protected here?

Boundary Turbulence. What are the boundaries? What are we hurting by pushing certain boundaries?

We understand endpoint rules (what we are trying to obtain), but how does technology catch up to what we are asking?

Ex: When factories were first established, we had child labor because children were the only ones small enough to get around equipment to fix things. Eventually, technology caught up and we could use machines to take the place of what children were forced to do. We protected children and workers by advancing technology.

Public privacy controls: Even though someone who doesn't know you posts something with you in it (and cannot tag you), doesn't mean that someone who does know you won't see it and identify you. The world of the internet is vast and social media connects us quicker than ever.

How is privacy controlled in a public space?

- Anyone can take a picture of you and post it however they please

Public space causes different behaviors from people because they always have this nagging thought that they might see someone they know (like how some people have a "phone voice")

Private spaces allow us to let our walls down and express what we want without feeling like there will be many repercussions.

Public space: outside a home (figuratively)
Private space: inside the home (but even then, we require specific rules to prevent others we allow in our home to follow the privacy rules that we have set for ourselves)

Rules of what we can apply for privacy are too limited (this is the problem. It's vague and we don't understand what we are trying to protect)

Privacy/security vs usability/functionality

- Usability will always win
- We want the new shiny right now instead of wanting to make sure it's protected

Online disinhibition effect (aka general dickwad theory of the internet)

- We can't stop what some other idiot is going to do

Facebook has started the idea of Group privacy.

- Public groups
    - Everyone can see them, and unless a setting is made, anyone can add them
- Closed groups
    - You can search for it and see who is in it, but you cannot join without permission, and most posts are protected to a certain degree
- Private/secret groups
    - You cannot search for these groups or see who is in them. You must be added by someone already on the inside

How do we set rules that allow people to understand security and how their choices effect everyone by becoming part of a group?

We can't control what other people are doing, but how do we get people to follow a policy?

- How do we do it if we want to? And how do we protect those who do want to follow this policy if someone doesn't?

When data mining becomes data in the future it may harm us and we may not be prepared to deal with it.

Privacy issues happen at collection, not at the use of the data collected

- Like with Equifax, someone has your information, but we are constantly forced to wonder if and when it will be used.
    - How do we protect ourselves before and after the collection of the data?

How sophisticated does a user need to be to protect their own identity/information based on what someone else is doing with it?

Knowing a policy, but not expressing what you want from it

- A big issue of not protecting ourselves… not knowing how

Has the price of privacy become to simply not become involved with society?

Adapting to the newest tools and technology change our sociobehaviors.

- We as humans adapt as a whole to what technology is and what we expect from it
- People are changing their expectations of what all these social media tools can do
- We also bring past tools and experiences and apply expectations to the new tools
    - Different generations have different expectations of things

Even private groups can be leaked (copy and paste, screenshots, etc)

Ideal of platonic solid (Plato) vs shadow of the real world

Design pattern for group privacy over ideal of platonic solid?

- Can we attempt closest perfection to reach these policies?

Mapping of human interaction onto a graph effecting privacy wishes of certain people (this is a goal to move us towards what time of privacy goals we wish to reach)

Group privacy a subset of public privacy policy?

- What can we use as a base to build into what we want from something we already have?

Social contracts to respect each other

- It is typically in our human nature to have some sort of respect for others (even if it's only those we hold to certain standards)

Specifying language of what it means when someone says "I don't want my picture taken"

- Defining the language of human privacy

What's reasonable to expect? What's reasonable to ask of others?

As a society, we come up with expectations and rules as we experience things

- We are building that plane as we are taking off
- How can we prepare the plane to be ready before takeoff?

Building Community for Sovrin and Hyperledger Indy

Wednesday 3B
Convener: Sean Bohan
Notes-taker(s): Sean Bohan

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

Purpose: Discuss and crowdsource ideas for growing the communities of Sovrin Foundation and Hyperledger Indy

How do we get more contributors to both

Ways to start building a movement behind self-sovereign identity via Sovrin Foundation

Who: Sean Bohan (Sovrin, Indy), Nathan George (Sovrin, Indy), Steve Tolman (Sovrin, Indy)

What Happened:

Instead of crowdsourcing ideas, we did a mid-deep dive on:

- Indy and Sovrin
  - Indy is the open source Ledger and SDK codebase
  - Sovrin is the first public DLT based on Indy
- History of the two
  - Evernym - Self Sovereign Identity startup

    - Sovrin - launched by Evernym to be a global, independent nonprofit that runs the Sovrin DLT, manages the governance of the network and is an advocacy group behind the concepts of Self Sovereign Identity, Verifiable Claims, Pairwise IDs, user agency, etc.
    - Indy - Hyperledger invited Sovrin to apply to be contribute the code and be the first blockchain in Hyperledger purpose-built for identity
- How they work
    - Trust Framework and Governance
    - What is a Public/Permissioned Ledger vs. Public or Private
    - Network structure of Sovrin
        - Trust Framework
        - Stewards
        - Validator Nodes (write)
        - Observer Nodes (read)
        - Agents
        - Apps
- Resources to find out more
    - WIndley.org (Phil WIndley's blog)
    - Sovrin.org
    - hyperledger.org
- 4 ways to work with Sovrin
    - Production Network (live Sovrin network)
    - Sovrin Test Network
    - ETN (Enterprise Test Network)
    - Getting Started Guide
- We need more content
    - Explainers, videos, webinars, blog posts
- What other WGs can add value?
    - We have Ledger and Agent WGs
    - would an Indy UX WG be helpful? Should that be included in Sovrin
- Discussed ways to get more people participating
- Starting points for Indy: https://wiki.hyperledger.org/projects/indy

Digital ID in Cities – Use Cases and Pilots

Conveners: John Wittrock (john@sidewalklabs.com), Chris Anderson (canderson@sidewalklabs.com)
Notes-takers: John Wittrock, Chris Anderson

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

Cities, Municipal ID, Self-sovereign ID user experience, ...

- Intro to Sidewalk Labs:
    - Building a part of a city, and sees identity as crucial to the experience in a city from the internet up
    - But see the need to preserve privacy and social contracts around how we already interact with cities.
- Why cities?
    - Flexibility - doesn't need to work for an entire country
    - Smallest unit of gov't - allows public oversight
- Precedents
    - Municipal IDs: nycID, Elm City ID, Dubai
    - Digital driver's licenses
    - Federated logins: Securekey
    - Status quo: log in and pay parking ticket with your driver's license
    - Digital ID: Dubai, Switzerland, Singapore
- How do cities tend to work?
    - Pilots, RFPs, etc.
- Unique challenges to cities
    - Cities are going to require a credible "help button" for users
    - Cities may want some sort of ability to reset the system or at least prevent forks
    - Equity, accessibility problems pervade all city services problems
    - As much as we like to talk about the backend tech, much of this is a user experience problem
- Use cases
    - Access to city services
        - Physical services - courthouses, police stations
        - Digital services
    - Verifiable citizen engagement
    - Proofing for service providers
    - Physical access control
- Existing pilots
    - Illinois, would love to hear about that
    - British Columbia: DIACC
- Potential pilots
    - Start small: citizen engagement, feedback, homeowners association
- Open Questions:
    - What's the best-in-class tech for user experience and backend implementation?

How 'Private Sharing' Breaks the See-Saw or Do More With Data, Not Less or Thank You GDPR

Wednesday 3E
Convener: Julian & Tarik
Notes-taker(s): Tarik

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

Typically, privacy and sharing are seen as diametrically opposite and in a fixed relationship where more of one means less of the other - kind of like a see-saw.

We explored the concept of "Private Sharing" where permission to access data is granted to an application that processes that data on-device or next to the data and doesn't need to send it off somewhere else for processing. Once the data is processed only the results are sent off and the data is discarded.

This concept of private sharing would entice users to share more data (as it is just processed to produce a result) and preserve privacy, thus breaking the locked-in "see-saw" relationship between the two.

In addition, we looked at Consent Access as implemented by digi.me and some sample apps that request data locally, process it on-device, produce a result that is sent off and then discard the data. We think more companies should adopt private sharing.

For more info, or to continue the chat, reach out to julian@digi.me and/or tarik@digi.me.

Intro to Cryptocurrencies, Tokens, Token Distribution Events, and Tokenomics

Wednesday 3G
Convener: Nick Johnson
Notes-taker(s): Nick Johnson

Tags for the session - technology discussed/ideas considered:
ICOs, Fund Raising, Community Building, Crowdsales

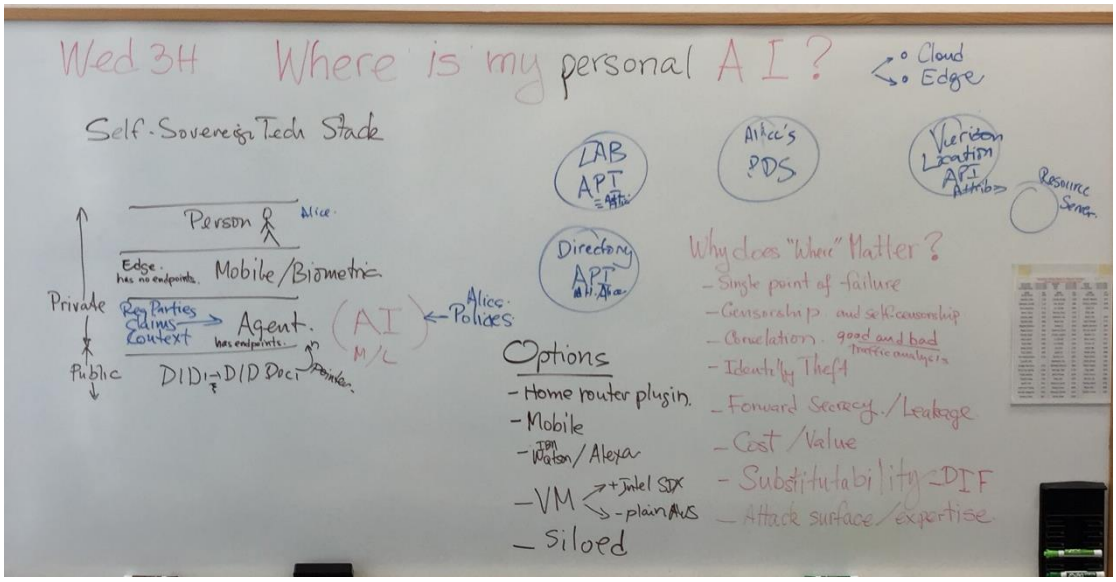
Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

Here is a link to the slides used:
https://docs.google.com/presentation/d/10nmTw_6FDO0PmoK1hWssbaNRZg16wCK9mVDXaUqC2Y8/edit?usp=sharing

Where Is My Personal AI?

Wednesday 3H
Convener: Adrian Gropper
Notes-taker(s): Adrian Gropper

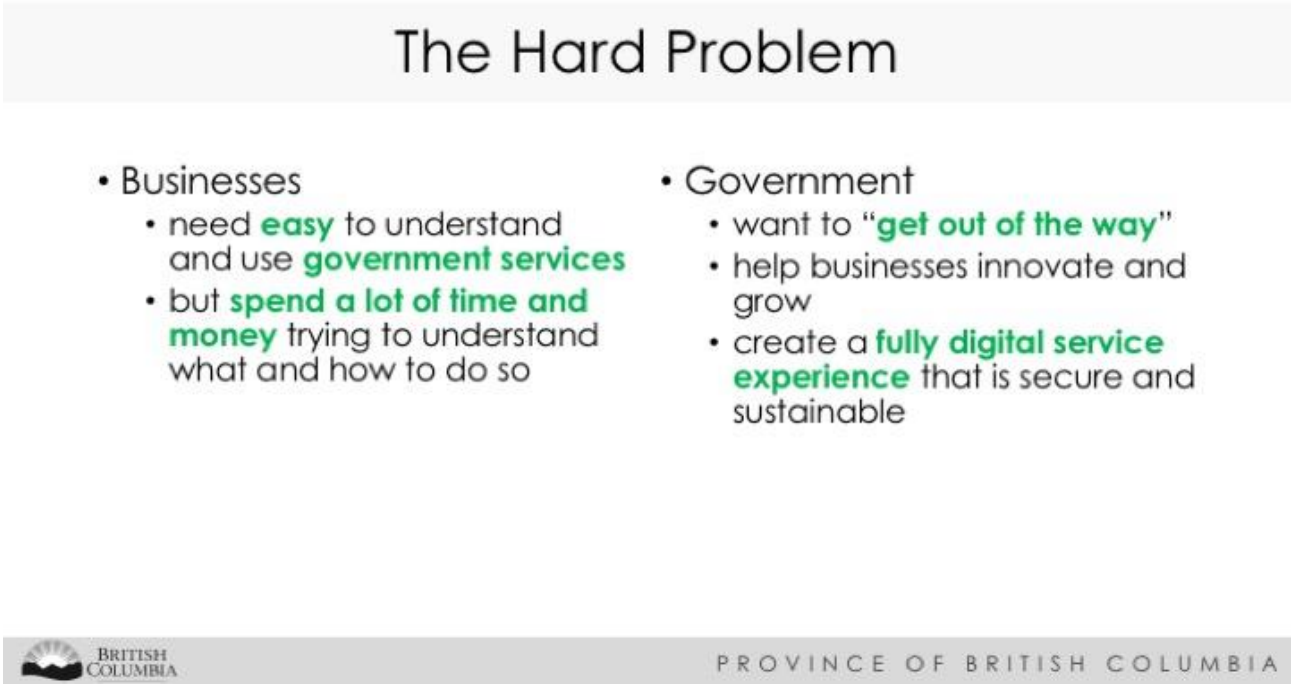
Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:



Verified Organizations – Bootstrapping a Self-Sovereign Identity Ecosystem via Government Services for Organizations

Wednesday 3I
Convener: John Jordan & Stephen Curran
Notes-taker(s): John Jordan

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



Digital ID & Authentication Council of Canada

Non-profit coalition of public and private sector leaders

Developing Canadian Digital Identity standards

Foundational work to Canada's full and secure participation the global digital economy

How are we learning?

