IIWXXIII

INTERNET IDENTITY WORKSHOP 23

OCTOBER 25, 26 & 27 2016

Book of Proceedings

www.internetidentityworkshop.com

Collected & Compiled by
MILLICENT BOGERT, HEIDI N SAUL AND JACOB WINDLEY

Notes in this book can also be found online at
http://iiw.idcommons.net/IIW_23_Notes

Photo credit #IIW @Nobantu

Next IIW is May 2,3 & 4 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

Contents

Photo credit #IIW @identitymink

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.

To read descriptions of 'what IIW is' as articulated by attendees of the 11th event held in November 2010, you can go here: http://www.internetidentityworkshop.com/what-is-iiw/

The event is now in its 11th year and is Co-produced by Kaliya Hamlin, Phil Windley and Heidi Nobantu Saul. IIWXXI (#24) will be May 2 -4, 2017 in Mountain View, California at the Computer History Museum.

IIWXXIII Sponsors

Photo credit #IIW @JBFintech

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:

IIWXXIV #24 May 2, 3 & 4, 2017

IIWXXV #25 Oct 17, 18 & 19, 2017

Identity Films @ IIW

The Identity films produced at IIW #22 by Heather Schlagle @heathervescent, premiered at the start of IIW #23. Below are links to several of them.

What is IIW?

The Internet Identity Workshop just completed its 12th year and 23rd event. This is a short film of regular attendees describing it: https://vimeo.com/173562225

User Managed Access (UMA)

What is the User-Managed Access (UMA) standard? What's it good for? Is it ready to use now? What do "UMAnitarians" believe is important?

Learn the answers in two minutes flat! http://tinyurl.com/umamovie

OpenID Connect - "The Foundation of Identity"

This film reinforces the ideas that the foundation of internet identity is a collaborative and ongoing endeavor.

OpenID Connect is as example of the kind of collaboration born at the IIW and necessary for the adoption of a "foundational" standard like OpenID Connect. The film is featured at OpenID Foundation website: http://openid.net/

Internet Identity Workshop – The Identity Documentary Film

The first cut of the film was shown and it is now in the process of being completed, taking in feedback from the viewing. We expect it to be complete by IIW #24.

Photo credit #IIW @JamieXML

IIW 23 Session Topics / Agenda Creation

Photo credit #IIW @JamieXML

Tuesday Oct 25, 2016

Session 1
1A/ PDEC (Personal Data Ecosystem Consortium) Update
1B/ “Correlation” TA.F.K.A. “Idenitity”
1C/ Intro to Verifiable Claims
1E/ The End-to-End Decentralized Identity Platform – What is looks like, how we can achieve it.
1F/ The Blue Button Experience
1G/ Introduction to OAuth2 (101)
1H/ The Four Kinds of Privacy – Defensive – Human Rights – Personal - Contextual

Session 2
2A/ ONTY A new communication platform based on private sharing
2B/ UX Hacking the Personal Data Dashboard
2C/ ACCOUNT CHOOSER to RE-charter
2E/ Data Portability/Data Interop – How do we get this done? With Whom? What’s come before? What’s stopping this? Consortium?
2F/ Personal Data Stores in the Enterprise (collaboration and ownership)
2G/ INTRO: Open ID Connect (101)
2H /Remote Identity Proofing
2I/ Kantara Incubator – R&D $ < $1M Re-run of April ++

Session 3

3A/ JLINC 101 for Alice and Bob Co
3B/Personal API's – Scope of and where we are now
3C/ Financial Data $ Aggregation and Sovereign Identity
3E/ Your (1st party) Terms that companies agree to
3F/ A Discussion of Military Identity use cases
3G/ Defining the Sphere of Privacy
3I/Smart Contracts for Self-Sovereign Data Usage
3J/Project Ipseity (Latin word for 'selfhood') –A correlation model for digital identity, given user ownership & control of personal data

Session 4

4A/FAST FED – OpenID Foundation Working Group and How to "identity enable a cloud business service in 30 min.
4B/Self-sovereign Identity Container DEEP DIVE
4C/Help me "help" my professor…
4E/What is SOVRIN?
4G/INTRO (101) User Managed Access /UMA
4I/Signed Biometric Storage + Transport Specification
4J/Literature Review for Personal Data, Personal Info Economy

Session 5

5A/Security Events 101 – Distributed Architecture Evolution
5E/Foundations of Privacy – Respecting Identity in Sovrin
5F/Self-Sovereign Support Technology (DID – Mobile – Bots -…)
5G/Principles of Self-Sovereign Identity
5I/Self-Sovereign Identity for KIDS (onboarding the next generation to the web we want)
5K/Standards and their use for IoT/Riding the crest of DDoS Event

Wednesday Oct 26, 2016

Session 1

1A/ SMS for 2-Factor Authentication: Secure Enough?
1B/ Tutorial PBFT In Depth What's the "f" in BFT
1C/ DID spec Decentralized Identifiers (the secret ingredient powering Self-Sovereign ID) Intro and work on Working Draft 05
1F/ Well Fargo: Never Again (?)
1G/ Ways to use the IIW Films

Session 2

2A/Healthcare & ID unconference?
2B/Why Distributed Ledgers for Self-Sovereign Identity? How Sovrin Works
2C/ MFA 3.0
2F/An Association for Identity Professionals
2G/Identity Verification Flows and Machine Learning in Fintech
2I/Payments – Ne2B BillPay & P2P CP and CNP – Self Sovereign Identity

Session 3

3A/Security Events Distribution
3B/Student Profiles & Virtual Universities
3C/Verifiable Claims Deep Dive
3F/Blockchain Family Value – re:Trust
3G/My Data Technology Stack '101' Realizing the White Paper in Code
3H/Building a Secure Consumer Fintech Service from Scratch

Session 4
4A/FAST FED Part II
4B/Interactive Session on 'applying' Decentralized ID's and Idenitity Containers to real use cases
4C/ONTY.com Connect Via Private Share
4D/Life Cycle for People's Online Identities
4E/Consent Receipts – Crossing the Finish Line
4F/Self-Sovereign Identity – What's Different?
4G/PicoLabs
4H/OTTO = Open Trust Taxonomy for Federation Operators
4I/Ecosystem Maps – What's happening in standards bodies.
4J/Identity Breeder Documents - Claiming Yours

Session 5
5A/Reputation Algorithms and Scoring for Curating Sefl-Sovereign Data
5B/Personal API Implementation using AWS
5C/XDI Update – 2 Demo's
5E/Access Control & Data Rights for the Industrial Internet
5G/Identity in Physics – What can we learn?
5H/OIDC Identity Federations
5I/Team Data Demo – personal data store
5J/Identity Without the Individual – Institutional Authorization in Publishing

Thursday Oct 27, 2016

Session 1
1E/Introduction to OAuth2 – 101 second offering
1F/Design of a Scalable Service Broker
1G/"Federated" / Decentralized Social Web – What happened? Can it happen?
1I/Verifiable Claims Intro – Problem Statement Goals

Session 2
2A/Identity Container Wars! Plah JSON vs RDF vs XDI
2E/#No Stalking: 'Just give me ads not based on tracking me'
2F/Identity in the Elevator – Brainstorm 15 second explorations for IIW jargon for lay people
2I/ Verifiable Claims - Use Cases

Session 3
3A/Market-Facing Terminology Harmonization
3E/ Sophisticated Ledgers and Smart Contracts – Are the useful?
3F/From DB to PDS: Blessing data about you with your identity preserve Privacy
3G/ ID correlation (no $) startup architecture & business model
3I/ Verifiable Claims – Use Cases Deep Dive

Session 4 / Working Lunch
4A/Sovrin Trust Framework
4E/Self-Sovereign Technology Stack
4G/ Time and Identity in Physics
4I/Verifiable Cliams – Architecture and Goals

Session 5
4A/ Burn It Down and Start Over
4E/ Biometric Recovery of Self-Sovereign Identity
4G/Will Smart Contracts Drive Civilization Over a Cliff?
4I/ Verifiable Claims Data Model & Representation

Tuesday October 25

PDEC Update

Tuesday 1A
Convener: Dean Landsman
Notes-taker(s): Dean Landsman

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

Rather than a crowd assembling at the start and sitting through a presentation and then doing a Q & A or having a spirited discussion, this time we had the fortuitous result (perhaps of being in far away Room A, with its projector) of attendees trickling in and out. This enabled us to have one-on-one or two-on-one sessions with members or prospective members, and to focus on their questions or insights, and to delve deeply into their areas of interest.

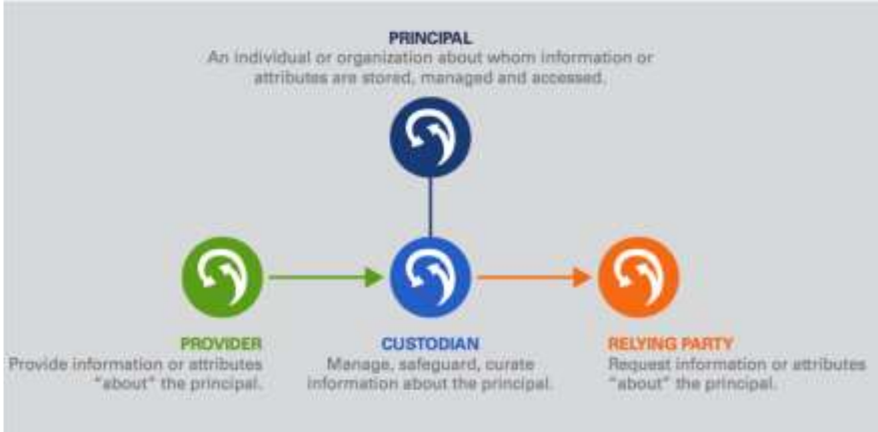
We showed the most current PDEC slide deck to all who came by, and also at other times during the conference Key points and a graphic from the deck:
PDEC Principles:

Empower individuals [aka principals] to control their personal information on their terms

Empower organizations [aka providers, custodians, relying parties] to enter into an exchange of personal information on an individual's terms

Support open personal information frameworks, standards and best practices

Support new business model evolution


PRINCIPAL
An individual or organization about whom information or attributes are stored, managed and accessed.
PROVIDER
Provide information or attributes "about" the principal.
CUSTODIAN
Manage, safeguard, curate information about the principal.
RELYING PARTY
Request information or attributes "about" the principal.

An additional note: PDEC was proud to announce at this IIW that we have signed alliance agreement with Kantara and OIX (and we do mean at this IIW23, where the signings took place), as we are separate organizations with separate agendae but many Venn diagram-like concerns in common. Our overall goals for personal data and identity and standards and practices are in alignment. Our statement(s) of alliance puts that at the forefront and sends the message to our members and to our communities, and to the enterprise, that we are working together to bring about positive change and opportunity via standards and practices applicable to commerce and the personal data ecosystem at large.

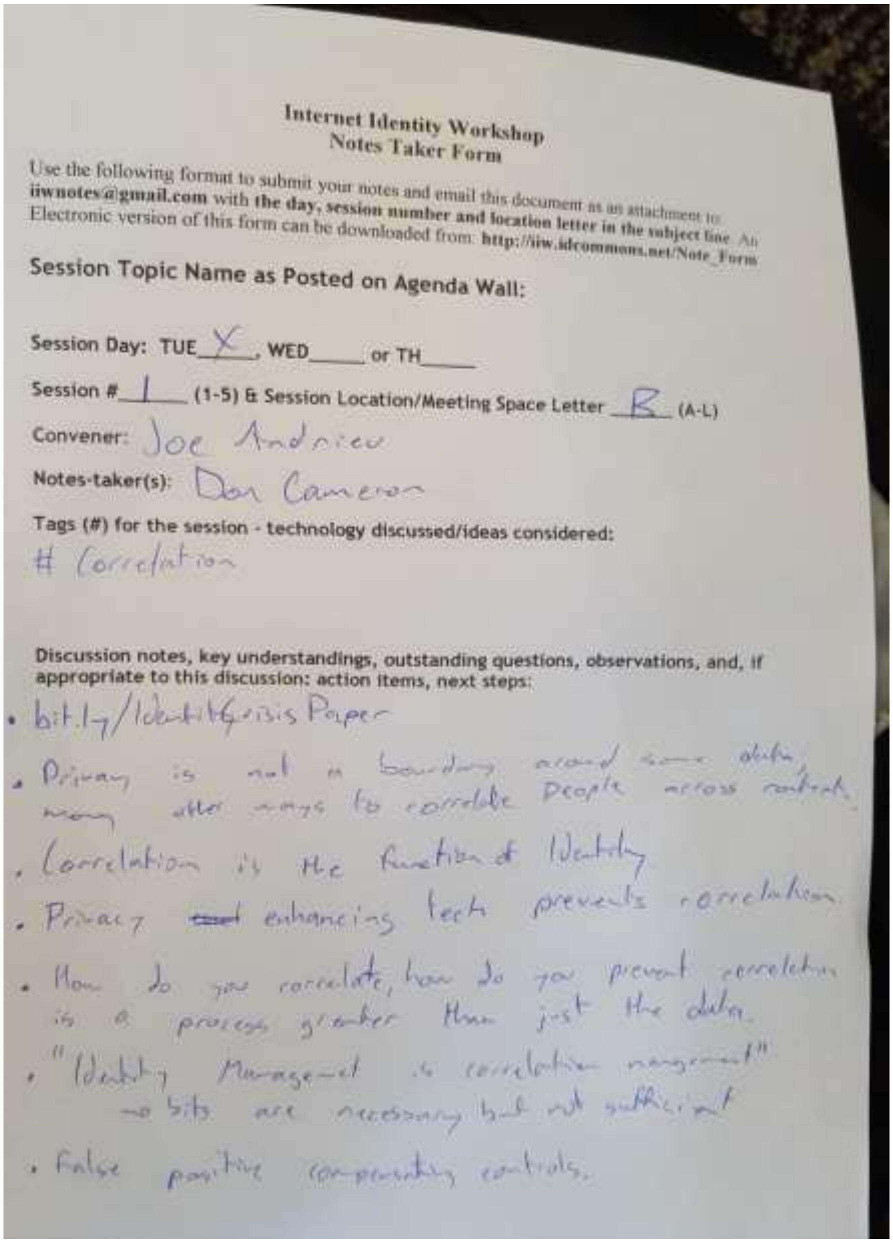
“Correlation” TAFKA “Identity”

Tuesday 1B
Convener: Joe Andrieu
Notes-taker(s): Don Cameron

Tags for the session - : Correlation

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

What goes on a permanent public record? ~ Correlation does not necessarily change identity system. ~ Identity proofing is focused on bits, not correlation.



Internet Identity Workshop
Notes Taker Form

Use the following format to submit your notes and email this document as an attachment to **iiwnotes@gmail.com** with **the day, session number and location letter in the subject line**. An Electronic version of this form can be downloaded from: **http://iiw.idcommons.net/Note_Form**

Session Topic Name as Posted on Agenda Wall:

Session Day: TUE X, WED____ or TH____

Session # 1 (1-5) & Session Location/Meeting Space Letter B (A-L)

Convener: Joe Andrieu

Notes-taker(s): Don Cameron

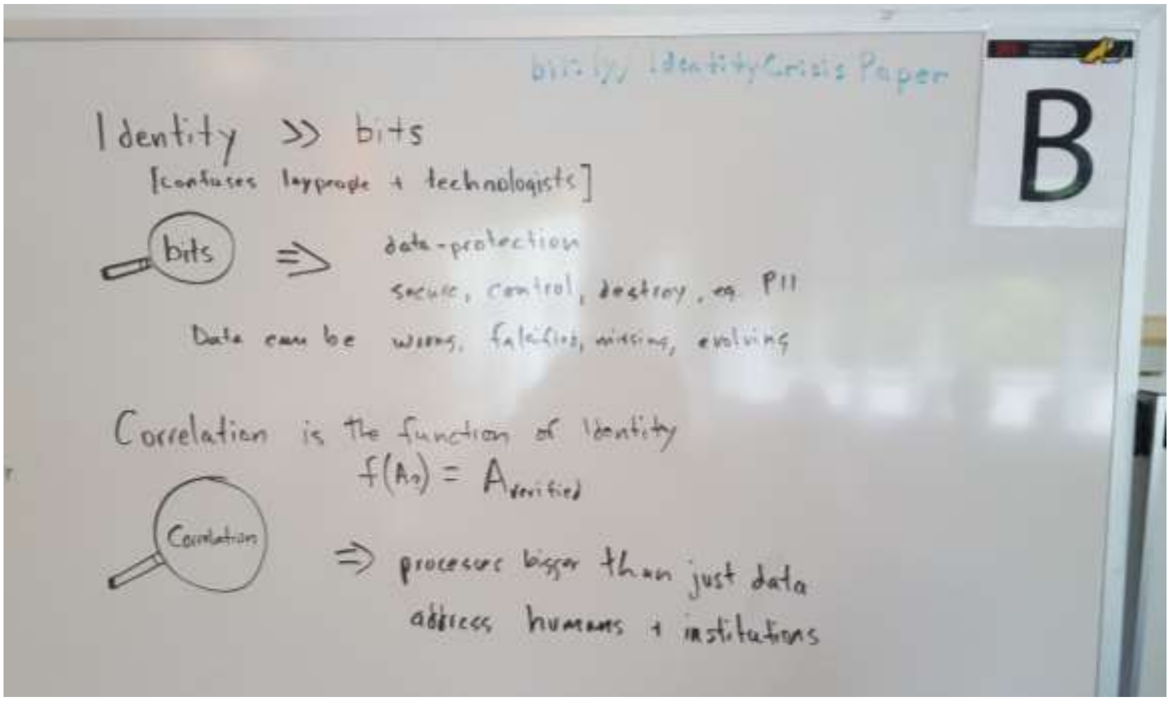
Tags (#) for the session - technology discussed/ideas considered:

Correlation

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

- bit.ly/IdentityCrisisPaper
- Privacy is not a boundary around some data, many other ways to correlate people across contexts.
- Correlation is the function of Identity
- Privacy ~~and~~ enhancing tech prevents correlation.
- How do you correlate, how do you prevent correlation is a process greater than just the data.
- "Identity Management is correlation management" → bits are necessary but not sufficient
- False positive compensating controls.

Photo from whiteboard:



bit.ly/ IdentityCrisis Paper

Identity >> bits

[confuses laypeople + technologists]

⇒ data-protection

secure, control, destroy, eg PII

Data can be wrong, falsified, missing, evolving

Correlation is the function of Identity

$f(A_?) = A_{verified}$

⇒ processes bigger than just data

address humans + institutions

Intro to Verifiable Claims

Tuesday 1C
Convener: Manu Sporny
Notes-taker(s): Manu Sporny

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

It is currently difficult to transmit banking account information, proof of age, education qualifications, healthcare data, and other sorts of verified personal information via the Web. These sorts of data are often referred to as verifiable claims. The mission of the Verifiable Claims Working Group is to make expressing, exchanging, and verifying claims easier and more secure on the Web.

The Credentials Community Group and the Verifiable Claims Task Force of the Web Payments Interest Group at W3C have extensively researched the problem and proposed an architecture and specification to enable the interoperable expression and verification of claims. The narrow scope of work in the draft Verifiable Claims Working Group Charter proposes that the first step toward broad interoperability is standardizing a data model and syntaxes for the expression and verification of verifiable claims.

Specifically, the Verifiable Claims Working Group will Recommend:

- a data model and syntax(es) for the expression of rich verifiable claims, including one or more core vocabularies.