- Committed to strong participation in the Pan-Canadian Standards community
- Learning by Doing Approach
  - First Proof of Concept – Corporate Registries – Complete
    - Developed Blockchain proof of concept to allow shared writing of data from multiple Corporate Registries to a unified ledger
  - Second Proof of Concept – Verified Organization Network
    - An open and trusted network of organizational data that enables the discovery and verification of organizational identity and related verifiable claims
    - Collaboration with the Office of Small and Medium Enterprises in the Government of Canada, DIACC
  - Continuous Service Improvement Lab
    - Over 10 teams delivering a range of programs working together to design and deliver digital services in a co-located space, with tech, tools and training to support the team and increase productivity.
    - Hiring staff skilled in agile and new development methods to leverage new thinking, ideas and expertise

What do we verify?

Verified Organization Network

Verified Organization Record

- A digital service which provides visibility of an organizations activities with government (at all levels) from creation to dissolution. A trusted digital record for a **Verified Organization**.

Verified Organization Affiliations

- A digital service allowing people to easily manage who (and what) is acting on behalf of their organization. A unified experience where a **Verified Person** with a **Verified Relationship** to a **Verified Organization** can manage their digital relationship with government.

Mary's Bakery

Provincial: Incorporation

Regional Health Authority: Health Operating Permit

Municipality: Business Licence

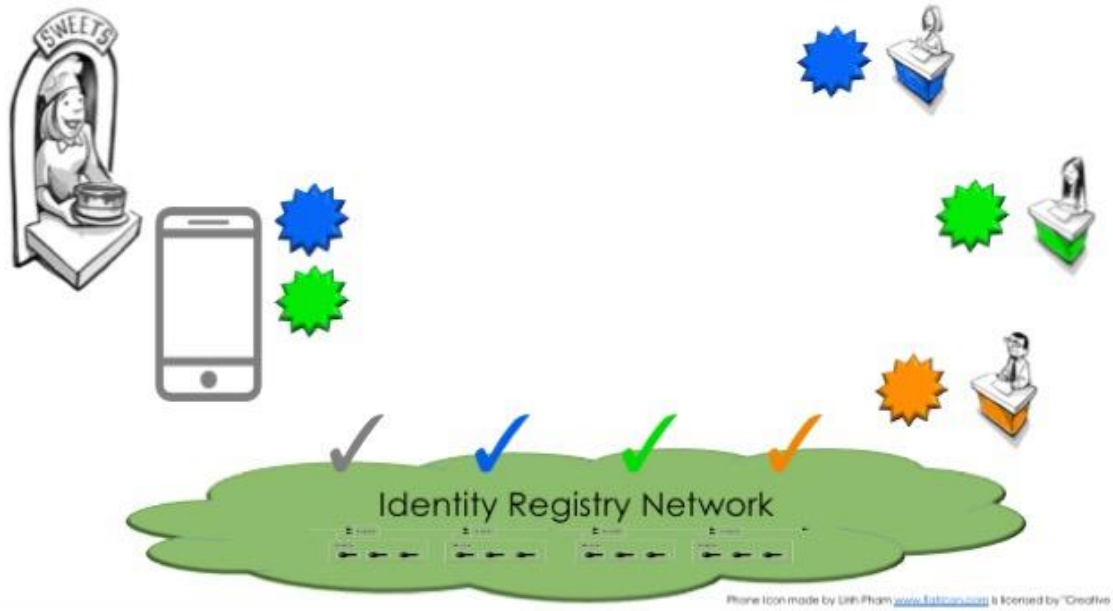
BRITISH COLUMBIA PROVINCE OF BRITISH COLUMBIA

BRITISH COLUMBIA PROVINCE OF BRITISH COLUMBIA

The new awesome way

- Businesses
  - **don't need to re-establish** who they are every time they access a new service
  - have a **stable and enduring relationship** with governments under their explicit control
  - can **consent to data sharing** between government programs and other businesses
- Government
  - programs **don't need to ask** businesses for information they've already provided
  - **don't have to build and maintain** their own login and identity services
  - **enable businesses** to do business digitally anywhere

BRITISH COLUMBIA PROVINCE OF BRITISH COLUMBIA

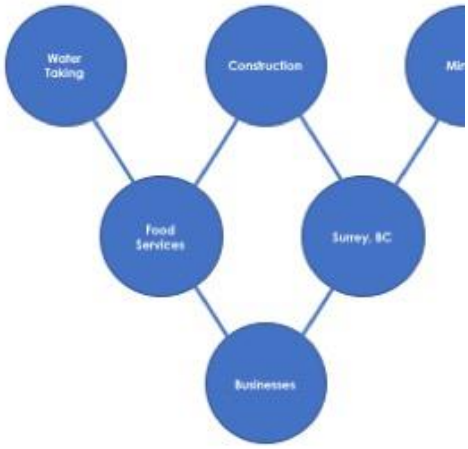


Phone icon made by Linh Pham www.flaticon.com is licensed by "Creative Commons 3.0"

BRITISH COLUMBIA PROVINCE OF BRITISH COLUMBIA

Bootstrap to drive Network Effects …

- Government **issues verifiable claims** for businesses
  - incorporations, permits, licences, contracts, grants and more
- Government establishes a **trusted public repository** of verifiable claims
- Adoption and Growth Strategies
  - "**Single User Mode**" provides immediate value
  - "**Bowling Alley Strategy**" breaks problem down into manageable segments



- ✓ Create TheOrgBook (like "TheFaceBook")
- ✓ Identity-enable TheOrgBook, Services
- ✓ Load Verified Public Claims

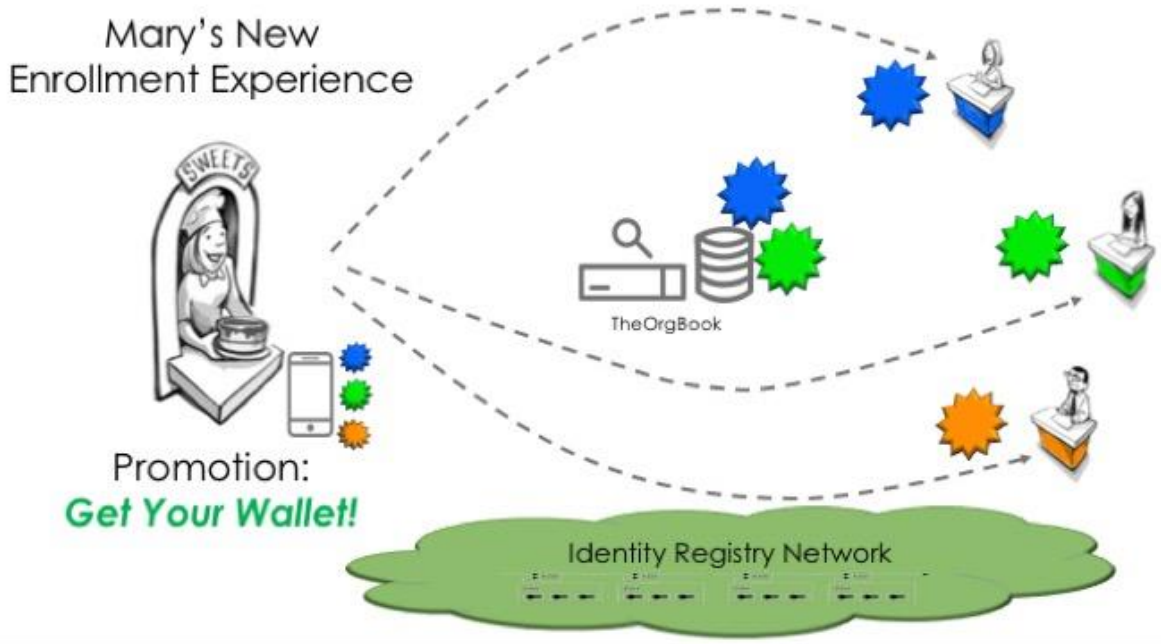
Approach:
Drive the Supply Side
SSI-enabling Government Services

TheOrgBook

✓ Identity-Enabled Services – one-side of the market

✓ Services receiving, creating Verified Claims

✓ Patterns (and code!) to SSI-enable more Services



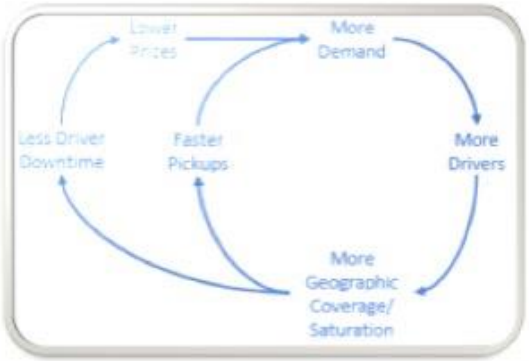
BC's Trusted Digital Ecosystem for Business

Empower businesses with
a **locally**-issued
trusted digital identity
that can be used **globally**.

BRITISH COLUMBIA PROVINCE OF BRITISH COLUMBIA

Whiteboard Plan: Verified Organization Network

TheOrgBook-model generates
network effects that drive
self-sovereign identity **adoption**.



BRITISH COLUMBIA PROVINCE OF BRITISH COLUMBIA

Learn More?

GitHub

https://bcgov.github.io/TheOrgBook/

PROVINCE OF BRITISH COLUMBIA

Proofing + Assurance Combo – ID Proofing & Standards for Identity Assurance Across Systems?

Wednesday 3J
Convener: Larry Vernec (Intuit), Lily Bragg, Alan Viars
Notes-taker(s): Scott Mace

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

Larry: Doing some phone proofing. KBA [knowledge based authentication] 65% success rate. Phone proofing similar.

Q: A couple of B to B examples. Turning.io, Turn Technologies, data broker in Chicago. Greek Sky Credit in Atlanta.

Q: FBI runs identity proofing as a service. Even for school bus drivers.

Q: The challenge is the in-person component. Hospitals. Also banks. It's more remote ID proofing. Imprivata offers one. Symantec offers remote login.

Q: authenticid.co has moved into identity proofing.

Q: Morphotrust is now Idemia.

Q: Tascent.com

Lily: How do you aggregate behavioral antecedents?

Q: Depends on the context. What behavioral touchpoints are there?

Lily: Medical credentialing. How do we get something more rigorous than KBA?

Q: Peru has a government-issued identity card.

Intuition (Part 1) - From Ego Identity to Field Identity

Wednesday 3K
Convener: Sharon Franquemont
Notes-taker(s): Sharon Franquemont

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

Intuition: Definition, Intueri Latin for *to know all at once*.

Discussion 1.

- Our understanding of intuition.
- Intuitions arise out of a base of information and knowledge already acquired, e.g. Mozart doesn't intuit DNA molecules, athlete doesn't intuit mathematical formulas
- People often describe the source of intuition in body-based terms, e.g. "my gut (most often used by men) or my heart (most often used by women) told me." Neuropeptides (protein-like molecules used by neurons to communicate) in gut and heart similar to brain
- End of seeing intelligence as arising from the ability of 'human containers' to spit out information. Intelligence, to some degree, is the ability to take information in and spill it out directly or in new arrangements
- Living in sea of information discernment of inquiry and identifying *most* useful direction becomes important
- God's importance is brought up…definition of God as a distributed force or a parent figure, e.g. what is role of God or spirit concept in intuition

Discussion 2. Patanjali's question thousands of years ago: *How does anyone know anything?* His answer: 4 Stages of Knowing.

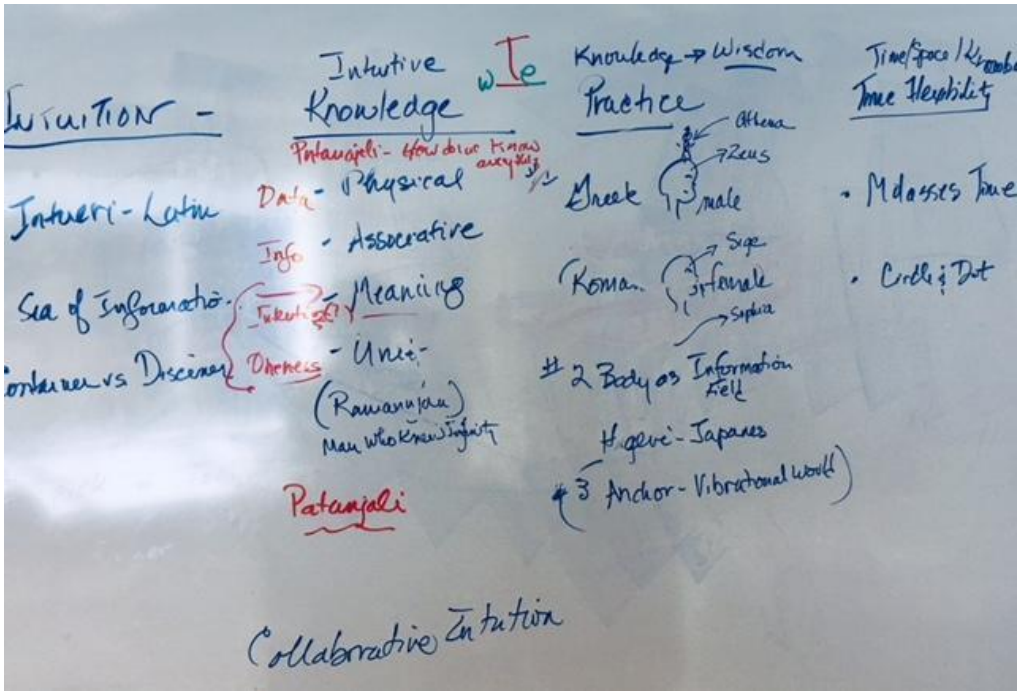
1. **Physical knowledge**: appearance, touch, hearing, etc. through the senses knowing (Data)
2. **Associative knowledge:** understandings based on previous experience and relationship (Information—relational)
3. **Meaning knowledge:** intention, purpose found in people, organizations, things, events
4. **Unity knowledge,** oneness between knower and know (example is famous turn of 20th C. mathematician Srinivasa Ramanujan who solved equations, but could not provide proofs. He had little formal education in mathematics, became the youngest person to be inducted as a Fellow of the Royal Society at Cambridge, and his formulas are being used today to explore of black holes. 2015 movie about his life is *The Man Who Knew Infinity.* He explained that his solutions came from the Goddess he worshipped and said, "An equation has no meaning, unless it represents a thought of God."