- a note specifying how these data models should be used with existing attribute exchange protocols, a suggestion that existing protocols should be modified, or a suggestion that a new protocol is required to address the problems stated earlier in this document.
- The Working Group will NOT define a new protocol for attribute exchange or JavaScript browser APIs. These work items may be proposed at a future date if there is support for them, but are not necessary to successfully achieve the first step of interoperability.

Session
Slides: https://docs.google.com/presentation/d/1pY6TGsCBzmui_KVM5Q71t1LbHgdv10vRPov7SoISjqU/edit

Verifiable Claims Architecture: https://w3c.github.io/webpayments-ig/VCTF/architecture/

Use Cases: https://w3c.github.io/webpayments-ig/VCTF/use-cases/

Primer: https://w3c.github.io/webpayments-ig/VCTF/primer/

More supporting information (W3C charter, due diligence documents, etc.) can be found here:

https://w3c.github.io/webpayments-ig/VCTF/

End-to-End Decentralized Identity Platform

Tuesday 1E
Convener: Daniel Buchner
Notes-taker(s): Daniel Buchner

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

The presentation is at:
https://1drv.ms/p/s!AuxagrhAB0NJjyhIIE50ZGpnpaQS

The Blue Button Experience

Tuesday 1F
Convener: Sarah Medjek
Notes-taker(s): Tom Brown

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

Link (english) for control of personal data in general: http://mesinfos.fing.org/english/

MesInfos Santé : "My Data" (2013) - give personal info to individuals and see what would happen. 6 companies, 8 months.

Finding: Use of health data very different from other personal data

There is a lot of health data that is not medical data.

Group discussion:

Veterans administration seems to be the socialized exception of U.S. health care.

Hand notes makes doctors less liable

Epic - most popular medical records supplier

In France, doctors reluctant to share data because they seems to think it belongs to them. very similar in U.S. - if they operate in a legal environment, they have to be reluctant

Patient has no influence

Part of the idea of having electronic records is that diagnosis and treatment of condition can be known over time among several specialists

Intro to Oauth2

Tuesday 1G
Convener: Justin Richer
Notes-taker(s): Garrett Schlesinger

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

Justin has a full 2 day curriculum on OAuth 2 / Author of OAuth 2 in action
Overview of today: **What is OAuth 2**
- 3rd party apps getting limited access
- delegation protocol to allow apps to access resources on the owner's behalf
- key players:
1. rescue owner,
2. protected resource (a web API) that protects things on behalf of the resource owner,
3. the client application. the third party accessing the API. Often a web server itself.
4.
    - problem to solve: granting clients access to these resources.
    - old way of doing this: stealing keys (or copying keys)
    - in the new world, we do multi factor. can't just replay credentials since we're architecting more secure systems now.
    - if you can't steal it, ask for the credentials and login on the owner's behalf...
    - ... but this doesn't help the resource delineate between the resource owner and the third party. still fails int he MFA world, too, but the biggest problem is getting users into bad habits. it's the same as phishing when done maliciously, and it's not a good idea to habituate users to do this.
    - another possible solution: API key/universal key. access is much too coarse. Giving access to everything is bad.

What about service-specific credentials? A token that can only access one protected resource? "Service-specific password" in Google's terminology. This is good. It's used a lot... doesn't leak user's credentials. However, the UX is really bad. Forces the user to manage all of these credentials for different apps. Okay. So let's try to make this usable.

Introducing: Authorization Server (AS). Bridges the gap between client and protected resource.

1. Generates tokens for client
2. Authenticates resource owners
3. Authenticates clients
4. Manages authorizations.

Oauth tokens:

1. Represents granted delegated authorities from resource owner to client for protected resource
2. Issued by authorization server
3. Used by client
4. Consumed by protected resource
5. No specific format... they are opaque to the client. The idea is to have a dumb client that just passes the token without knowing the format of the token.

Everybody has used Oauth... anybody who's used a FB app, an android phone, etc. And it's opaque. You don't even realize that you're handing off these tokens.
Auth service can do it statefully or entirely self-contained a token. Self-contained makes revoking tokens difficult. Or token introspection can help you see what a token is good for (often by calling to a service or even the auth server).

Refresh tokens

- Once a token stops working, just do Oauth again
- Problem: this only makes sense when the user is still there. Scraping data in a long-lived process or batch, for e.g. doesn't make sense.
- However, there can be refreshes. Refresh tokens cannot be used to call resources, though. It's just for getting a new token and needs to be generated alongside the access token. It's not a bearer token.
- Bearer tokens exist because they work! It's easy to use them, so even though anyone who has them can use them and this isn't ideal security. Allows for the user to auth only once.

Oauth is not an authentication protocol.

- Relies on authentication, but does not communicate anything about the user. However, authentication protocols can be written using Oauth.

Client cannot interpret the token, but it's recommended that your auth server can tell you what a token is good for.

The Authorization Code Flow (canonical OAuth 2.0 transaction)

- Two forms of communication:
    - Backchannel: direct HTTP connections, server-to-server. User/browser is not involved. Instead, requires user to pass credentials to the wrong place.
    - Frontchannel: uses redirects through web browsers without direct connections. Client redirects browser to the auth server, so the auth server is getting the request. The user talks directly to the authentication server, which was the goal. Woo! Then, the result goes back the the client via another redirect. The key here is that there's something in the middle. This obviously can cause problems with man-in-the-middle attacks, but there could be problems with getting user credentials through this vulnerability even w/o Oauth.
- Step 1) client redirects to authorization server. 2) User (resource owner) authenticates to auth server... OAuth is agnostic to this auth. Auth server could do SFA, MFA, or anything it wants. 3) Resource owner authorizes client (grants scopes... "yes, you can read my profile

information and see my bank transactions"). 4) authorization server redirects back to the client with an authorization code (front channel), 5) server-to-server exchange of authorization code. authorization code has a fairly tight timeout. 6) authorization server issues access/bearer token to client. 7) client uses token via backchannel. user doesn't need to be present since the client has a bearer token that resulted from the exchange.

- Layered trust model: whitelist: centralized control, traditional. blacklist: centralized control, also traditional. greylist: end-user decisions... not on a whitelist or blacklist. need extensive auditing and logging. rules on when to move to the white or black lists.

Lots of choices in the Oauth space. need to pick the appropriate one for the apps you're building! Implicit? Authorization code? Resource owner credentials? Client Credentials? Assertion? Add PKCE or DynReg? Very tricky decision space to manage, but once you figure out that Oauth is a good thing, it's a crucial decision to figure out the right way to use Oauth.

The 4 Kinds of Privacy

Tuesday 1H
Convener: Christopher Allen
Notes-taker(s): Christopher Allen

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

Blog post on 4 kinds of privacy:
http://www.lifewithalacrity.com/2015/04/the-four-kinds-of-privacy.html

ONTY

Tuesday 2A
Convener: Simon Jones
Notes-taker(s): Doc Searls

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

Onty is about privacy. / Privacy ⊂ freedom. (Privacy is a subset of freedom.)
"I wanted to find out if anyone else on my street had a miscarriage so we coud talk tp them ; I couldn't go to Facebook with that." — Soho, London, March 2016
gagging by exposure.
broadcast model
lack of data sovereignty
degree of data inspection
Onty: private <—> sharing
no broadcast
confident in confidence
reduce digital litter (it's a targeted matching system—you can target it to whoever you want to hear it, not to the world)

Does any Canadian woman in London want to have a baby with me?

There may be an obscure forum for this, you may still not want to go there, because it's to exposed, for example.

Wouldn't it be good to build your half of this and leave it privately on the internet.

Uses a digital lock and key (not PKI)

Woman
canadian
wants
baby
lives
london

It's a story and a thought matching system

It's story agnostic. Doesn't know or care, because your story is private.

It multi-graphs.

Others might be

- Who does your job in China, or who drives their kids to your kid's school?
- Who does .net programming in Bali, surfs and speaks fluent English
- Who's on Airbnb in Paris, is Japanese and can tutor.
- Has anyone found my GoPro that I lost in Cornwall

The idea is that Onty can take all these stories, these halves and combine them into a self-soveriegn picture of you. There are bits of my life in here.

Q: is this uni-directional?

A: It's hierarchical, but the matching doesn't care about the representation

We may allow cross-links in the future. Experimental aspect.

Q: *Something about people trying to game / entrap people to expose them somehow:*

A: Soon as you find a bad use, you know you have a good project. There are lots of self-policing efforts.

Q: Can you allow time delayed feedback loops.

A: there are many experiments we need to have

stories: privacy encourages breadth and depth mine system for connectoins and talk. be selectively searchable on any part of youir story. Onty is agnostic.

When youi find what you're looking for, you can immediately chat.

The key is the only thing you know about each other is shared information.

Q: what about the exposure of communicating yoiur life story in the clear?

A: A good point. a hard challenge framing this project. Avoiding "private" and "anonymous."

(Digressive point about anonymity: <https://www.quora.com/What-is-the-Greater-Internet-Fuckwad-Theory>)

Discussion about exposure.

There is no idea of a profile. There is no avatar, no other digital version of you. Designed so you can project the plurality of your self. No individual match is a whole.

Demo: Onty.com

Ontys are quick and easy to read. Designed to solve the matching problem for any two statements.

Don't want to match blocks of prose.

Hosting intent
controlling
monetising
collaborating

Imagine a story where a woman retired is mmaking honey from rose nectar.

Can't preëmpt all the ways this might be used.

Q: do any canonization? Pluralization? Synonyms?

A: Yes, plus designed to be language neutral.

A self-organising system. At any point in the graph, onty will give you suggestions from everywhere in every graph. Persons in messages are represented by numeric strings. The respondent can see no more identity than a match.
Q: ever heard of bio-pin? Might be similar or relevant.
It has a number of long term goals, beyond being a private sharing system.
When it becomes established, it has emerging properties people can benefit from. One for example is being used to generate a proxy ID on the internet. Airbnb has a massive paradox of choice issue.
The solution to all matching problems can never be designed by developers. Need to hand control over the design of the service, or the problem, back to the users.
While it looks like the solution to the private sharing problem, it is suitable to the intention economy. matching intent to sell or buy.
Q: Parallel effort: platform business models. business is about matching third parties.
Advantage is private search.
In matching demand and supply. making the intention economy happen
Advantage in discovery.
Opportunities in corporate search
If you ask a question, the only people who will discover it are others with the same question or those that have the answer.
You need to
Q: where you going with the protocol?
Q: note the metacurrency project — deep wealthy, non-currency ways of valuing. cemtrex

UX Hacking the Personal Data Dashboard

Tuesday 2B
Convener: John Wunderlich
Notes-taker(s): Giles Watkins

Tags for the session - technology discussed/ideas considered:

#GDPR #PersonalDataDashboard #ConsentDashboard #ContextBasedConsent
#ConsentRevocation #AIagents
Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

Problem statement – wonderful having all your info and under your control – especially if you are a geek. However, most people don't want the depth and complexity of a comprehensive 'engine management system'. We need something simple, with 'levers'(or pedals !) to be able to control the juggernaut
What sort of visual cues do we need ?
What would make it usable / contagious for people outside of the identity community?
Christopher Allen

- Sharing research from Bitcoin and Wallets
- Progressive disclosure has been an emerging concept
- Taking a step further – 'decision-based' disclosure
- Perhaps taking learnings from the 'Gaming Horizon' concept

Joe Andrieu

- Best UX is the one that doesn't exist…..
- Don't want a generalised permission dialogue

- Need it built into the decision / workflow

Phil Windley

- Better to deconstruct the dashboard
- Eg typical LMS – replicates things they already have (eg calendar, to do list etc)
- Why not put that information into the places they already go

Joyce Searles

- But its useful to have a 'contextual dashboard' – eh when I am driving, its useful to know whats going on with the car….

Phil Windley

- There probably IS a case for a 'persona data dashboard' – because nothing exists right now, and there are an increasing number of complexities springing up

Katryna Dow

- Now taking first person information and putting it into third person contexts
- Making it 'easier' often means giving everything away – with no control…..
- GDPR brings some of this into a legal context
- Is there something between the dashboard and the third party that provides control over what gets shared and with who

Phil Windley

- There are some existing technical standards (eg calendars) but where are there not standards

Katryna Dow

- Not a technology problem….. More about how we get the existing world to adapt to and adopt the new principles about first person control

John Wunderlich

- So maybe we need a protocol that says APIs can push information into the dashboard, but can't pull information from the dashboard into third party systems

AN Other

- Do we need systems that can put certain information into dashboards / calendars, but have links to where more detailed information can be found (which needs to be permissioned)

AN Other

- Dashboard / authorisation as a service – two different things…..
- People are not going to go to the dashboard everyday (probably)
- But would want to have episodic / contextual views

John Wunderlich

- No such thing as an 'intuitive interface'
- So, how do we create something that is going to make 'general sense to the general user' ?

Phil Windley

- Need to integrate AI with contextual view, to create a time-based push of information
- Would be useful if the AI could look at data usage and ask you questions about what you are sharing and whether you still want to
- Is this possible outside of the large players (Google, Apple etc) – is the Network effect too dominant. Or, are we just going to create another dominant player?
- Would this be possible with personalised AI, personalised search and a personalised timeline???

Jim Fournier

- If the big players always have to ask permission for the data / access to it, then we can break the cycle of their network learning effect

John Wunderlich

To draw the discussion together - What does a dashboard / service need to give us ?

Responses:

- We are going to need a 'magical undo' function – to pull back previous decisions

- We will need ability to know 'what have I shared'?
- We also need to know 'what WILL I share'?

Tiffany

- We need to work out whether we are creating a UX to 'educate' or to meet a 'demand' from someone.

Giles Watkins

- Too big a problem to try and educate every citizen to drive adoption
- We need to work out how to get a 'band of competitors' to collaborate on working out common standards/approach to this problem and push it out to citizens
- Possibly like the OIX model…..

AN Other

- Perhaps we could develop some sort of algorithmic / questionnaire based way of learning what a specific citizens 'attitude to Privacy' is…. Not everyone is equal….

Katryna Dow

- There is a looming problem with the potential to feed a lot of really detailed and sensitive information into a 'black box' that start processing it with algorithmic learning without proper standards and controls
- It will be hard to roll-back from a bad situation like that

AN Other

Recommendation – people should try and read the recent posts from Adrian Colyer (website – www.themorningpaper.com) – discussing the problem with Git…. We need a better understanding of how human beings learn and design around that

John Wunderlich

Maybe the learning from this session has been (apart from the obvious, that this is a hard problem to solve!) – if the back-end systems aren't already based on 'human centric' design, then we will not be able to put a human centric 'dashboard' on top.

It is going to take some collaboration, probably by competitors, to create some usable and standard approaches to the problem.

Next Steps: John to consider the themes arising and what might be a useful way to continue the debate.

Account Chooser, the Re-Charter

Tuesday 2C
Convener: Pamela Dingle
Notes-taker(s): Pamela Dingle

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

Rechartering presentation available at: http://openid.net/wordpress-content/uploads/2016/11/Account-Chooser-Rechartering.pdf

Questions:

How do you see this interacting with 2-factor authentication?

- there are 2 levels — device locks like pin codes screen locks
- or authentication services
- Might be possible to store that information in the preference manager

Could an application bar password managers from being used? *Today the application can specify what the support, so that the account chooser knows what to render
Isn't this just encouraging password manager proliferation, why not just federate?

- The thought is that federation is not an easy lift for all, but embracing programmatic authentication could be an important first step that could move us in a direction that could move us towards more mainstream federated mechanisms

Will this just mean passwords are all over the place?

- Storage of passwords is an implementation decision out of the control of the charter of this WG

What does the process flow for the credential save API lookalike?

- There are concepts like tentative saves, etc that help with ephemeral password saving

Can you talk about how the isolation works between the password manager and mobile apps

- Security aspects of the app talking to the password manager depend on the capabilities of the mobile operating system

How do you prevent XSS in the retrieval of credentials via the API?

- This is going to get released as part of the WG work
- Developer education is also an important mechanism

How is this different from the W3C credential management work?

- The W3C effort just assumes that the browser is the password manager, this effort is focused on the mechanism for choosing a provider, as well as the API for interacting
- Is there any assumption that the credential is local or cloud?
- Doesn't matter, it is an interaction between parties, how those parties store information is up to the party

Data Portability

Tuesday 2E
Convener: Mary Hodder, Doc Searls
Notes-taker(s): Scott David

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

Mary's outline of discussion:

- List existing pieces
  - terms and policy
  - data schemas
  - data dictionary and taxonomy
- What can we learn from companies and projects that have failed
  - list of failed efforts and learnings
- List of needed schemas, rules and policies, taxonomy
- List of entities that need to be in the room
- Find and list gaps in ecosystem
- Use cases or verticals:
  - Health

- emergent use cases

- Open source effort
- UX for taxonomy

Discussion notes:
Where does VRM go next?
Missing piece of control to distribute may be data flowing in ways that keep user at the center.
Even though it is nuts and bolts, it is a point of power – gatekeeping function.
Working on schemas and standards from organizations have silos with agenda. Interest in keeping things not portable.
Kantara CISWG as starting point – looking at 2 pieces of the many pieces that need to be established for a user-driven (not necessarily user "centric") system.
Clarifying question: Desire for control and moving their data. But which data between which entities? What is the scope of that.
Back to general issue setting: Lots of information can move easily.
So, session called to talk about the idea of bringing people together to fill the gap – standards making and schema making body – what in individual at the center. Also a UX element that is important. Make it accessible.
If putting the user at the center and in control – need it to be accessible to people. UX component. Variable.
Who is here. Who need to pull in. What work need to be done. Use this as an organizational session.
New comment: Pieces of a platform may be across a range of things. Distributed infrastructure. Tracking it across platforms, etc.
information and rights around it. Move the information.
New comment: Don't look at the movement of the data, look at the movement of the data rights – as information. That manifests in value o and harm which is the source of the challenges and business plans. what if it is information not data that moving. Data rights management can yield. Rights different plumbing than data itself. Secrecy is dead, long live privacy
New comment: Challenge of connecting the shared data to get it into some type of stored thing. Project to map ID System can provide useful cartography for parties and relationships in the system.
Noted Fing in France – 300 people put data in central store, and made it available to companies. They have reports from 2013 from the experiment. Testing. Shared data under French data laws. Data store. Only individual had access. What would an individual do if they got this information available to them.
Question with systems of "if you build it they will come." does that work?
New discussion of scope: How do we self define scope of the notion. What parts are we seeking to derive. Might consider narrow scope to help us stay on task on user centric notions and goals. What changes in older systems when we move to user centricity.
What are focused pieces that are needed? What is boundary set?
Example provided in XML context. First question there was what is needed. Needed reliable data repository, registry, data dictionary, etc. Had components identified.
It is genus and species question. List species to derive genus.
What can we learn from the companies that have tried and failed?
Consideration of end to end platform. Talk about all in concert, but never enough because not "hummm" as one machine. Want data to be more standardized in terms of output. Company willingness to make data public, not wanting to retain it in silos. Looking from systems perspective and de facto standardization.
Comment: GDPR will make it happen – Article 20 – right to data portability. Will be a driver.
UK MyDATA project – in markets prone to cartels and inertia – drive data back to data subjects. Industry managed to slow it down with standards. E.g. E-on energy when switch as customer is required to provide data to the data subject.