Discussion 3. Practices to enhance intuition

A. Western views of how wisdom arises.
   Greek: Athena, Goddess of Wisdom, is born out of the head of her father Zeus, emphasis on *male and intellect*

Roman: Sophia, Goddess of Wisdom, is born out of the womb of her mother Sige, the Goddess of Silence, emphasis on *female and silence.*
Practice: to bring balance to your intellect increase your practice of silence (not just verbal—mental, emotional, body silence) in a conscious, daily way.

B. Adopt full body knowledge—See body as an information field.
   a. **Check with gut:** Japanese call this your *haragei* and no successful business person makes a decision without consulting his or her *haragei.*
   b. **Check with heart:** Many people refer to this as "it feels right" or "it feels wrong"
   c. **Alignment** with intellect, heart, gut and whole body is most effective.



Identity for All

Wednesday 4B
Conveners: Bryan Pon, Jeff Arresty, Peter Simpson
Note taker: Mei Lin Fung

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

Identity for Financial Inclusion and Identity for Refugees => how to empower self sovereign identity – need to have network effects and collaborate on a proof of network effect. SLACK group will be formed - ID2020-discuss@googlegroups.com

UN and World Bank were part of the discussion, lots of interest in continuing the discussion.

Transcript of session

Brian of Caribou – new tech and systems for identity – what does it mean for emerging markets and constraints, vulnerabilities, use cases – diverse landscape

Perspective for next generation technology solutions – where appropriate and can provide value?

Doc – those doing things say what we are doing

Brian of Caribou Digital – research firm, 6-month project in India interviewing end users about experience in managing multiple identities, digital, analog, state based etc; Long tail for whom system does not work very well – what is impact of being enrolled. Social Science research. DIFID identity with refugees, World Bank field work on experience with identity systems

Peter Simpson – iRespond – SE Asia – UN refugee camps 100k UNIoM, provide digital identity – support of govts – give stateless individuals biometric identity, then transcript of skills, training, education, shift from stateless to documented

Thai gov - anti human trafficking – 700K migrant workers to get digital identity to not be exploited – thru block chain – Africa HIV experience

ID 2020 – Dakota Groom – UN Exec Director – thinking about challenges from 2 lenses

1. How to assure new and emerging technology is brought to bear on these challenges in developing markets? UN agencies understand needs on the ground- have input to tech developments – bring actors together in an institutionalized way, governance mechanism – beneficial to people – convening that conversation
2. Funding – significant attention by UN agencies and others to provide some form of identification eg UNICEF supported birth registration, UNDP voter registration – they use different vocabularies and fundraise in different streams – silos – so cover smaller populations – hugely inefficient use of funds, repeat and conflicting investments, ensure people's information is fractured and out of their control

Need to change flow of funding by UN agencies – no communal fund for enabling people to access identity – key market failure and key opportunity

Working with 2 large international organizations to scope out GAVI – global vaccination for 60% of world's children. Vaccination card – no follow up, or tracking. Huge incentive to manage that relationship

UNHCR – bio metric identification system – valuable to a refugee while in a camp – ultimate goal is to seek re-settlement

How to work better with World Food program, etc

World Bank – IT dept – innovation and technology unit – Susan Saravich

1. Blockchain lab – looking internally and externally into how to prepare clients to leapfrog development – identity is the big use case; new organization – found that there are lots of innovation labs in UN agencies and open to collaborating together – WB senior mgmt. agree important to work across Un agencies

Jeff Aresty – Internet Bar Organization – Justice layer as a community for all- Haiti, Brazil, Africa, Afghanistan – like American Idol on line – recruit talent, do training in law, do video work and put process up on line – sold music

Created opportunity to look at Justice layer – and Identity system is broken. This is key – identity for entry into justice layer

Identity for the next billion – IGF could start in developing world – identity

Where is pilot – discussion with Peter Simpson - presented digital identity for stateless refugees

Norms can emerge separate from state organizations – in stateless environments

Myanmar – Peter Simpson – set of tools for response agencies – develop a system that could grow – connect to FinTech

Use US Vets are evaluators – ones who know the cultures, dispute resolution approaches

Build a set of norms – ISO and ANSI folks – what would we need to do in a pilot to develop best practices, working to get project off the ground – take to refugee camps

Mei Lin – People Centered Internet co-founded with Vint Cerf – In the next generation of the internet, need to assure humans are at the center of what we do. This is a shift from talking to trying things and learning. We have identified PILOT'ing in NorCal, with the intention of moving out and rolling out next in Puerto Rico. Currently working with Solano County Public Health and Medical Reserve Corps on medical identity – next establishing identity for educational and financial purposes. Will have a workshop on Day 3 first session on scoping out the Norcal Pilot.

Tony Rose – micro loans via AirTime – digital identity – JUVO.com consultant; empower individual to accelerate whole economy

Guiding something this year – onboarding small loans in Paraguay and Malaysia – financial institutions that will accept this and shift to more than microloans

Kaliya – Pillar Wallet – open source wallet – personal data wallet

Nick Johnson – Sovereign Foundation – Identity for All – council charge is to support experiments to proof of use cases

Drummond – trustee on Sovereign foundation – global public utility to serve identity for all – we have a social responsibility to pay attention to those not in a position to have identity at all

We will support you – Brian, Dakota, Susan

Tech is only a small part of the problem

Jack – John Callaghan VERIDIUM– Grant from Gates Foundation using biometric identity for payment system – Identity assertion system – UAF – hooks for active assertion – DSF project is limited to Android system – want to USF

Lara – Georgetown University – BECK center – thinking about scaling social impact – receive money from Rockefeller Foundation to build an ethical framework for using Blockchain – eg refugee identity – what are risks? Want to come up with questions so developers know what to be thinking about

Dakota - UN ID 2020 Alliance – purpose is to sort out risks – Dakota – governing board, ethics and risk, technical committees (front end eg biometrics, UX, UI, interoperability) Implementation, Eco system and advisory committees; Framework for working groups to ensure mechanism to bring issue to the fore – eg new bio metric – have a process for feeding it into the advisory committees and feed up to the board Dakota@ID2020.org

Lily Bragg – go no go decisions – where is this being documented?

Dakota – there is no clear and consistent documentation – many procurement processes –

Susan – WB – set up a knowledge share that is open to toss ideas around – locations what you've learned in specific implementations, partnering, dealing with govts; Use cases – what is WB working on?

Brian/Caribou – ID4D team – is looking at it.

Susan – not public report

Dave Crocker – is there a place to register for an ongoing discussion that could be turned into deliverables and get group collaboration

Dakota will set it up….

Jeff Aresty – we have set up JusticeHubs.tools - as a justice project – Justice cross culturally means different things to different people and generations – space for connection – linking into organizations – SLACK, GITHUB – print up a set of notes from this discussion

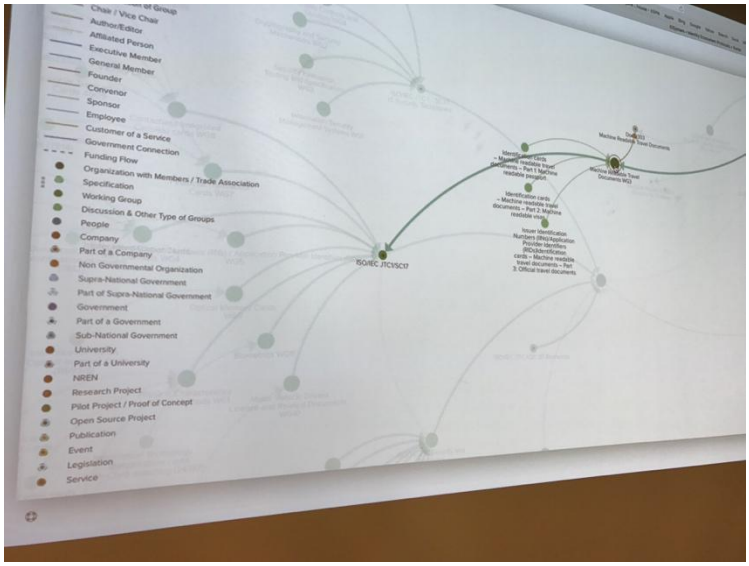
We are looking for guidance and direction – at this early stage we can set it up

Lily – guidance and direction on what? Is that intentionally nebulous

Jeff – the next 3 billion coming on line – refugee communities are a vulnerable use case – what tools do they utilize

First, we started with Fintech then, health became a priority instead – has happened even as Internet Bar Organization started with Music

Kaliya – funded with your tax dollars – Photo – URL but not published



Please do not circulate – it is an early version of the Eco System Map – all standards, all specifications, all papers, all people, all events – contact Kaliya kaliya@identitywoman.net Moving to UWashington Scott David and Kaliya

What communities need?

Web interface to add node to the map and create accounts for people in this room who have write permission to the Map.

Lily Bragg – do outputs of different entities also get logged eg work from team Canada for processes from identity group so can compare to Estonia group

Kaliya – if there are specifications we can point to it from this map

US Gov, state of Virginia

Maria/IEEE – how would we get our IEEE working groups in there?

Kaliya – Would have IEEE authorized to add nodes, and have moderated input from others

If you are interested in writing to the eco-system – I will send out a note to this room- here's how you create an account to add to this

Susan World Bankl – This is a lot more elaborate than a sharing experience that I envisaged – I am afraid of messing this up

Kaliya – we have a great taxonomy – Anil of Dept of Homeland Security pushed to have a reasonable web UI to add data

Tony Rose – how to have a collaborative process?

Kaliya – could have a project as a "thing" – so what projects are getting government and other funding in the Identity space

Joyce –this is just a list – if you want to contact everyone – people might leave organizations

Kaliya – there is a community building piece –

Jeff – we are connecting 300 community legal aid organizations – IT people and exec directors – to limit first round of participants – then reach out further – a SLACK channel and different ways to communicate – then community can design how to go forward

Maria – we have our blockchain SIG on SLACK – development, issues are all discussed – share projects, links to GitHub – sometimes get a lull – have to keep each other inspired to keep going – recognize that it's the nature of the beast – this fills our digital inclusion thru trust and agency – not just emerging regions, but in developed areas where people can't afford broadband and bring them online within a trusted platform – not to exploit them, and prevent them from being exploited later. Find ways so all are equally projected. What does it look like when you have AGENCY over your digital identity. When a digitally illiterate person comes online – how to prepare them

That's what we explore in the Industry Connections program

Lily Bragg (Vouch.id) – how to get an MVP up during a Blitz attack

(different entities focused on different areas – tech, policy – but we are talking about humans – so why not think about how we impact humans together and get actionable tools for humans. Must get enough momentum around some small community – have to get it done in one area)

Maria IEEE – idea is that each org has a different focus, IEEE is technical, ID 2020 is more development focus

Lily – is there interest to get work done?

Susan – could use Kaliya's map to see who is doing payment systems in Somalia – this is great

Dakota ID2020 – to answer Lily's question – we don't want to have 6 conversations all of which vaguely overlap – home for connecting two different related conversations

Kaliya – I would like this to be a home for the concrete documentation, it's not for ongoing community conversations

Dave Crocker – just created a google group called ID 2020/Discuss – this is for NOW and you will migrate

Dakota – I will set up a SLACK

Tony Rose – network effect of a self-sovereign identity – needs financial institutions etc

Dakota – that's our core perspective – how can we bring that network effect about – imagine for large companies – it's not a commercial opportunity in identity itself, but we can benefit by facilitating identity for people – a way to finance that global public good

Tony Rose – if there is a locale with self-sovereign identity – does it really increase economic opportunity?

Drummond: Everyone sign up here: ID2020-discuss@googlegroups.com
To have an overall solution – the decentralized identity layer will serve all of us – and we will get the network effects – the wallet in developed world may be more specialized, and also different in the developing world ~ Its momentum for overall network effect for identity

Kaliya – Sean Conway's model – lab with 6 companies – then next generation with 6 more partners – to build apps using infrastructure and there will be more.

OAuth OpenID Decentralized Identity

Wednesday 4F
Convener: Justin Richer & Nathan George
Notes-taker(s): Scott Mace

Looking for patterns and commonalities; looking for terminology mismatches.

A lot of patterns have been solved.

How do get enough nomenclature up on the board.

Justin on OAuth: Started 10-11 years ago when APIs were protected with user names and passwords. How OAuth works, the fundamental assumption. Web site on one side and other side. Wasn't want the entire world looked like. OAuth2 added things that didn't exist, such as mobile.

Still assumption OAuth is about protecting some type of API. The interesting thing with Open ID Connect is we will define an API. That API is who is the current user. That's who you're protecting. Twitter and Facebook did this exact pattern. A million versions these days. The architectural assumption is there is an API that has all my identity information that I'm trying to give access to.

Nathan: Self-sovereign idea. Trouble is a lot of these services, the only construct that makes the user the user is under their control so you can disintermediate the user entirely. Self-sovereign: Intermediate the data and the user. No one can impersonate this entity. Differs a lot from UMA. Not that user manages access. Point is entity can't be impersonate. No central CA or root of trust. Use cryptographic key instead.

Q: Core of all truth starts there and not anyplace else.