Comment: This data is a manifestation of the operation of these kinds of systems.
XDI – semantic elements of link contract designed for data sharing. We are reaching a problem space for which XDI was designed.
Question of whether all the schemas have been defined. Schemas may already exist. Maybe need to start with mapping to figure out where holes are and with a larger set of stakeholders.
Question of subverting process. How can the "user at the center" vision happen, when it messes up a bunch of business models.
Comment: Pushing from the wrong direction. More effective to define the end to end system that delivers customer value. If can deliver user value, then pulls the other companies into it.
Question of whether this is still centralized.
Answer: Still user permissioned.
Back and forth on terms – They want to define the system with what they can control. Question of enforcement. Question of whether can make a statement of will and whether it is enforceable.
Market solution and user solution. Is there a negotiation? Is this a notice and consent?
Question of assertion and enforcement of rights.
This becomes easier in system of user expression, need to sign a receipt. Enforceability through reputation network is what is going to enforce these. Question of whether enforcement is manifested through reputation systems.
Description of NSTIC/IDESG provided as suggestion of "reputation" type systems to compete on user-centric standards.
Fact of rating not affect how good going to be with a particular user.
What are the ratings, and do they talk about how made public.
EFF runs a system like that now, like a consumer reports. Done on expert score, not aggregated consumer score.
Need mapping to help with reputation mapping.
What things could we track and map and decide where there are holders. Where can we combine taxonomies.
Kantara examples – of things proposing to create.
Not need to work within one organization
Electric generation facilities all produce energy into system. Standards organizations.
Syntheses of concepts.
Create artifacts of mutual desire for interaction normalization in the gaps. The ideas of what works in the gaps will perpetuate themselves through the chosen artifacts, but each will be incomplete. Get "end to end" harmonization through coordination of the gaps.
Healthcare is a use case. Optimum takes all claims data and harmonizes it.
If going to do that, need formalities of inter-organizational licensing, and liability constraining rules.
Needs to be an open source effort. If protected in some way,
Not every aspect needs to be open. Need some subset of core functionality to be open. Can let folks sell lemonade at the public park.
Let's use everything we can that is out there. Not remake things already made.
Build universe of use where user is at the center
Suggest using wikispace to collect the information. What kind of information needed. What levels of detail needed.
Possibility of this effort collaboration with the creation of a map to leverage existing pieces. Lots of disparate pieces – how can we bring them together? Not need to build everything.
Expose what is needed to create user-centric market.
Health care may be a challenging area because of high level regulation and interested parties.
Maybe not try to hard. Organic emergence of structures. ~ Also, what can we learn.

Personal Data Stores in the Enterprise

Tuesday 2F
Convener: Tarik Kurspahic and Shane Green
Notes-taker(s): Tarik Kurspahic

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

In this session, we shared market intelligence from TeamData's (previously Personal.com) various attempts at getting consumers to embrace personal data stores (PDS) and the reasons behind some the failures. There are recent successes as well though and they stem from going through enterprises.

While it's hard to get consumers to embrace a PDS, enterprises know they are lacking security & privacy around sensitive company data and are more willing to be proactive. Getting to the right stakeholders who want to clean up their process and tools means a wider adoption by employees, who eventually get to the "aha" moment and turn around and use it in their private lives. This allows us to preserve the wider mission of getting consumers to eventually adopt a PDS and get better about managing their data by being introduced to it through their workplace.

Intro to Open ID Connect

Tuesday 2G
Convener: George Fletcher, Don tTibeau
Notes-taker(s): Garrett Schlesinger

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

An identity/authentication layer on top of OAuth 2.0

Connection protocol suite

- Key piece: core spec (all bits of the protocol) which include implementation guides.
- Discovery & dynamic client registration are about making the pre-registration bit in OAuth 2.0 to become more dynamic. Important for IOT.
- Form post response mode: less important.
- Session management: more important. How do sessions end? How do you know a session is still valid?

Session management:

- Front-channel logout (logout in the browser. Propagate to all relying parties.)
- Back-channel logout (logout all on server side. works if you have server-side sessions everywhere)

See: http://openid.net/wg/connect/

Health relationship trust (Heart)
Internation assurance government profile

OpenID Certification

- Enables openid connect implementation to be certified for interoperability, etc.

Authentication
Definition: "how do we know it's you"

Web site wants to know who you are. Site redirects (OAuth 2) to one (or a selection amongst several) IdPs (identity providers). Requires an opened scope. IdP will often first look for an SSO token. Prompt for credentials otherwise. IdP prompts for consents ("Do you want to share your email address?" etc). IdP redirects back with a code + state parameter (mitigates CSRF). Code is an artifact (like in SAML) that is then used for then generating an access token via site's backend calling to the IdP. IdP passes back id_token (possibly also access token and refresh token). Requires client credentials in addition to the code. OpenID allows for several methods of authentication, some using public key infrastructure (PKI) ,signed JWTs, client shared secrets, etc.

Flows: code, implicit, hybrid.

No value in secrets in the browser.

Implicit flow optimizes the code flow by shoving everything into the browser. Sends id token etc in browser hash since the browser shouldn't persist this in history. Doesn't in practice work that well on all browsers. In any case, really need to validate the id token. Look at the issuer. Validate their public key. Who knows what could happen with MiM attacks, etc. Also need to check that the id token was intended for you. Easy to mess this up, actually. Lots of big sites have gotten this wrong.

Hybrid flow--in between the code flow and implicit flows.

ID tokens are assertions. A best practice would be to have something to inspect the tokens.

Authorization requires layering if we've learned anything from social media apps. Can't 100% split out authentication as a result since we will need to come back to it for more scopes!

id_token (a JWT):

- iss: the IdP: who issued the token. introspect this to know what public key to look up to validate the token, make sure it comes from where you think it did.
- sub: the user (subject)
- aud: audience (client): to whom the token was issued. possibly an array, but that's a detail.
- iat: issued-at time
- exp: when the token expires
- jti: unique id (possibly a uuid) for this token

JOSE spec. Signing mechanism. Encryption also possible.

JWT parts:
Header: {typ: JWT, alg: RS256, kid: pubkey1}: cryptographic envelope
Payload: (just has to be JSON): {"iss": "https://auth.blah....", "sub": "9X8FH2"}

Signature:

format: <b64-encoded header>.<b64-encoded payload>.<signature>

Signature is used to validate the header and payload. Dead simple. Validate the original b64-encoding since generating your own could get mucked up with JSON key ordering.

Remote Identity Proofing

Tuesday 2H
Convener: Francisco Corella, Karen Lewison
Notes-taker(s): Francisco Corella, Karen Lewison

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

Remote identity proofing usually relies on asking the subject multiple-choice knowledge questions (e.g. which of the following zip codes did you live in five years ago?), but this method is privacy-invasive and has become ineffective due to the proliferation of personal data available online.

We have identified five remote identity proofing solutions that can be used as alternatives to knowledge-based verification. Solution 1 uses a rich credential issued by a DMV and containing a facial image for three factor verification with spoofing detection. Solution 2 uses an adaptation of a rich credential for use in conjunction with a blockchain. In Solution 3, the subject demonstrates possession of a contactless EMV credit card to a remote verifier via a native app that interacts with the card over a Near Field Communication (NFC) connection and with the verifier over a secure Internet connection, and relays Application Protocol Data Units (APDUs) between the card and the verifier. In Solution 4, the subject demonstrates possession of a contactless medical identification smart card containing a certificate and a facial image, via a native app that relays APDUs and submits an audio-visual stream that the verifier uses for face recognition with spoofing detection. Finally, Solution 5 relies on face recognition with spoofing detection using the signed facial image and biographic data contained in the RFID chip embedded in a passport.

Slides: https://pomcor.com/documents/IIW23.pdf
Blog: https://pomcor.com/2016/10/28/remote-identity-proofing-discussed-at-the-internet-identity-workshop/

Kantara Incubator R&D Funds

Tuesday 2I
Convener: Colin Wallis
Notes-taker(s): Colin Wallis

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

The link to the Program is here:
https://kantarainitiative.org/confluence/display/ccicada/Home

And the slide presentation is here:
https://kantarainitiative.org/confluence/display/ccicada/Presentations

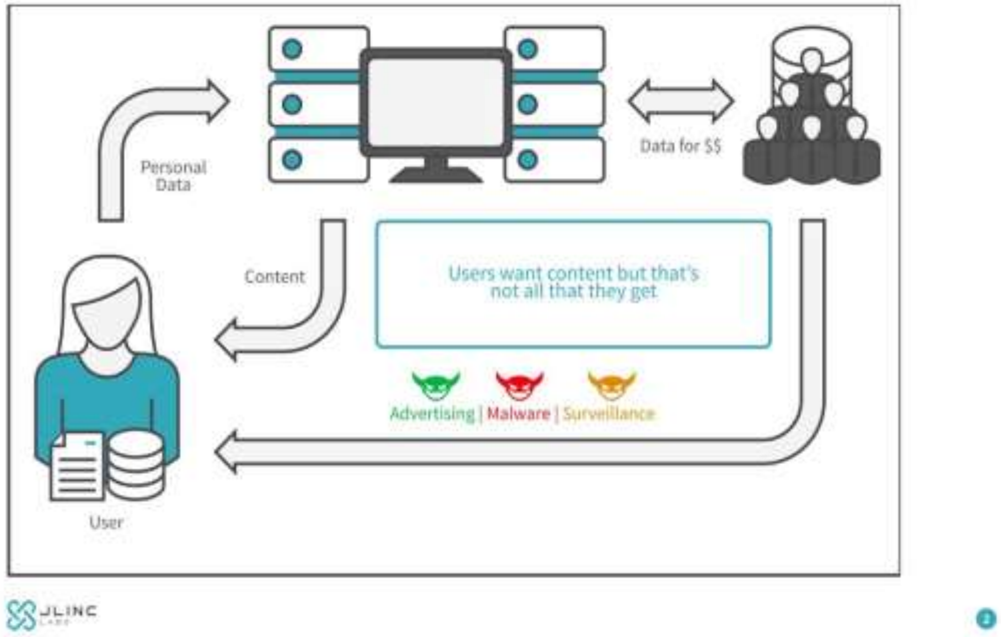
JLINC

Tuesday 3A
Convener: Jim Fournier
Notes-taker(s): Jim Fournier

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

JLINC is an open protocol for controlling data use on the Internet –- after it is shared.
The session focused on an Alice and Bob Co volunteered personal data use-case.