Justin: An antipattern Open ID Connect set out against. If look at more traditional SSO systems, spit out encrypted domain cookies, SAML and Open ID 2, hand something to user's browser who hands it to a bunch of different sites. But this whole notion of the user having to carry that artifact with them, when you build this around a Web browser, turns out to have holes and bad problems. Info leaks into browsers and plug ins. Browsers being tricked to send cookies to domains. So one thing Connect did by basing specifically off OAuth was to get user info directly from the API. What user had was generated by a trusted authority. Harkens back to X.509 PKI. You get same thing, your cert, for everyone who asks. Lots of problems with lack of flexibility. The whole API-based Connect model was by and large a community tech response to a lot of the problems with that system, which is why it doesn't get rid of the notion of the API but moves closer to it.

Nathan: Self-sovereign doubles down on claims being verified by a third party for triangulation. All info can resolve back to something I'm willing to use to grant access to the API info.

Q: These problems bit first-generation bitcoin startups.
Nathan: You're looking for third party attestations. Look at the CA authority, that is their business model. To bind a key to an attribute in question. By moving model away from RP, info flows more easily, but also making seeking back to the root of trust a multistep process. Hope is you are dealing with the same issuers over and over again so you're not paying for the expense every time. What's the plausible deniability of a driver's license? By automating this, I can ask a driver's license authority, how are you an authority? The hope is to boil it down to a smaller set of info. To present minimal

information to a bouncer. Just like identity is contextual, trust is contextual.

Justin: In order to get scalability, we outsource a lot of that stuff.

Nathan: One of the strangest topics, how do I know what this attestation means. Anyone who has worked with medical data knows people don't put the right things in the right fields. Trust is who is the issue as well as the schema and how strict that is. Need some sort of chain of custody.

Justin: Do you want market forces controlling your schema?

Nathan: Some sort. It may be glacial.

Justin: It's the acceptance of trust I would be surprised.

Q: You can have a normally trustworthy source be untrustworthy for a time.

Nathan: Which is why a ledger can be helpful, because of timestamps.

Sam Smith, Xaltry: If you use distributed consensus as part of your trust chain, windows of lack of trust become much smaller. Been motivated by the blockchain.

Debbie Bucci: Like caching?

Nathan: If I can sign a resource, I can distribute it. The way we're doing claims and proofs doesn't give us the ability to reshare, but the idea is once you have this signed data, you don't have to serve as the primary source over time.

Q: Are we still not anchored in the traditional CAs?

Justin: With parts of the Connect protocol, we took an interesting approach. If you look at keys for servers, they are published at HTTPS URLs. If it's in the right place, the key in that location is the key that represents that party at that time. It anchors in that cert without being tied to the CA. That's the interesting bit. You have endpoints that can enter and rotate keys as needed. Web PKI is still a problem we have to solve. But we're not making the mistake of offloading all the trust to the CA. Avoid man in the middle. Leveraged for the application layer key discovery. That is one of the most interesting things to me that came out of Open ID Connect. It explicitly doesn't have a trust chain built in. As I understand it, there is a lot of key addressing on the ledger than can accomplish a similar approach.

Sam Smith: If you think about data security from a common mode failure POV, you can get to low exploits by having a single layer of distributed consensus. If a majority have the same public key, the probability someone exploited all locations is so small…

Justin: Do it right is never the right answer for security.

Q: What's the ledger equivalent of TLDs?

Nathan: I can't speak for all the self sovereign solutions. In Sovrin it's the name space. Search is not one answer for any key. Get a whole list of answers. You will want to search on lots of different types of attestations. From infrastructure, we haven't picked a winner. What are you the authority over? Make attestations over that. The reality is names are contextual depending on the data involved.

Justin: Doesn't that lead to a bunch of competing fiefdoms though? With the Internet, DNS did that for us.

Nathan: Schema anchoring on a ledger can devolve into that. Sovrin is trying to encourage flow of data. So the popularity contest serves a purpose. How do you manage a proximity of different schemas?

Justin: Avenues for innovation. In DNS the text record has been used for so many absurd things because it's so difficult to get a DNS extension through the IETF. It means you have this bizarre free form another layer of parsers and processors to make that happen.

Nathan: You need people to make whatever attestation they want about whatever topic.

Q: How did Consumer Reports become the authority? They did reports. People liked it. Private orgs that become the defacto authority can emerge solely on their quality.

Nathan: Passports and driver's licenses can be trusted from the beginning. The kinds of organizations you look to to bootstrap a network like a self-sovereign network. It's a diffuse route of trust because it's topic-specific.

Q: We're replacing centralized trust with diffuse trust.

Justin: Reality and history dictate that developers and consumers are lazy. You will end up with static whitelists of things I trust. Employees down the line just know we've always done it this way.

Nathan: Self-sovereignty allows mix and match of applications. Right now they don't have a choice because they don't issue common schemas.

Justin: One of the biggest problems federated ID has today. I have a ton of IDPs. Those are all perfectly good. The problem is getting RPs to accept data from any of those. Efficiency pushes things toward centralization in very natural ways. The ideal is a wonderful distributed network. But the practicality of building it and deploying it at scale led to concentration.

Nathan: If we sacrifice trust and verification, we lose the ability to rebalance over time.
Q: Google Docs phishing last year. No way to verify the claims of the application or the person. That is where verifiable claims, distributed ledgers with fault tolerance can elevate the level of trust.

Justin: Something the OAuth world never really solved.

Q: Issue of ID services acting for universities that users don't trust even though they should.

Nathan: This is why search is a good way to validate. The source of trust for signed attestations is everyone.

Q: Any tangible steps to use Open ID Connect with self-sovereign ID?

Justin: If I can get an ID token that says I am a Stanford student and check that using the verifiable claims model, that claim I am making, this hash is me, means I am a Stanford student, need to be able to have your client app do this processing. Ownership of who are Stanford students or what a student is is veriable and calculable.

Nathan: Leverage this Web of trust into your assertions. We have keys for every party in the system we

can do mutual authentication.

Q: Still have to have integrity of the access channel.

Nathan: I can validate non-repudiation on the ledger...dusty threads of thoughts on Kim Cameron's ABC of Trust.

Justin: I don't see these two worlds merging as much as having a handful of conduits between them.

Q: Example. Tokenization of email.

Justin: One of the biggest problems with Open ID Connect in practice is people treat their email address as a global identifier. Nothing ties the email address to the issuer of an identity assertion. Therein lies something interesting. People think about themselves often as an email address. You haven't proven any correlation between the two. In certain subdomains that's fine. With this technology, I could lay claim to something that says I have a veriable set of attributes that I own that email address and I can get it from there.

Nathan: Instead of a Webfinger approach, we relate key material to the token for validation.

Q: We also have the problem of non-email address identifiers such as phone numbers. Allowing people to claim phone numbers.

Know Everything About a Customer, But Know Nothing – How intentional amnesia can be good for Security & Privacy

Wednesday 4G
Convener: Tarik
Notes-taker(s): Tarik

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

This was a more in-depth session on Consent Access, Consent Access Contracts, Consent Receipts and how one could get an app up and running using the digi.me SDK / sample apps for iOS and Android in a matter of hours.

We talked about the benefits of "private sharing" which are enabled by this technology and the major types of data available today: social, financial and health.

We also covered the types of information that are stored in a Consent Access Contract and what it means for the individual and the 3rd party application. The user is consenting to let the 3rd party app access specific types of data from a specific time period, for a specific purpose with the understanding that the 3rd party app will or will not implement the right to forget and process the data ON or OFF device.

Find out more here: http://devsupport.digi.me or reach out to tarik@digi.me.

Mental Models of Identity

Wednesday 4l
Convener: Joe Andrieu
Notes-taker(s): Matthew Schutte

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

SECURITY - focused on bodies. Reducing to a **singularity** Freedom From. I want to feel secure. Space-time travel data

LIBERTY - about how I engage with society, how I am tracked etc. Should not be reduced to my physicality. Privacy is about contextual integrity. Liberty is about **multiplicity**. "I am a different Joe to different people because I reveal different pieces of information. Pseudonym / Alias / Persona. Freedom From. Gay Joe.

DATA - This is about **specificity**. Example: ISO defined. Your identity is a set of attributes related to you. The engineer saying "look, I got to build the system. Just tell me what goes in the database." Bundle of attributes. Point in time.

COMPLEXITY - **emergence**. Identity emerges as a result of interactions. Association. Complex Adaptive System. Ever changing. Time Happens (continuum / endpoints / continuous). Drunk John. Group. Context (spiritual / cultural). Organisms, including social organisms:

- sense
    - interpret
    - decide
    - prioritize
    - act

Others Looking IN: Security / Data
Reductive / Define: Security / Data
Self Looking OUT: Liberty
Relationship (both): Complexity
Elements of: Data
Values: Liberty / Complexity
Identifier: Security / Data? (Identifier as observer)
Identified: Security / Liberty
Verified Anonymous: Security / Data

How The GDPR Is Making Me TRACK MORE

Wednesday 4J
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:

General discussion about GDPR requirements (not exhaustive)

User ability to…

        - Request what is being tracked
        - Download data the company has on me
        - Update some data elements (if they are incorrect)
        - Delete all my data
    - Clear and informed consent
    - Requirement to report data tracked by device identifier and not directly tied to a user (e.g. persistent browser cookie)

- The issue of concern. If we have to give out tracked data based on device identifiers, how do we ensure that data is only given to the correct entity
    - low confidence — device reports the identifiers to the host
        - no way to verify that the identifiers the device is claiming is "theirs" are really valid (i.e. the correct value and not impersonated/stolen)
    - medium confidence — possibly OAuth2 dynamical client reg with pub/priv keys, apps report identifiers in a JWS (signed JSON Web Token) on a periodic basis, host builds a risk-based profile of device based on these signed assertions. At data request time match signed identifiers to risk-based profile to define a higher level of confidence
    - high confidence — didn't discuss this much… probably requires special hardware on the device

- Conclusion — in order to support safe release of data to a device identifier additional tracking must be done

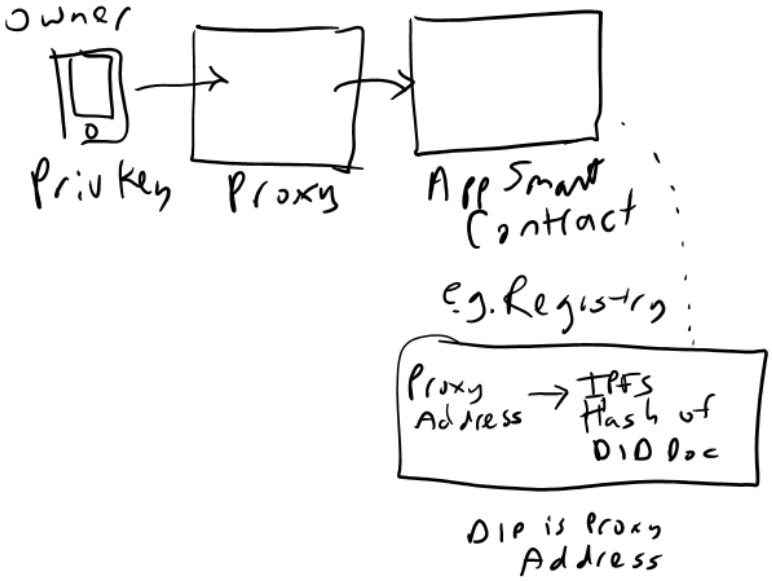
Identity Smart Contracts on Ethereum

Wednesday 5B
Convener: Christian Lundkvist
Notes-taker(s): Ed Eykholt

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

Christian Lundkvist - Uport / Consensys from the uPort team presented their smart contract designs similar to as documented in their whitepaper http://whitepaper.uport.me/

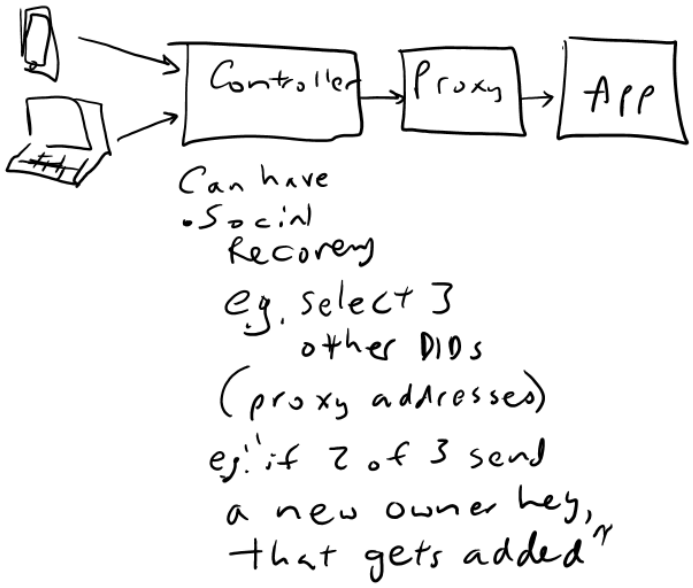
- Smart Contracts in Uport
  - Use smart contract to…
  - Map DID to a DID Document (contains PubKey)
  - Provide a persistent Identity for interactions with other Ethereum contracts
- Proxy Contract
  - Tiny contract
  - Act as a level of indirection
  - Has an "owner" address
    - Can forward transactions from the owner.



Discussions:

- What about Key Revocation (e.g. for a key that was compromised at some as-of date)?
- In the case of a revocation, should previous signed verifiable claims still be interpreted as valid?
- This is an argument for keeping dates in the DDO specification.
- On the blockchain, how is time reliably recorded? Could use a secure timestamping services like Tieron or OpenTimestamps

- What about multiple "owner" keys?



- Main drawback of this design is privacy. Can see the delegates
- Another approach would be Shamir's Secret Sharing Scheme, which would not be visible on the blockchain. Another approach might be the "Horcrux protocol".
- Friction of this approach on Ethereum:
  - Signing a transaction on a device (e.g. to a controller contract) requires paying a fee in ETH to run the network.
  - Could instead have the user create a signature with a key, but have a service that gets that signed transaction, pays the fee, and broadcasts the transaction to the Ethereum network.
    - It is now on the Ethereum roadmap to add an Account Abstraction feature, the access control logic can be handled by the smart contract (and a minor can decide whether to mine that transaction). EIP 86 https://github.com/ethereum/EIPs/issues/86, potentially to be included in the second Metropolis release.
- Risks:
  - There could be taint of one transaction with another. For example, if there is a verifiable claim “I'm over 21” can it be found out how much ETH I own?
- Christian wrote a blog post on how to simplify multisig contracts.

MANIFOLD – A Self Sovereign Internet of Things Platform #Picos

Wednesday 5C
Convener: Phil Windley
Notes-taker(s): Phil Windley

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

- Picos (persistent compute objects). See http://www.windley.com/archives/2015/11/reactive_programming_with_picos.shtml
- Squaretag and its purpose. See http://www.windley.com/archives/2013/05/using_products_to_build_customer_relationships.shtml
- Social things and trustworthy spaces. See http://www.windley.com/archives/2015/07/social_things_trustworthy_spaces_and_the_internet_of_things.shtml
- Demo'd Manifold and the new pico engine.

Pico mesh concept. See http://www.windley.com/archives/2017/07/a_mesh_for_picos.shtml

Fluid Boundaries of Self

Wednesday 5D
Convener: Matthew Schutte
Notes-taker(s): Matthew Schutte

Tags for the session - technology discussed/ideas considered:
Consciousness
Fluid Boundaries of Self
Self-Sovereign Identity
Holochain
General Relativity

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

1. Presented a model of how consciousness emerges and persists;
2. Discussed implications for
    a. Einstein's general theory of relativity
    b. how a human's perception of self is fluid, not constant;
    c. Self-Sovereign identity
    d. Q&A including ways in which this perspective has informed the design of Holochain.

Recording is here: https://youtu.be/yewe6k55hbs

Reputation as a Primal Use Case for Data Intensive Applications of Decentralized Identifiers

Wednesday 5F
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:

ReputationIIW2017.pdf
https://github.com/SmithSamuelM/Papers/tree/master/presentations

Distributed Token Validity API: How do we solve SSO true logout issues?

Wednesday 5G
Convener: David Waite
Notes-taker: Danielle Johnson

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

Detailed information can be found at the following links:

https://www.pingidentity.com/en/company/blog/2017/06/22/introducing_distributed_token_validity.html

https://github.com/pingidentity/dtva-reference

https://bitbucket.org/openid/connect/src/4dc66f0077597e08f9758379a87fb5f9be06359c/distributed-token-validity-api.txt?at=default&fileviewer=file-view-default

https://bitbucket.org/openid/connect/src/4dc66f0077597e08f9758379a87fb5f9be06359c/dtva-hashgraph-system.txt?at=default&fileviewer=file-view-default

Additional notes:

No single spec for logout currently works.

Frontend: redirect, iframe, cookies

- Possibility of not actually logging out, especially with multiple redirects

Admin logout

- Sessions can still exist if token life continues.
- There is no update check for a user who was fired and they may still have access

Backend

- REST APIs

SSO not typically integrated into each app, typically it is just a cookie used to try and tell them to logout

Logout typically refers to all applications access for SSO, not just you logging out of the current application

What does logout actually mean?

- What is the expectation when someone logs out?
- Trying to tell browser or app they need to be reauthenticated at the next access

OIDC session management spec

SSO/SAML focuses on logging in, but logout wasn't thought through

- Destroying the cookie
- Logout of browser
- Undoing all the work it just did to login

Login uses tokens

- So if logout instead removes validity of token, all access is removed and true logout exists by removal of accesses

Using tokens to update information

OIDC session management

- Html 5, POST message, javascript, etc
- Load page on IdP domain (PULL, web socket, etc), sends message on your app saying token is good or bad, if bad get a new token

Ex: Google will periodically require login credentials and will go across all tabs, but an API being used with that same Google account won't be effected by the "logout"

Single interface for users initiating logout or admin logging you out

This suggests using:

Frontend RESTful API

- Deployed individually by user still actively using the app or by a single IdP

Hashgraph

How is data synchronized?

Cross domain liveness check; is the user still actively using the app

Main focus is how to main overall experience more dynamic

- If a token is good for a week and someone is fired on day 4, how do you make token invalid?
    - Session change requires new token no matter what the token lifetime is

Changes or updates to policy, causing untrusted previously approved token to no longer appear valid

Blockchain idea can be used to require new token (through checking again previous data)

Hashgraph said IdP can actually create

Actual tokens aren't tracked; it leverages the Sessionid

Digital Identity of K-12

Wednesday 5H
Convener: Akiko ORITA
Notes-taker(s): Akiko ORITA

Tags for the session - technology discussed/ideas considered:

#education #privacy

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

After introducing the Internet usage by K-12 in Japan, we discussed followings;

1) How do they manage digital identities?
2) How do they learn about identity and privacy?
3) What can we do for them?

Comments;
- Do teens feel themselves safe or are they safe really?
- What "risky" means varies by generation. Resilience is important.
- We can't solve the problem at the level that created the problem.
- It is necessary to educate not only students but also teachers and parents. Kids are often more aware of online risk than teachers.
- Real-name policy in US must be considered.

Thursday October 19

Lost Identity – Post Disaster Recovery (Nor Cal Fire, Puerto Rico)

Thursday 1C
Convener: Mei Lin Fung
Notes-taker(s): John Philpin, Louis Rawlins, Mei Lin Fung

Tags for the session - technology discussed/ideas considered:

#PostDisasterIDRecovery #FinancialID #HealthID #EducationID #NOTFirstResponders #WildFireRelief

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

Mei Lin Setup

There is a great need to be able to verify individual identity while simultaneously safeguarding personal information. Recent events that highlight this problem include the Equifax data breach; the recent series of hurricanes in the Atlantic; and, closer to home, the wildfires in California.

To make matters worse, Californian's are at the top of the list in the US as most likely to experience Identify Theft according to a recent Wallethub report: https://wallethub.com/edu/states-where-identity-theft-and-fraud-are-worst/17549/#main-findings.

These situations have the potential to leave people without valid ID and with no access to their medications & medication lists for extended periods of time.

We are Individuals, Communities and Organizations that are networking together to promote change using technology as an enabler.

Call to action
If you are ready to help at this frontier where tech and reality meet, we can use your help. Please provide your information by following the link below and completing the on-line form and we will take it from there. https://beyondbridges.net/tvn/

Thank you in advance for your support!

Overview of Session : JP

A short rapid fire general discussion that included input from all

Focus was to achieve a broad consensus to approach that had already been kicked off outside of IIW

Photos of whiteboards and attendees can be found here :
https://www.dropbox.com/s/whe62ql2czwgaga/New%20Folder%20With%20Items.zip?dl=0

(it is a zip file – and potentially not helpful to the passing reader. Data will be extracted and summarized in a form more readily consumable and circulated to everyone we have an email for.)

Anyone can register their interest at www.beyondbridges.net/tvn or email john@people-first.net

Note – the Beyond Bridges page will disappear once our dedicated web site is AVAILABLE. At that point, the page at Beyond Bridges will be redirected to the full site.

We agreed that this was an initiative that should work to deliver immediate impact both here in California – in relation to the Wine Country Wild Fires and Puerto Rico.

Simultaneously preparing ourselves to solve real problems now – but laying a foundation for an approach when the next disaster occurs.

The Main Topic Silos Identified were …

Bio Metric
Safety
Social
Commercial
Cross Silo Activities
Integration
Recovery

We identified people who are interested in / can contribute to each of those areas which we will document separately.

As we moved forward, we will seek to deliver a transition plan that we can utilize to better prepare for the future.

First Pass Notes Details – MANY THANKS TO LOUIS FOR THE FOLLOWING … *(red Highlights below are specific people actions – this will grow in final documentation)*

NorCal Fire - Recovery of Artifacts

Facilitators
==========

Mei Lin Fung - mlf@alum.mit.edu - peoplecentered.net
John Philpin - people-first.net
Joe Andrew

Participants
==========
Joyca ~ John ~ Carlton ~ Sharon ~ Rick ~ Lubna ~ Adrian ~ Lara ~ Julian ~ Peter
Joe ~ Anne ~ Louis ~ Matthew ~ Lily Bragg ~ Brian ~ Jeff ~ Trey ~ Jonny

Ideas
=====
Functional Identity
Web of Trust --> Preponderance of Evidence
Patterns --> Ecosystem Map

Fraud
Priorities
- health
- education
- finance

Medical ID
Insurance
DMV
Post Office Mail Forwarding
Education
Phone
Email

Security Questions / Triangulation
- Email
- Cell Phone
- Fingerprints
- Birth Place / Data
- Ancestry / Community / Family
- Social Media
- Service Providers

Recovery of Identity --> Reestablishment of Correlation

Biometric | Safety / Health | Social Ties | Commercial Ties | Security | Integration | Recovery

Transition from each category to "demonstrate who I am"

Biometric
- Photo
- Magic Crypto

Safety / Health
- DMV
- Poor
- Very Poor
- Vulnerable

Social Ties
- Churches
- Premises
- Occupation
- Professional Associations
- Facebook
- Community Library

Commercial Ties
- FEMA Card
- Purchase History
- Public Utilities

- Carriers (Phone, Cable)
- Banks

Security
- Methods to:
- Dispute
- Appeal
- Revoke
- Claim

- Permission
- Withdraw
- Alert
- Delegate
- Who is representing?
- Pretending

Integration
- Cross-Siloes
- Legal Q & A for Legit / Illegitimate Claims
- Composite View
- Preponderance of Evidence (Jeff Arresty)

Recovery
- Wallet - Physical (Adrian Gropper)
- Voice
- Wault - Phone

Transition
- Education (Joe Andrieu)
- Citizens
- Organizations
- Private Sector

- Verifiable Claims (Matt Schutte)
- Connect Siloes (Matt Schutte)
- Expert Vetting of Solutions for Safety and Security

- Guardians of Identity (High-Trust Individuals)
- Recover Capability

Next Steps

John Philpin will circulate all notes, original images and conclusions to all attendees on the day that we already have emails for, plus others that we have already talked to and worked with on the same topic.

If you want to be included on this circulation – please email john@people-first.net

Images can be found here (link included in doc)

https://www.dropbox.com/s/whe62ql2czwgaga/New%20Folder%20With%20Items.zip?dl=0

Bringing It Together – DID + What We Already Have = How Do They Work Together

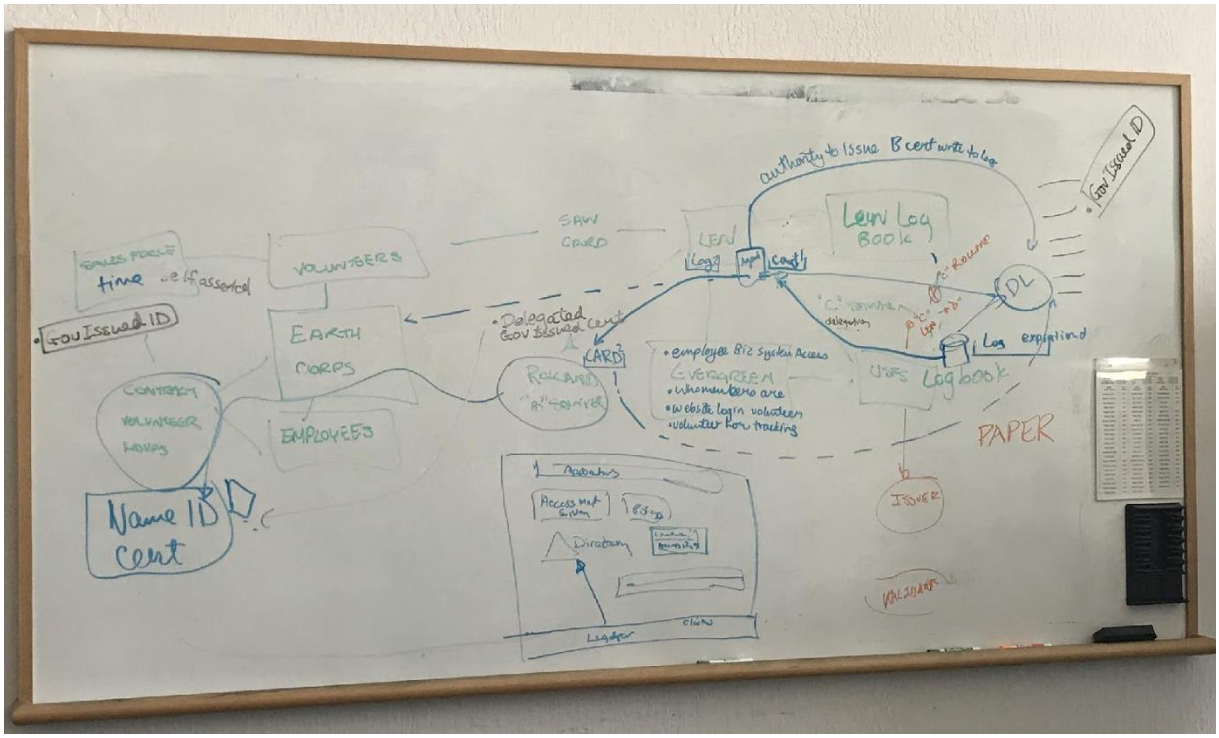
Thursday 1G
Convener: Susan David Carevic
Notes-taker(s): Susan David Carevic

Tags for the session - technology discussed/ideas considered:

DID, Blockchain, Identity Management System

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

The purpose of the session was to look at how decentralized identity components interoperate with or potentially replace components most organizations have in their internal identity management systems. The conversation took a different turn and focused on a sample use case of an agency providing a license to a user who that includes delegated authority to give lesser licenses to other people and seeing how that would play out with a decentralized identity system.