http://www.jlinclabs.com



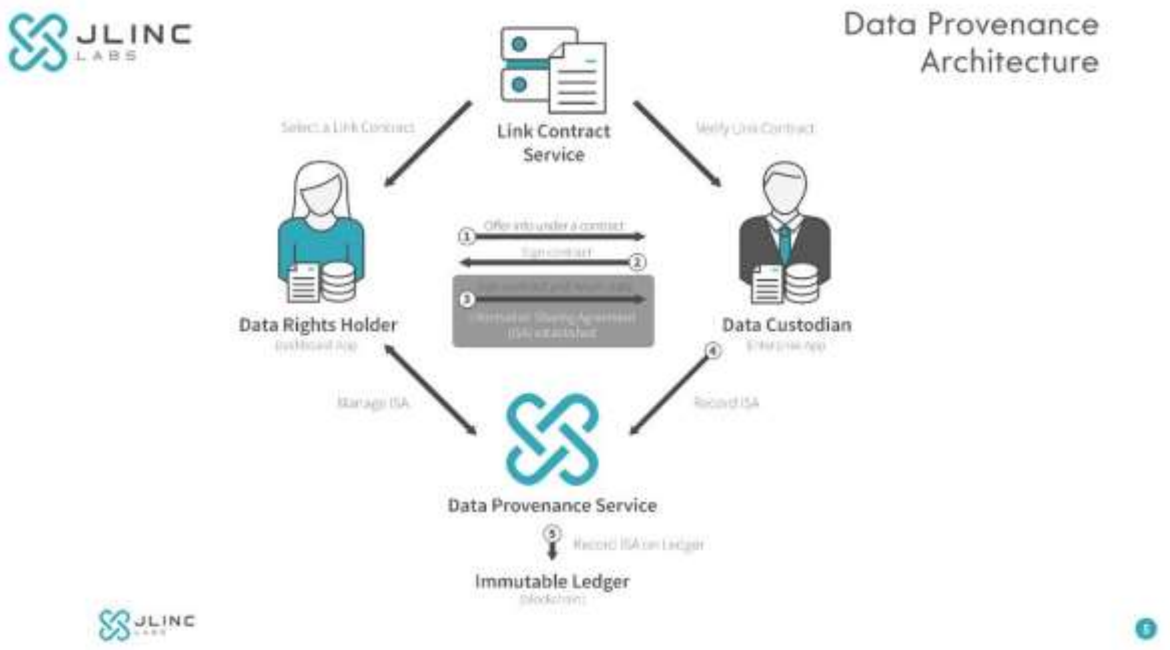
Users want content but that's not all that they get

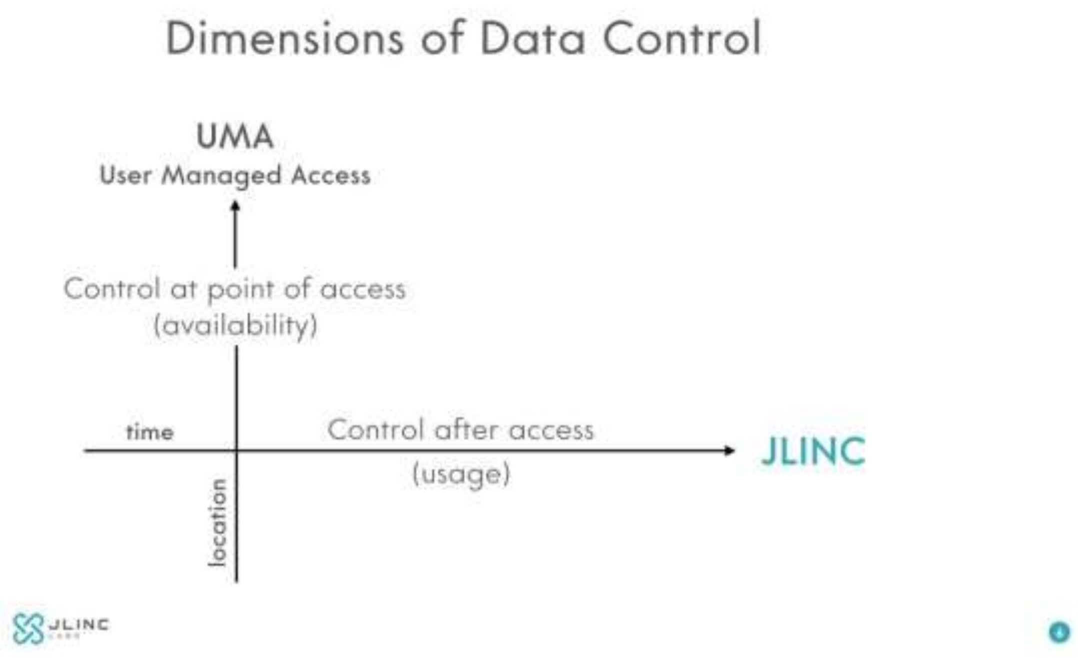
JLINC is an open protocol for controlling data exchange across the internet. It combines several strands of recently evolved technology to create a fully decentralized solution for Internet "data provenance" – a signed, private chain-of-custody to control data, after it is shared.

Human and machine-readable Information Sharing Agreements (ISAs) written in the universal web language JSON, are signed using industry standard curve25519 public key cryptography.

A compact digital fingerprint of the signed agreement, called a "hash," is recorded on a distributed global ledger (blockchain).

This provides a "digital return receipt" and an audit trail, which allows all parties to prove that the signed copy of the agreement they each hold covers their data, and that it was signed by the opposite party when it was recorded on the ledger.





Dimensions of Data Control

UMA

User Managed Access

Control at point of access

(availability)

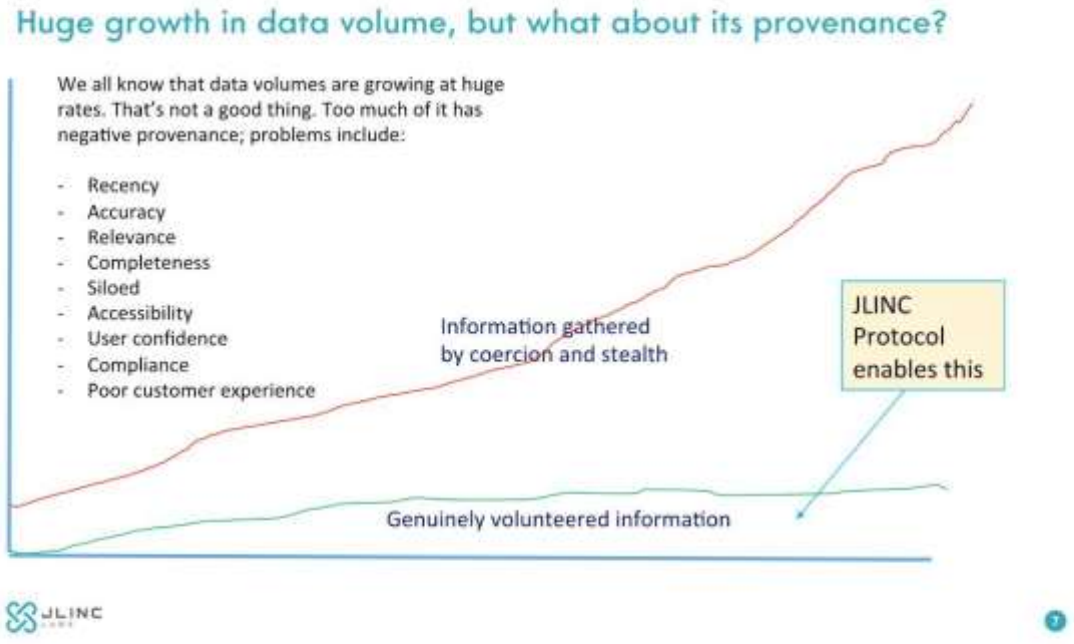
time

Control after access

(usage)

location

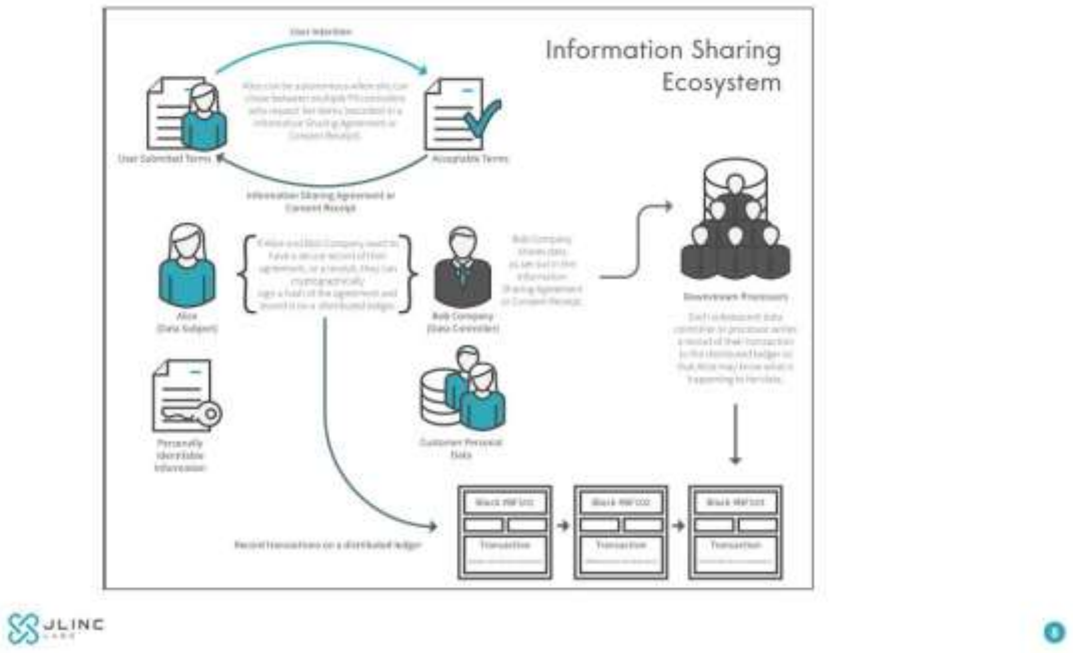
JLINC



Huge growth in data volume, but what about its provenance?

We all know that data volumes are growing at huge rates. That's not a good thing. Too much of it has negative provenance; problems include:

- Recency
- Accuracy
- Relevance
- Completeness
- Siloed
- Accessibility
- User confidence
- Compliance
- Poor customer experience


Information Sharing Ecosystem
User Intention
User Submitted Terms
Acceptable Terms
Information Sharing Agreement or Consent Receipt
Alice (Data Subject)
Bob Company (Data Controller)
Downstream Processors
Personally Identifiable Information
Customer Personal Data
Record transactions on a distributed ledger
Transaction
Transaction
Transaction
JLINC

Personal APIs

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

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

Businesses have APIs, why shouldn't people? This puts people on a level field with companies. Personal APIs can be called by businesses as well as other people.

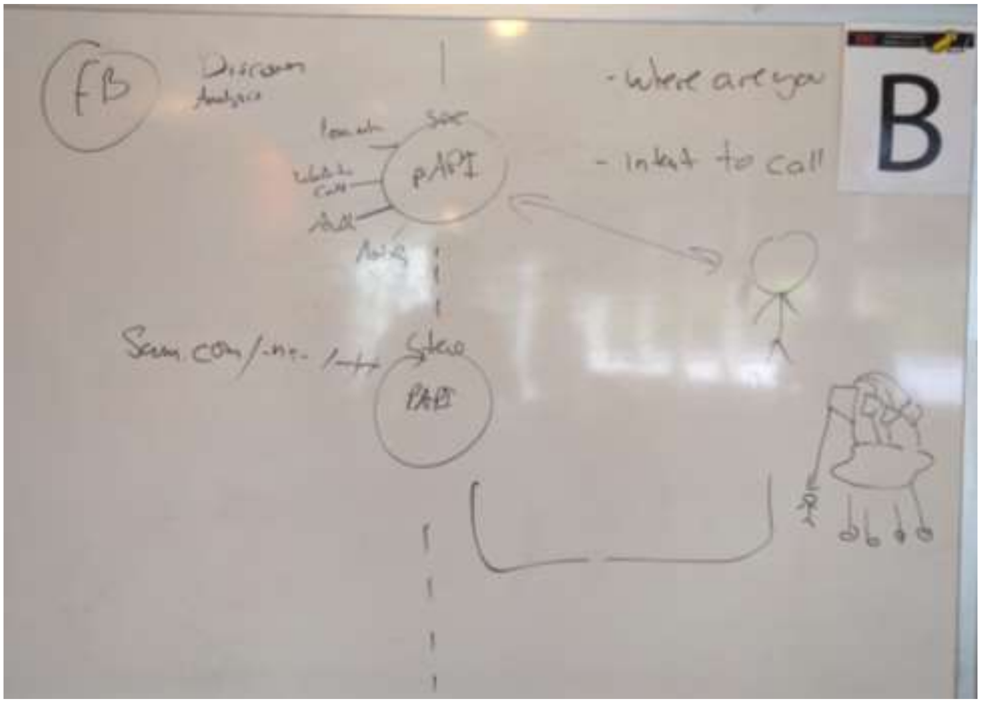
PersonalAPIs have a consistant interface, but do not dictate the behavior underneath the API (behind the curtain, if you will). There is a business opportunity here, for paid servies that provide this behavior.

Personal APIs can host multiple interfaces by placing each one in a namespace via url segment: my.api.com/namespace/paths/within/namespace

Only minimal behavior will be supported by the core API itself, mainly focused around discovery of installed api extensions.

Example queries via the API:
- Where are you?
Shares back location subject to permission and granularity configuration.
- I'd like to talk when convenient

Registers a request to talk when convenient. Underneath the API, the request is not surfaced to the person until deemed non-disruptive.



Financial Data Aggregation & Sovereign Identity

Tuesday 3C
Convener: Paul Ablack and John Best
Notes-taker(s): Ed Gonzalez

Tags for the session - technology discussed/ideas considered:

#DataAnalytics #Aggregators

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

Aggregators
- Mint
- Money Desktop
- Yodelee

3% adoption rate
Users don’t feel its secure
Users don’t know how there data is being used.
Screen scraping technology make aggregator sites unreliable
The battle is security vs control
Corelation of data is a problem – companies that collect and correlate can sell this valuable data.

OnApproach has developed the tools to better aggregate data from multiple platforms without screen scraping through the financial institutions.

Holding the data is not the advantage, it is how you use it.

Giving uses back control of their data. Instead of pulling information for a loan, what if you send the application to where the data is. Analyze and process to send a decision back out.

Portability

Standardization of data is a challenge.
Currently data resides in different data silos.

How do you normalize data across an entire industry?

OnApproach allows Institutions to collect data for their members bypassing PFM Aggregators who your data into silos

First Party Terms

Tuesday 3E
Convener: Scott David & Doc Searls
Notes-taker(s): Scott David

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

User terms:
Assumption that always need to be subordinate party.
First party terms – resonates better.
When signing contract of adhesion, you are always a second party.
Question of the dance of contracting. What are the power relationships.
Customer commons is modeled on creative commons – do for terms what Creative commons did for copyright.
Assumption that can come up with few simple terms to express what we want in a give context.

> E.g., do not track – Can this be put into terms, can be audited and can be enforced.
> e.g., how long the data is held is another.

Those terms are somewhat arcane to the intent casting scenario. There are settings in which those are not workable in different contexts.
For our purposes, to begin with, take areas of practice and put them into customer commons things that will be useful to the world.
Then question of how want to grow customer commons.
We then engaged in Kantara group review – consent and information sharing working group reviewed.
Looked at models of no tracking and no stalking.
Look at ad blocking, etc.
Three kinds of advertising:

> Old fashioned brand advertising – not targeted
> Search advertising – correlation
> Tracking based – it is not advertising, it is direct marketing. Comes from the junk mail business – but looks like advertising.

What if people asked for ads not based on tracking – still allows analytics. Doesn't speak to re-identification.
Many folks say do not track, but what is the nature of the understanding had.
Question of using the stalking and talking terms. What is the impact of using tracking and stalking terms.
Question of the spirit and the letter of the law. How manifest each.
There are pathways to violation of the spirit. Trying to create representations that get people in trouble. Sometimes you violate your own bugs and don't get in trouble.
How get enforcement of user terms.
With arrival of the GDPR, have chance of individuals t o instantiate the GDPR. Severe penalties under it.
What if you put the GDPR into Virginia trust framework to offer terms as product in the US for companies and people that want to carry forward elements into US relationships without connection.
Look at Kantara Consent and Information sharing terms on website:
Have the human readable and legaleze versions of the language.
This is kantara project (under their terms) under the consent and information sharing group based on work of customer commons. Customer commons will be where the terms live, that is main job of the customer commons.
If you put in a term that says, "no third party sharing of information" make it so can be seen and easily understood.
Company that uses the protocol to create intent casting on J-Link, for example, could see the flows.
J-Link protocol allows the assertion of terms and the receipt of answers to that term within the context of that term.
Group meets on Monday AM, 8am pacific.
Want to develop more terms, multiple terms
Human readable, machine readable and engineering layer that has piece that can be "asked and answered" about questions in terms. Cheddar is collection of best practices on server side, a measurement of whether the standards are met.
There is not yet a lot of work on the machine readable stuff.
Want to generate something that NOT poisoned in favor of either party. Put it in the middle of the interests, so that not hurt or harm one type of party from the inception.
Can have sunsetting provision that requires disposal of data after a time. Limits mischief of later use of data.
How do we crank out the terms to those that are not confrontational.
Ian presentation on J-Link –
4 parties of JLINC described. And describe the user submitted terms. Coaching function described – it provides terms for user to present, but not limited to those default terms.
It is a contract negotiation choreography tool and agreement capture tool.
Suggestion to think about things that benefit both parties and what they cannot do unilaterally. They will come to this for cost savings and risk reduction. If company, must come for cost reductions to maximize income for shareholders).
Unpacks the contract negotiation dance, and slows it down so that people don't miss the nature of the rights and duties being exchanged and negotiated.
Terms recommendation engine.
Like markets – what can you do unilaterally and what is best done in markets.
Can have terms that
What is the notion of pricing of their terms.
Pricing of terms – what is pricing.
Sliding scale of pricing.
Would like to take Faustian bargains off the table, but it may be honest to reveal the bargain that is in fact being made.

That piece happening now – if running ad blocker – then pricing for access. More honest. Question of whether one strategy is better than the other.
Did we discuss the permissions and obligations at W3C – artists create work and attach permissions to the work. Have a policy language – with data. Verifiable claims stuff can do the same thing. Could you hash that together and with work and use it as DRM.
Some are working on version based on Koala IP to gather with intent receipts – overlap on 95% of the terms. Have a reference to PDF document.
Other promising part is in blockchain – san start to create real world use cases, personal data used from first party perspective.
Can have a market in data rights that can help with pricing.