Autonomous Agents & Identity Delegation (JHV Research Project)

Thursday 1H
Convener: Maria Vachino
Notes-taker(s): Maria Vachino

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

Tags: #Agents , #IdentityDelegation , #Permissions , #IdentityManagement , #DID

Three students in the Master's program at the JHU Information Security Institute (https://isi.jhu.edu/) proposed a session to get feedback on their Thesis proposal:

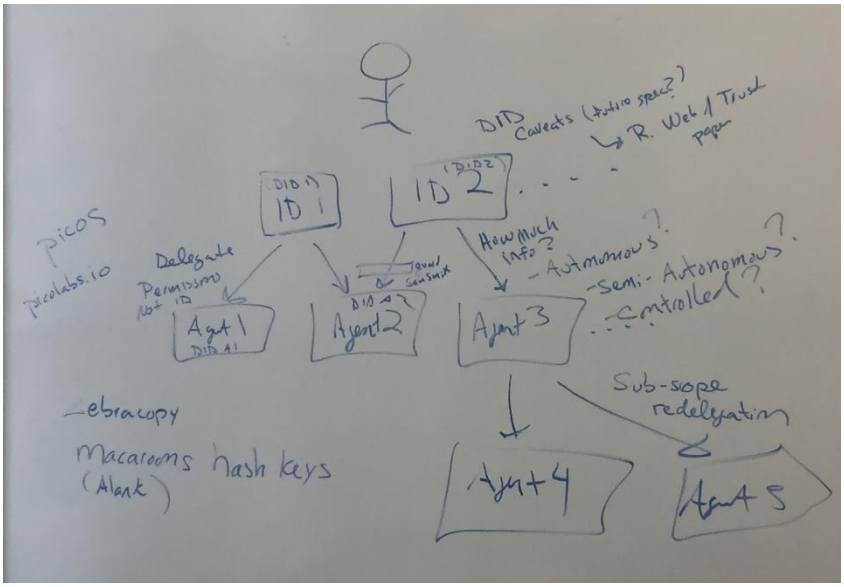
Autonomous agents and Identity Delegation

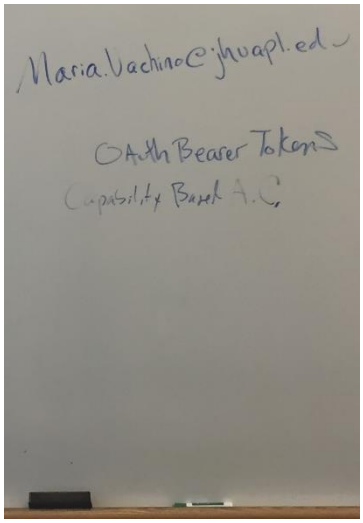
Our aim is to research and develop an identity management system that has identity delegation to agents, baked into it. We plan to make use of an underlying API that can be used to authenticate a person's agent to act on behalf of one of his many identities.

Additionally, we face the problem of controlling how much access of the human identity should be given to each agent. As each agent has a set of identities that are ultimately tied to a human being. Thus, we are focused to find a way to provide only a sliver of human identity without extra information leakage.

Students: Manan Wason, Ujjawal Sharma, Dewank Pant (Instructor: Seth Nielson)

Writeup:
https://drive.google.com/open?id=0B_luqCyRPBXjbl9oRF9zWkhhQzc1akFaUG5rWkd4RWRHWU5v





The GS1 Identity System

Thursday 2F
Convener: Paul Dietrich, Bill McBeath
Notes-taker(s): Paul Dietrich

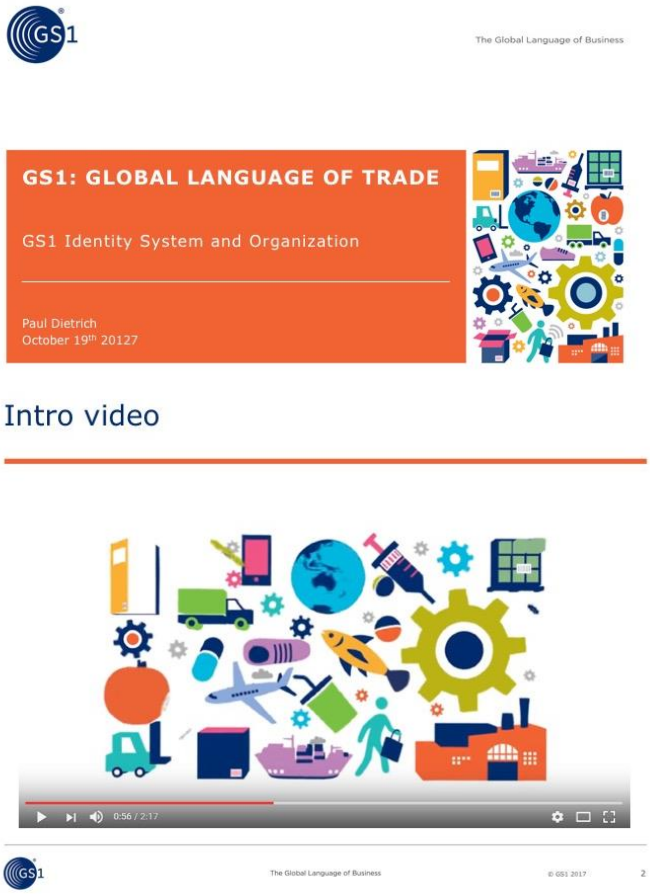
Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

Tags: GS1, Identity, Identifier
Approximately 12-15 attendees.

Discussion Notes: Paul and Bill presented overview material from the GS1 website http://www.gs1.org approximately in the order provided on website.

Slides were prepared and are attached to this note, but were not presented due to incompatibility between the computer and project (computer was USB-C and projector was HDMI)

They also talked about some real-life stories around identity and its evolution within GS1. Finally, the grouped discussed the ramifications of digital user and product identities in future trade systems.



GS1 – the global language of business

GS1 is a global standards organization

Neutral and not-for-profit

User-driven and governed

Global and local

Inclusive and collaborative

GS1 in numbers

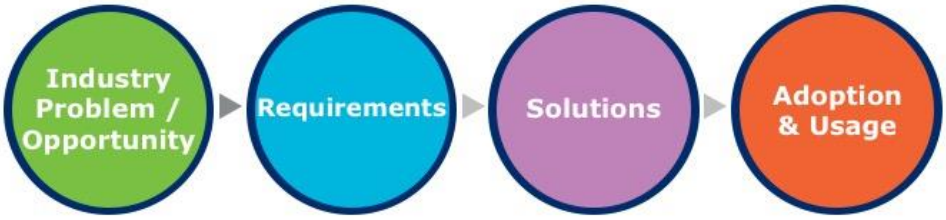
- **112 local GS1 Organizations**
- **1.5 million companies** use GS1 standards
- **> 100 million products** carry GS1 barcodes
- **6 billion GS1 barcodes** are scanned every day

Key industries served

Our Management Board:

Top business Executives represent the following companies from different sectors and all regions around the world

How we solve industry needs



GS1 creates communities of retailers and manufacturers and helps to identify a problem or opportunity and organize to solve it

GS1 helps industry define their needs/goals and create adoption plans

GS1 develops:

- **Standards**
- **Services**
- **Education & Training**

GS1 measures how industry adopts and uses standardized technology

GS1 Value Proposition

- **Using** GS1 Standards as a key component of business processes will deliver **lower costs and higher revenue for retailers and manufacturers**

- Some Key Benefits for Retail sector:
  - Point of Sales (Barcodes)
  - Master product Data Exchange (GDSN)
  - Order to Cash (EDI)
  - Inventory Management
  - eCommerce
  - Traceability

GS1 Portfolio

- **Global Standards**
  - Identification
  - Carriers (e.g. Bar Codes, Electronic Product Codes)
  - Sharing (e.g. Electronic Data Interchange)
- **Global Services**
  - Global Data Synchronization Network (GDSN)
  - Traceability

GS1 standards **identify products**

Logistic Label

00614141234567890

Serial Shipping Container Code (SSCC)

006141410000123452

Global Trade Item Number (GTIN)

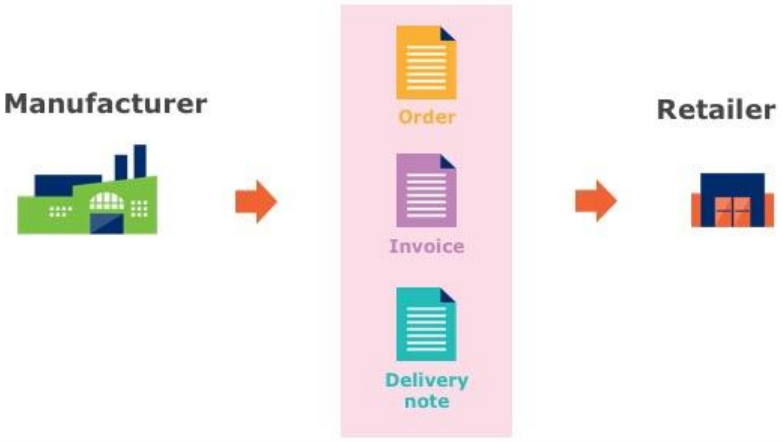
614141000036

GS1 standards **identify physical locations**

GS1 standards provide **carriers** to hold the identifiers

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

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



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

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

Master product data
- Brand
- Size
- Manufacturer
- Picture
- Ingredients
- Allergens
- ...

➢ **More than 40,000 companies exchange their product information via GDSN**

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

GS1 in the digital age: GS1 Standards and Services are extended to the **Digital world**

MANY THANKS!!!

The Global Language of Business
The Global Language of Trade

IndieWeb

Thursday 2G
Convener: Tom Brown
Notes Taker: Tom Brown

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

We went through an **Indieweb Wordpress Installation**. We installed the **Indieweb Plugin for Wordpress** and it guided us through installing plugins for **Webmention** and **Post Kinds**, for instance. **Doc Searls** posted **Digging Indieweb** on **Customer Commons** and we tested webmention and learned that under Settings/Discussion, there is a "Attempt to notify any blogs linked to from the article" setting that needs to be on. Thanks to **David Shanske** for the pointer. David created a **new github issue** to make it more obvious from the user interface during installation.

(this summary is also at: http://herestomwiththeweather.com/2017/10/19/indieweb-for-wordpress-at-iiw/)

Sovrin Ecosystem

Thursday 2H
Convener: Phil Windley
Notes-taker(s): Susan David Carevic

Tags for the session - technology discussed/ideas considered:
Sovrin Ecosystem, Verifiable Claims

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

Bank issues Alice a verifiable claim.
Alice shares a proof of her address with ATT based on verifiable claim
ATT and Bank do not need business relationship.
In the system, the Bank, Alice and ATT are Decentralized Identifiers (DIDs)

Verifiable claim contains information about who the bank is and who Alice is.
Identifiers are important to be able to track the proof to the right source

ATT needs to know something about the bank – they need to know a public identifier for the bank.
ATT knows the Banks DID for these types of credentials

Why does the bank need to issue the verifiable claim to Alice in the first place? If you are the bank, you have KYC data for Alice, why would they share it? Another bank could freeload off of that information.

- There is a bi-directional aspect to this work – if you are creating them, you want to accept them as well.
- ATT will want to know that there was a bank relationship.
- The arrows could go in the other direction as well. ATT's verifiable claim for Alice could be useful to the bank as well

Converted network effect to two sided network that can scale – typing point will be reached where two sided network will receive more value from single sided.

Rabbit hole discussion:

Know your customer (KYC) processes are very expensive – if the costs go down for this, entities will engage in more business.

In terms of an organization, how do you delegrate authority over an organization's agent? Delegation for Agents: Need to make sure that the agent can't impersonate you. Agent gives proof of credential and proof of authorization to provide it. Recipient needs to decide if that is good enough.

Mary (at the bank): acted fraudulently – bank needs to be able to revoke proof retroactively.

User can have two bank accounts and two accounts with ATT – User decides whether or not to correlate them.

Verifiable claims based on information contained in the ledger. Identifier for the claim definition for the schema in question (not using tech stack of certificates).

Back to discussion.. rabbit hole tabled:

ATT can only unlock proof if they pay for it. Bank ultimately get's paid for proof. Trying to create a system without correlation. Payment mechanism needs to be built into the lock. This is why we are exploring a token for Sovrin – so that we can have verifiable claims that are paid for by the identity owner, or the business needing the claim. (real world examples: transcripts)

Question from earlier session: ATT relies on the bank for my address, and they screwed it up. Maybe Alice put in a false address intentionally. Token could be used for insurance.

Privacy preserving value transfer is an important part of making system work. People will want to receive payment for providing a verifiable claim.

In order for the sovrin ecosystem to be an economy, any of the actors could be receiving and giving payment at the same time. Everyone should have an opportunity to participate in the economy. You don't want all of the tokens ending up with the same parties, and not getting dispersed.

Working with Imperial School of Economics to look at the "Tokenomics" of all of this.

ATT get's to choose what type of credentials they will accept. Business would have to decide what types of proofs they are willing to accept.

Is consideration being put in place so that people who can't afford services are not priced out of this service? Sovrin has an "Identity for All" counsel. They will delegate tokens for this purpose. Sovrin is sensitive to the idea of a tax, or denial of service due to not being able to pay.

For Etherium or Bitcoin there are built in transaction costs. What is the difference between this and sovrin:

Writing to the network looks free: we haven't put in a built-in transaction fee. Sovrin is on a public\permissioned network.

What is the advantage for a company to do KYC this way? For companies that don't have this, this might be easier. There are a lot of business bases where the integration for verification is too costly. This is also about giving another market for the data.

Premium claims: have a price tag on them.

Sovrin Governance:

Managing stewards on ledger
Agents: If I'm a person who wants to use Sovrin, I use an agent to store my information. And I need a connector to manage my keys and tell my agent what to do. The architecture for this is not dictated. Agents are specified and certified by Sovrin Foundation, but they are run by outside companies and we call them Agencies. (similar to browsers) Agencies are private companies that build somewhere and run services for people.
Apps: Applications of Sovrin. Most work through Agents and use these to interact with Sovrin.

What is your vision for the token: Great set up papers "Community Token Economies" envisions large community with players on top of stack that might have their own tokens and economies. It requires interoperability and we are building this into the Sovrin Token.

Are there other options for structuring incentives? Sovereignty is a border – not 100% control. Alice has control over some things. Alice decides what claims she takes and what she sends over. In the physical world, you don't get to decide all the things people say to you. She can choose what she should share. It is possible for incentives to be structured, where Alice get's paid for her claims.

Another example: location claim as a transaction is taking place, so that the bank has additional information to prove who the customer is.

Alice wants to protect her money at Bank A – she might want to validate her location at the Bank and not receive it from ATT – are we excluding Alice from the system? No – just from the example.
The business process is up to people, not Sovrin – Sovrin is just an Ecosystem that supports the process.

Intuition (Part 2)

Thursday 2K
Convener: Sharon Franquemont
Notes-taker(s): Sharon Franquemont

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

Intuition: Definition, Intueri Latin for *to know all at once*.

Discussion 1.

- Use of intuition as a noun or thing to know, almost no use of the active verb intuit, so intuition becomes a thing to know rather than an action to live.
- Intuition, adding a field identity to an ego identity (the w**I**e…the I ad a simultaneous we)

Discussion 2. Review: Patanjali's question thousands of years ago: *How does anyone know anything?*
His answer: 4 Stages of Knowing.

1. **Physical knowledge**: (Data)
2. **Associative knowledge** (Information—relational)
3. **Meaning knowledge:** intention and purpose
4. **Unity knowledge,** oneness between knower and know

Discussion 3. Practices to enhance intuition

A. Review Western views of how wisdom arises.
Greek: Athena, Goddess of Wisdom, *male and intellect*
Roman: Sophia, Goddess of Wisdom, *female and silence.*
Practice: practice silence

B. See body as an information field. *What impact does the body as information filed have on identity?*

Discussion 4. Intuitive Skills or Awareness Levels (first 3 levels familiar)

1. Instinct (Body based)
2. Psychic and/or Psi Skills (Emotion based)
3. Great Ah Ha! (Creativity based)
4. System (Pattern based)
5. Visionary (Future informed based)
6. Collaborative (Team or group based, local or non-local)
7. Unitary (Oneness with knowledge)

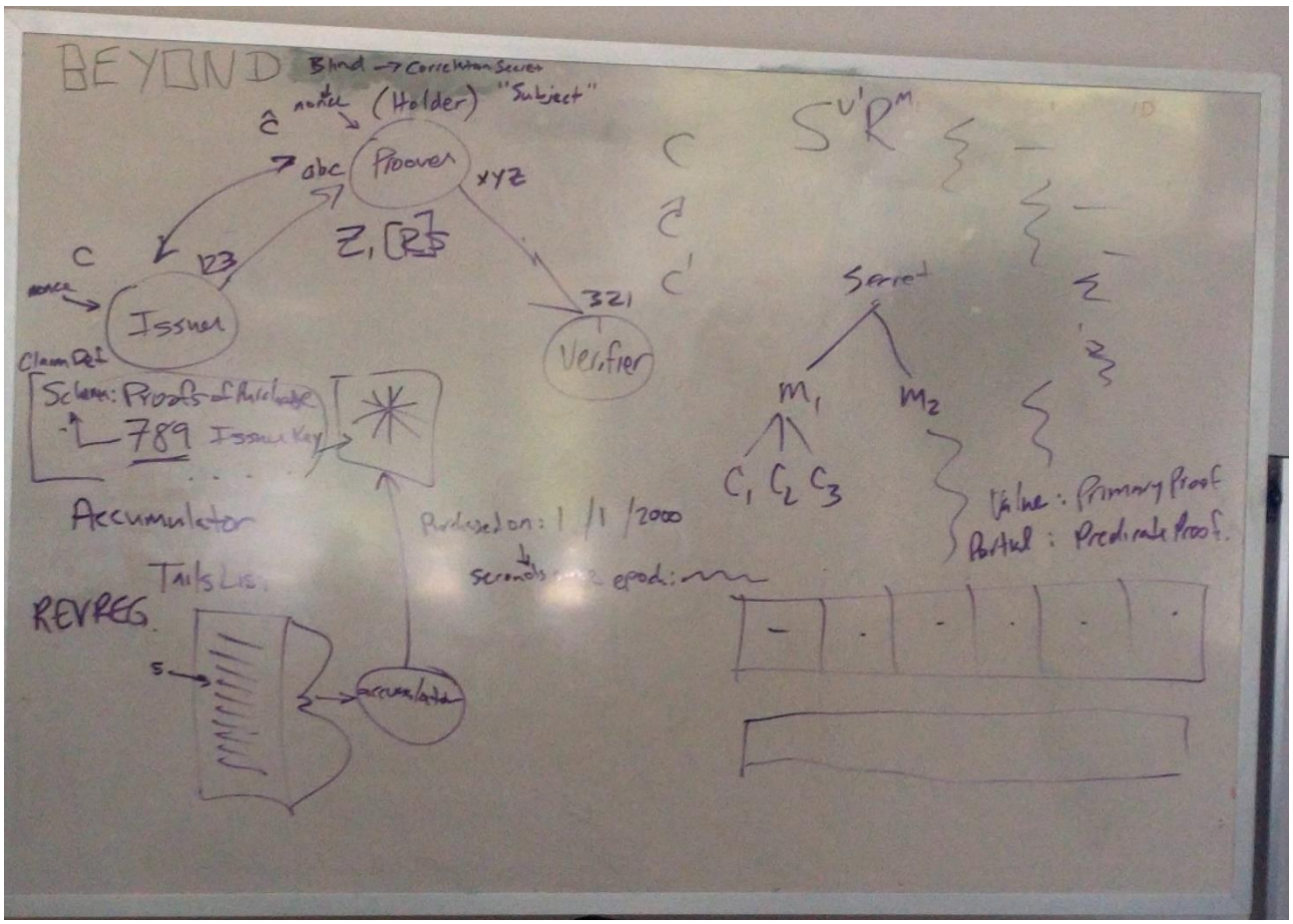
Discussion 5. Time Flexibility, Response Bias, IONS Research on future's influence on presence. PLAY with…

1. Molasses Time….experience slow motion time
2. Future….Circle and the Dot

Signatures and Selective Disclosure (show me the math)

Thursday 3C
Convener: Nathan
Notes-taker(s): John Callahan

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



Accountability vs. Safety in Permissioned Voting and/or Decision Systems

Thursday 3F
Convener: Dave Sandford
Notes-taker(s): Dave Sandford

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

We discussed identity and how a legal name or even long standing pseudonym can provide a reputation history and accountability for deliberations within a decision support system. Exposing legal names and valued pseudonyms can also allow attacks and reduce safety. Assumes a system which ensures participants are vetted and cannot use more than one pseudonym.

A concentric circle permissioned decision model was discussed where all participants are vetted - and can interact as:
- anonymous vetted (anonymous to other participants but vetted as a valid participant, could be implemented via ring signatures, or other means)
- psedonymous
- legal name

A concentric circle model was discussed where:

Outer circle - Purpose: discussion, Constraint: all participants can be anonymous vetted
Next inner circle - Purpose: voting or other human consensus process, Constraint: participant would have to identify themselves with their 'vote' at least pseudonmously
Innermost circle - Purpose: roles related to maintaining the decision making system process, Constraint: participant would have to identify by legal name

There might be an amount of time to be able to build the reputation to move from outer to inner circles. The intent would be to minimize barrier of entry to outer circle, and at each level balancing the cost of entry with the cost of safety.

What Should Large NGOs Be Doing to Help? What Role Should We Play in This Ecosystem?

Thursday 3G
Convener: Susan David Carevic
Notes-taker(s): Susan David Carevic

Tags for the session - technology discussed/ideas considered: Advocacy, NGOs

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

The purpose of the session was to hear and discuss with participants how an organization such as the World Bank can support technology development and projects that support sustainable development goals, such as providing people who don't have an identity with one.

We discussed systemic banking problems: remittances, and underserved populations where there is a lack of banking infrastructure. Gates Foundation set up a POS to provide services in one of these locations and it was a game changer for the community.

Actions that can be taken and would be helpful:

- Conditional funding: insist that projects utilize standards or principles when procuring systems
- Being vocal and public about support for technologies – adds legitimacy for technologies and solutions
- Becoming a steward, member or trustee of initiatives
- Funding for projects in non-profit sector to put infrastructure in place – Global Public Utilities.
- Working together with industry standards organizations
- Help attract more organizations to participate\convening power
- An Internet of Things council was been newly formed – participation\collaboration with these organizations.
- World Bank to recognize personal data as an asset: the idea that personal data can be the basis for a living wage. We are all producers of data, we are all data providers and should be rewarded for our data.

Recommendation for NGOs to view solutions to problems through the lens of the following 4 pillars:
- Tech
- Economic
- Legal
- Moral/Ethical

Call to add one more: Culture\location

Comment made that it would be interesting to try to create a document showing how a technology could evolve and when that might happen – something like a roadmap on the impact of disruptive technology.

The reality of this technology is actually here – however not all pillars are ready – legal\regulation is behind.

NGOs should serve as guardians & keepers of equity. Can't forget edge cases: can't exclude and they need to think about unintended consequences.

As we think about economic models: people take on externalities of Equifax: people end up with the risk.

The World Bank has up to date and good data on currencies\indexes. Would be interesting and could really shine some light on problems, if they also published asymmetric data flows – for example on remittances and other types of information. Would be interesting to see where there are unequal exchanges of information – look at information debt the same way we look at currencies.

The conversation morphed...some interesting points made:

- In 2010 we moved from a causation society to one of correlation
- AI driven world: informed consent could become illegal. People could receive immediate compensation of costs incurred.
- GDPR: on docket now in California
- GDPR will open up more data than close it down.
- We should learn more about CCN: Content Centric Network: Cisco just bought the patent for this.

DKMS – Key Recovery Summit: Biometric Recovery, Cold Storage, Social Recovery

Thursday 4A
Convener: Drummond, Jack, Kent
Notes-taker(s): Lily Bragg

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

Distributed Key Management System (DKMS)

DHS – Science and Tech division – phase one SBIR on DID, phase two is working on DKMS. Goal is an open standard. Key Management Interoperability Protocol – KMIP is an existing standard for vendors to manage keys in an enterprise. We need the equivalent for decentralized key management. Should meet the best practice and requirements. 800-130 Framework for designing cryptographic key management systems, we think that is the best. We are about 6 months into it. BYU Internet Security Research Lab specialized in usability. Ken ___ from BYU. Yearlong project in 4 phases 1) Analyze requirement – going through 800130 – 230+ requirements that any key management system must meet to sell to US gov. agency. We analyzed all those and how they will apply to decentralized. About 60% of the requirements are exactly the same. Another 36% needed to be modified. Only 4% we said do not apply. We identified 12 additional requirements. Summary of all of that was published a couple weeks ago.

Phase 2, we are designing an architecture for decentralized key management. The big hard problem is key recovery. There is no central authority to go to in order to get a new key. With Ken and his lab, we said probably the hardest part is usability. How will it actually work. We all learned how to manage passwords (kind of) … will now have to learn how to manage keys.

This session will be 1) a survey, 2) one option – 'cold storage', where someone keeps it, 3) another option biometric option being worked on, and 4) key recovery. We want to focus on usability.

Jack Callahan, CTO, Veridium

IBV – initial biometric vector – your fingerprint, voiceprint, etc.

BOPS2 – Biometric Open Protocol Standard IEE 2410 – covers collection, storage, etc. Today talking about modes and shares. Local mode – the IBV is split (I think sharded) into two or more 'shares', both resident on a mobile device. Like FIDO UAF. BOPS uses the IBV to generate a private key, using a TPM if its available on that device. FIDO is adamant that the private keys are only on the local device. BOPS is a super set, it also has remove configuration, though controversial, some customers want it. Your CBV (?Current? biometric vector) is sent across for checking remotely. BOPS does not prescribe which one to use. You can also split it with a shard locally and another shard on server – then bring it across and check it locally or remotely.

So, now the thought is, what if the shard is given to a friend, instead of another institution. Could put these shares on a blockchain. Now how to coalesce – might use ring signatures? (RingCT),

So, when someone comes with just a biometric, how do I discover the list of who might have the shares?

Still a lot of unanswered questions – usability, security. These live in our phones right now. Right now ___?New Mexico? doing server side matching for KYC.

Drummond – general architecture. Diagram with DIDs on blockchain on bottom – talking to cloud agent/wallet, connected to edge agent/wallet.

Biometrics will be entered at edge, but IBV can be stored at edge or cloud. The edge device is where the human physically interfaces.

One point, IoT devices may have some biometrics, that could be used as a 'fog' of devices that can do a face recognition, or fingerprint for authenticating you. But If your house burns down, those are gone. IoT manufacturers will often choose the cheapest chip. However, there is a spectrum of devices, just need sufficient density of devices with those that can ID you.

Key Ring = set of keys on one device. With Apple iCloud, potentially can be shared.

Trust Ring = Set of agents participating in key/credential backup and recovery.

Key expiration is important, for many use cases. But some keys I want to last a very long time.

Still need to test the concept of trust rings with individuals. Will people get the concept? Is it a common concept – or can there be a universal set of ways to do things.

Discussion on naming, maybe a Trust Ring should be called a Recovery Group.

Possibility for the group to be arbitrarily open ended.

Very little research and literature on decentralized key management.

The Human O/S Defending Privacy by Understanding I.T. Forces and Managing Human Nature

Thursday 4F
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:

Defending The Human Operating System: Intention/Identity Through Understanding I.T. Forces And Its Impact On Human Nature

There is a YouTube companion audio/video https://youtu.be/VECmh2rpt70 with full from all attendees and an active whiteboard reference throughout. It is much more encompassing than these rough outline notes. I hope this works out well and please pardon my apparent spate of "Valley Girl" linguistics as I used the word "like" about 700 times in the first minutes. I beg your pardon!

New Awareness\Language: Real-IT

Real-IT• is the relationship we choose to have, or not have, with Information Technologies (IT)

Newton & the Apple: What's with that apple falling? Why does it fall down, not up, much less at all? Gravity He put handles on thoughts with words allowing us to be able to discuss the idea and build understanding.

Props to the stage crew / Setting the stage:

Newton (again) – "If I have seen further than others, it is by standing upon the shoulders of giants." Nearly everyone I serve and learn from is my giant. Benefitting from those gifts I present this discussion.

Brene Brown: - "Maybe stories are just data with a soul." I share data and what I have learned often by story telling.

Daniel Pearl – Died at the hands of the terrorists, February 1st, 2002 – (Refer to audio)

The Human Animal As A Sensor \ Awareness Package

Baseline Human Capability:

- Visual was line of sight
- Audible what you could hear from where you stood.

Our sensor range \ awareness was gradually extended by messengers, then radio waves, to television, and currently I.T. Seen on the horizon, and a Superset of I.T. we have Virtual Reality (VR). While this evolution in awareness has been mostly great, it may be a bit, to a lot, too much. (refer to audio)

When do, each of us being different, we overload ? What behavioral elements are challenged? The outline below is very generalized. Maybe Middle C on the keyboard with variations of itself in either direction.

Impulse : how can we block the chain of I.T. systems and science gaming our impulse at new and ferice levels? vs. Consideration: How can we build a chain of thoughtful decision making by owning understanding of the exploits embedded in these I.T. forces?

FOMO! (typically a challenge to youth) Costs? (typically a concern of elders)

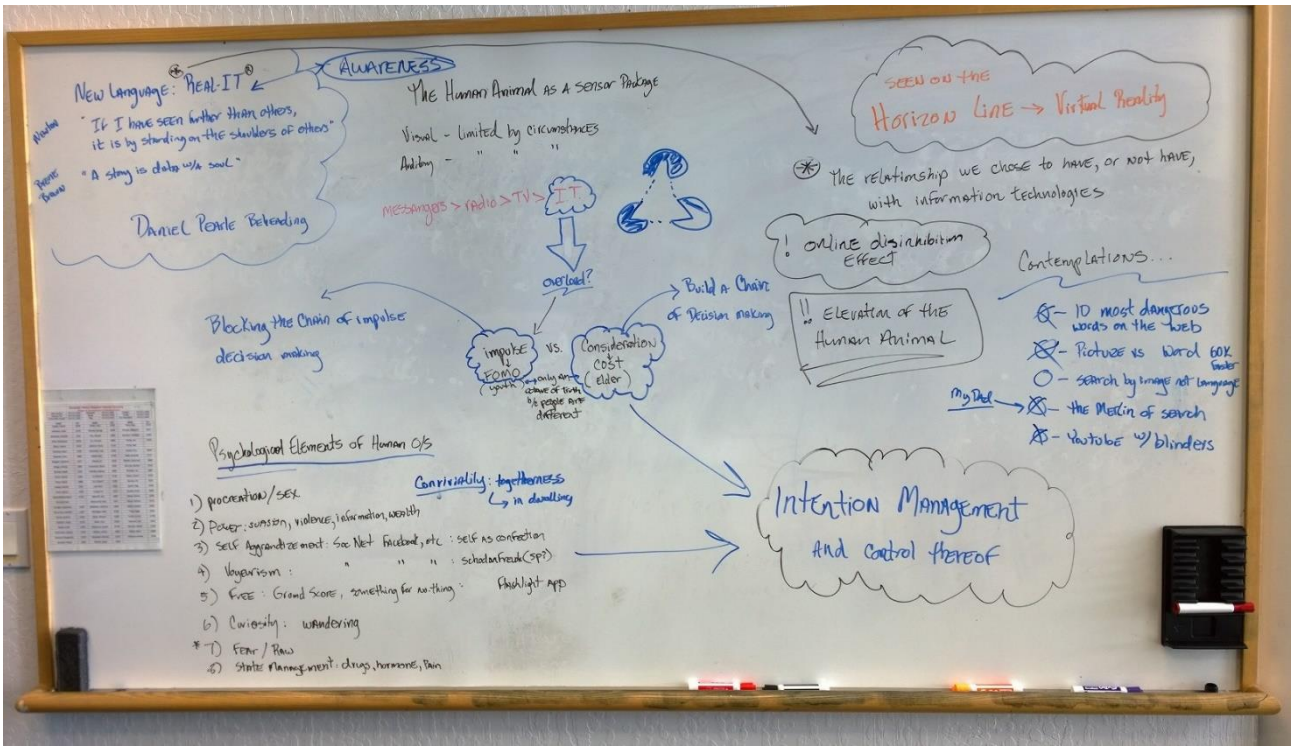
Psychological Elements of the Human O/S that will be susceptible to influence. (The Art of Intention Management and Control Thereof)

As animals we are compelled to pursue certain impulses that are very baked into our core nature. Each of us being different are affected by the following impulses by different degrees.

1. The drive to procreate: sex – porn, or pairing SocNet: Tinder, etc.
2. Power: information, violence, information, wealth
3. Self Social-Aggrandizement: Social Networking (SocNet) Facebook, etc. - Presenting ourselves as "a confection" [credit Gladwell & Victoria ??? presentation]
4. Voyeurism: Social Networking (SocNet) Facebook, etc. – schadenfreude
5. Free: Ground Score – something for nothing, caveman finds a nut (the flashlight app)
6. Curiosity: wandering
7. Fear: either a search for alteration in state of mind via endorphin stimulating viewing, pairing via SocNet, drug acquisition
8. Conviviality: search for togetherness and belonging (SocNet…AGAIN), in dwelling (per Doc Searles)

Extras / Contemplations

10 Most Dangerous Words on the Web
The Merlin of Search
Global Graphic Based Search vs. Multilingual Challenges of the Managing International Translation
Text vs. Image



Reputation II – Data Intensive Applications Using DID's

Thursday 5F
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:

https://github.com/SmithSamuelM/Papers/tree/master/presentations

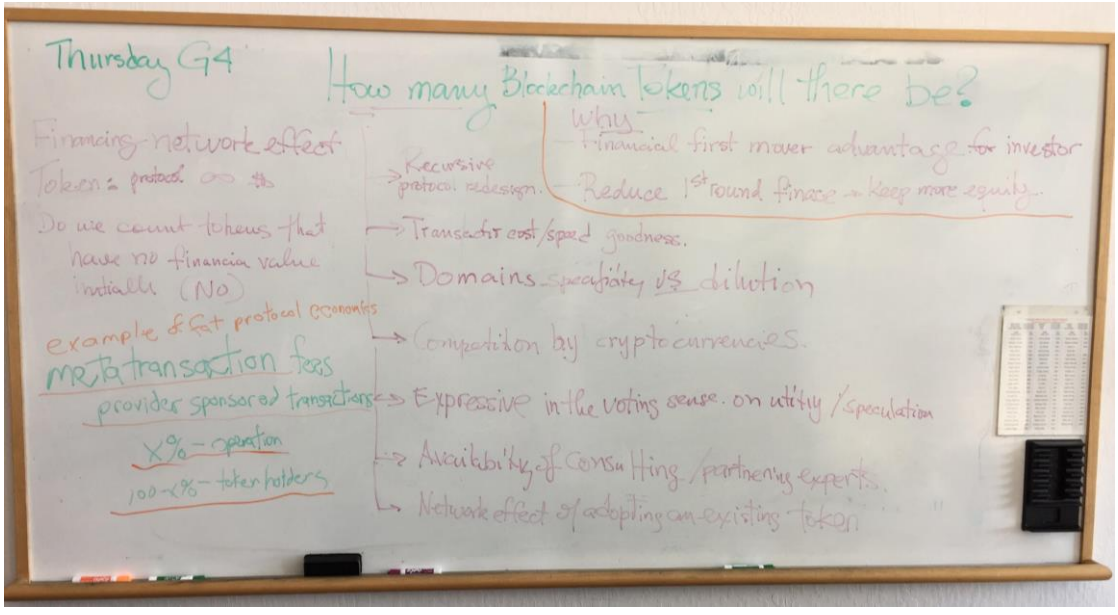
How Many Blockchain Tokens Will There Be?

Thursday 5G
Convener: Adrian Gropper
Notes-taker(s): Marsali

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

How many blockchain tokens will there be?
Why: Financial first mover advantage for investor
Reduce 1st round finance – keep more equity

Explore and evaluate the following:
1. Transfer cost / speed goodness.
2. Specificity vs dilution
3. Competition for and by cryptocurrencies
4. Expressive in the voting sense on utility/speculation
5. Availability of consulting partnering experts e.g. Partnering with ID token being offered by others



Thank You to All the Fabulous Notes-takers!

There were 97 sessions called and held. We received notes and/or white board shots for 68 of these sessions.

All notes are also posted to the IIW Wiki here: http://iiw.idcommons.net/IIW_25_Session_Notes

Simone loves it when you get your notes in!

Photo Credit
Julian Ranger @rangeri Oct 19
Simone at #IIW with a digi.me stickered MacBook - @spoutnikx say it's "the world, more beautiful with digi.me" !!!

Demo Hour

IIWXXV #25 Community Sharing / DEMO LIST
Wednesday October 18, 2017

Thanks to our Demo Hour Sponsor

1. **Gluu demo of Kong API Gateway with UMA Plugin: Mike Schwartz**
   URL: Kong: http://getkong.org Plugin: http://gluu.co/kong-uma
   Kong is a popular open source API gateway. Gluu has written a plugin to enable Kong to act as a compliant UMA Resource Server, enabling you to centralized policy management. Gluu has also written a web GUI that make it easy to configure the Kong plugin. Mike will provide a quick overview and a demo of Kong and UMA in action.

2. **Danube Tech - DIF Universal Resolver and Registrar:** Markus Sabadello
   URL: https://danubetech.com/ and http://identity.foundation/
   The Universal Resolver can resolve DIDs and other identifiers in a uniform way, so that Verifiable Claims as well as RDF and XDI protocols can be built on top of identifiers registered in any blockchain or by other means. A counterpart - the Universal Registrar - is also available.

3. **A Personal Digital WAULT:** Katherine Kern and Liwen Yaacoby
   URL: Https://Wault.tech and https://wymsical.com
   WAULT is a 3 way cybersecurity member network. Trusted Institutions who care about privacy authenticate WAULT Owners for $35/annually. Owners privately protect and share their vital documents on the WAULT network app. Third parties view & verify on the app, without leaving a trace.

4. **TheOrgBook Project - A Verified Organization Public Claims Repo:** John Jordan, Stephen Curran, The Government of British Columbia
   URL: https://bcgov.github.io/TheOrgBook
   TheOrgbook (a play on TheFacebook) is a repository of public claims issued by a government entity about a Verified Organization that can be used as is by other Services, and we hope will accelerate Organizations creating their on self-sovereign identity to "claim their Claims".

5. **HIE of One:** Adrian Gropper, MD
   URL: http://hieofone.org
   HIE of One demos self-sovereign tech as a patient-controlled independent health record. A personal UMA authorization server uses the doctor's self-hosted verifiable claims via self-sovereign uPort blockchain ID. No institution or federation mediates between doctor and patient.

6. **digi.me –current PC/Mac, iOS/Android version application:** Jim Pasquale & Julian Ranger
   URL: http://digi.me for product & http://digi.me/video for vision
   Demo will show what users can do when they own and are in the driver's seat of their own data on their own devices(s). More privacy through our new Consent Access feature, using two new external apps providing social analytics and monetary insight from financial data inside their library.

7. **City of Osmio VRD Enrollment Process:** Mike Maturo
   URL: http://osmio.ch/
   The City of Osmio is the identity certification authority for the Authenticity PKI. As with the city where you live, Osmio is owned and governed by its residents. Its certificates may back other credentials. Enrollments to be demonstrated.

8. **Deutsche Telekom Laboratories - managing credentials instead of identities: Jörg Heuer**
   URL: It's not a product (yet),information can only be provided upon request from joerg.heuer@telekom.de
   Identity is a concept hard to explain to users. Our prototype implements familiar credential types to ease implementation of typical identity, authentication and entitlement cases with one harmonized usage pattern. It embraces legacy, user-centric - and potentially - blockchain technology on several levels.

9. **Digi.me demo: Tarik Kurspahic**
   URL: http://digi.me for product & http://digi.me/video for vision
   Do more, privately – digi.me enables individuals to own their whole digital life (e.g. social, health, finance) & do more themselves, sharing, privately, with apps & web services opening data silos and democratizing data – it's real today

10. **Only Mobile Phone Number Card: Suhee Park**
    No URL: Come to the Demo to see an example of the card
    Physical Card on which your only mobile phone number is embossed, interlocking with your smartphone for verification. It's more than payment. It's for public & private and sharing services across borders, covering key cards as well for access and tickets. So, it could be used as a way of identifying yourself with fingerprint on your smartphone.

11. **FIDO & Mozilla – FIDO Needs Browsers! :** Yubico John Fontana & Chris Streeks
    URL: https://www.yubico.com/products/yubikey-hardware
    You've heard this before, but now it's here! See FIDO U2F working in Firefox (Nightly, Beta, Developer builds). We'll show it (simple demo) and talk with you about hardware-backed keys, why FIDO U2F, and strong authentication.

The IIWXXIII Demo List can also be found here
http://iiw.idcommons.net/IIW_25_Demo%27s

IIWXXV #25 Photos

Photo's in this document were posted on Twitter and taken by Doc Searls
Credit given at each image ~

IIW Co-founder Doc Searls always creates a wonderful candid capture of the faces and energy and spirit of IIW. You may see them all at the link below!

Links to Doc's Photo's IIW25 Day 1 – 3
https://www.flickr.com/photos/docsearls/albums/72157665717723489

See you April 3, 4 & 5 2018

for IIWXXI

The 26th Internet Identity Workshop!
Endorsed by History
www.InternetIdentityWorkshop.com