Military Identity Use Cases

Tuesday 3F
Convener: Heather Vescent
Notes-taker(s): Heather Vescent

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

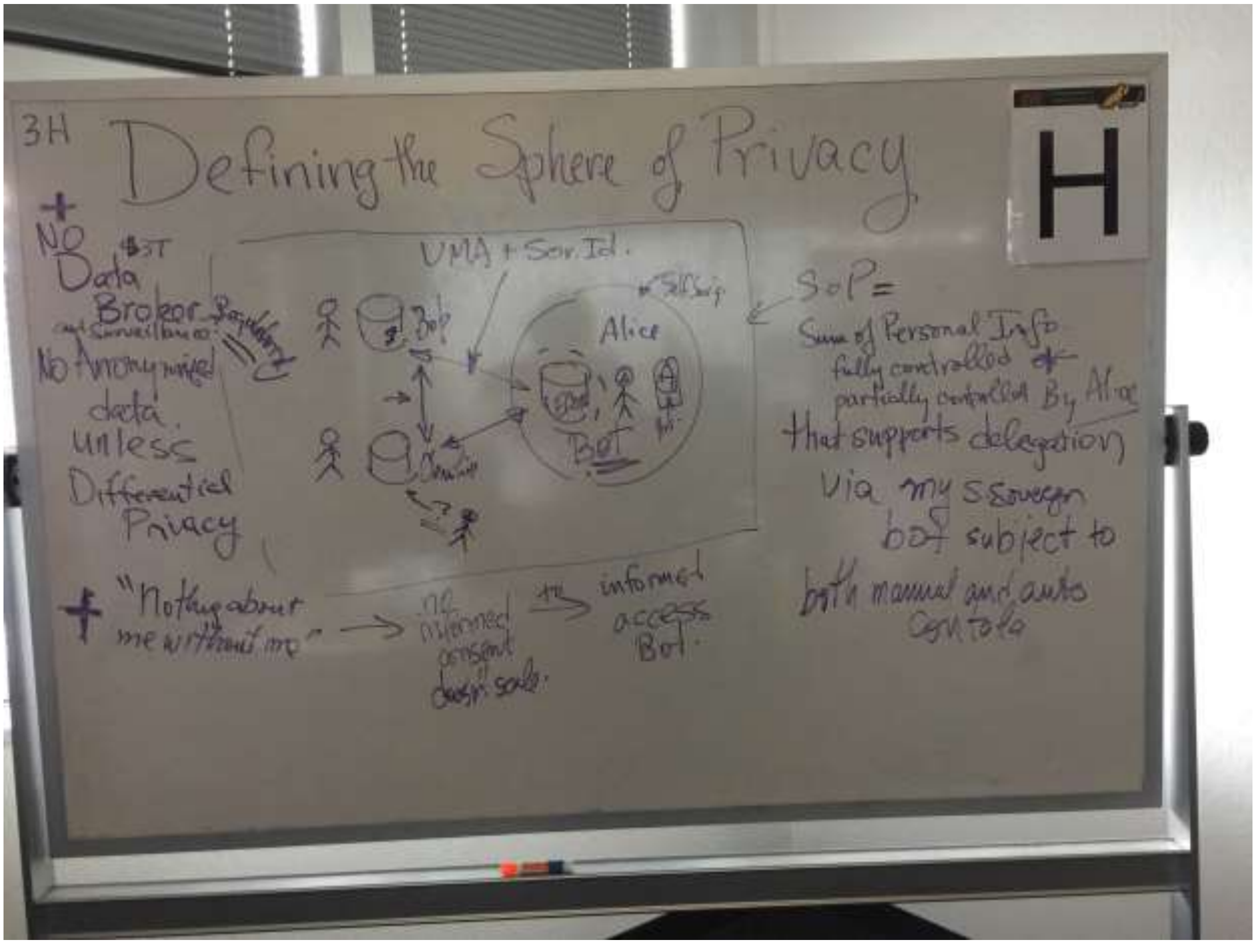
We discussed the different aspects of privacy and security for vulnerable populations - active duty soldiers are a vulnerable population and have similar identity requirements as other vulnerable populations - more security, who has access to identity information, how it is shared/given and what happens when concluding military service.

Defining the Sphere of Privacy

Tuesday 3H
Convener: Adrian Gropper
Notes-taker(s): Adrian Gropper
Tags for the session - technology discussed/ideas considered:

Identity Container, UMA, Self-Sovereign
Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

The Sphere of Privacy is the sum of personal info fully controlled by the subject plus personal info partially controlled by the subject, that supports delegation via the subject's self-sovereign bot, subject to both manual and automated controls.
Alice's Sphere of Privacy = Personal Info (fully or partially) controlled by Alice
Many details can be found at the ongoing open source reference implementation of this, using healthcare as the domain is at http://hieofone.org


3H
Defining the Sphere of Privacy
H
+
No Data Broker Regulatory and Surveillance
$3T
No Anonymized data unless Differential Privacy
UMA + Sov. Id.
Bob
Alice
Self Sov
Bot
Domain
SoP =
Sum of Personal Info
fully controlled +
partially controlled By Alice
that supports delegation
via my S.Sovereign
bot subject to
both manual and auto
controls
+ "Nothing about me without me" → informed consent design scale → informed access Bot.

Smart Contracts for Self-Sovereign Data

Tuesday 3I
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:

What is Self-Sovereign Data?

Portable Identifiers Portable Attributes Owner Controlled and Managed Decentralized

What is a smart contract

Block-Chain Rule Engine for terms and conditions and enforcement Riccardian Contracts Triple Entry Bookkeeping

Issues Forgetfulness Privacy (Third Party Correlation) Watermarking Enforcement

A lot of time was spent answering questions about block-chain and smart contracts

A use case was presented where a time-limit for use of data disclosed to a second party is included in a riccardian contract. A Riccardian contract is user readable text that can be executed by a computer such as JSON

The issue of enforcement or lack of enforcement was discussed

A request was made for more use cases of the types of terms and conditions that would be useful for data usage that could be the basis for forming smart contract.

Fast Fed and How to "Identity Enable" a Cloud Business Service

Tuesday 4A
Convener: Dick Hardt and Prateek Mishra
Notes-taker(s): Dick Hardt

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

Dick's Presentation – Click on 'View Raw"
https://bitbucket.org/openid/fastfed/src/master/FastFed%20OpenID%20Summit%20Fall%202016.key.pdf

Prateek's presentation – Click on "View Raw"
https://github.com/principalidentity/fastfed-use-case/blob/master/fast-fed-use-cases-04.pptx

Self-Sovereign Identity Container Deep Dive

Tuesday 4B
Convener: Daniel Buchner
Notes-taker(s): Daniel Buchner

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

Github draft here:
https://github.com/csuwildcat/ddi/blob/master/specs/container-overview.md

Help Me "Help" My Professor

Tuesday 4C
Convener: Kaliya Young
Notes-taker(s): Kaliya Young

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

Kaliya student at the MSIMS program at UT Austin.

I've been learning some "interesting" things at school. These include the below slide

____

The Notorious Three (now Four) Categories of Identifiable Information

What you KNOW
—-
What you HAVE
—-
What you ARE
—-
What you DO
____

I asked for help from the IIW crowd to figure out how to communicate the professor about the wrongness of the slide. Throughout the 12 years I have been working in the identity industry these have been referred to as the methods of authentication and NOT categories of identifiable information.

The suggestions included looking the absurdity of the statements themselves.

What you know - The list of things that include what one knows (presumably all the information in one's head)

What you have - All the things you have (presumably all items that one owns regardless of their ability to be identifying).

what you Are - looking at the science behind biometrics and how they work.

What you do - the way you type and your gate.

What you are and do only work if you are actually enrolled into a system. Other wise they just support correlation.

Understanding the Mosaic Theory of Identity
Looking up the ISO standards on identifiers that they are two kinds immutable and mutable
Understanding of Information Theory could help in debunking the error

What is Sovrin

Tuesday 4E
Convener: Phil Windley
Notes-taker(s): Scott David

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

Sovrin is a foundation to create distributed ledger technology
Permissioned
BItcoin blockchain is example of permissionless distributed ledger
Permissioned is Node that write to the ledger are known to the system.
Bitcoin blockstack enables distrib ledger to reach consensus. Use different mechanisms to reach consensus. Get problems like Sybil problem – addressed by miners.
Sovrin solves the Sybil problem by not letting there be unknown writers.
How get onto the list of who can write to the ledger.
In the production network – go through a process with the foundation to be a node.
Sovrin trust framework will run the network.
Need vetting – need to be let into it.
Sovrin foundation set up for public permissioned ledger for self sovrin identity and not other problems.
The known nodes is what makes it permissioned.
Whole class of permissioned blockchains – ripple, R3 are approaches.
Second word is public – distinguishes it from “private” network, like corda. Anyone can get an identity, but the nodes that validate the identity are known.
That is explanation of the “public, permissioned” ledger.
This is special purpose – for identity. Unlike Stellar which is not special purpose.
Permissioned part is why there is a SOVRIN foundation. Someone has to decide who are the nodes that can write to the ledger. SOVRIN selects nodes to decide who can write to ledger. This is primary purpose. IT does other things like outreach also, but this is main goal.
How do you reject bad actors. Every transaction you know how everyone voted If you voted against other nodes, threshold above. Intrusion detection like policy Network algorithmically protect against bad actors.

What percentage need for stability of system.
33% comes from byzantine generals algorithm. 2/3 of permissioned nodes threshold.
With bitcoin it is 51% of hash power.
Algorithm expects bad actors. Has a way to deal with it.
Foundation is structured so that the nodes have no identity whatever. Identities of system have complete privacy. Sovrin nodes have no privacy. Kirkoff's principle for identity.
One aspect of identity that is problem, is that different relying parties trust different things. DOD Might trust certain things in DOD, but not beyond. Is this a situation where SOVRIN foundation is trusted? Part of that is related to claims – question might be how do I trust a claim. But answer is that, yes, you need to trust the nodes. Software being run is open source. All in a trust framework that is transparent. Need to trust that nodes are doing the right thing.
Consensus system not depend on a single point of failure. If distributed then like an insurance pool. Risk of loss is reduced. If concerned about sovereign. Single point of failure is node selection process. Need to trust the SOVRIN.
What are the ways to check the code (code reviews). Need enterprise corporate governance, etc. Need competent audit and other functions.
Why permissioned? Performance: Permissioned use less computational power to do transactions. Also, at banks and healthcare – liked the permissioned model.
There will be lots of distributed ledgers used for different things. This is potentially useful for identity systems.
Financial organizations are starting to look at this as a model for identity.
The intention of these presentations is to solicit help with SOVRIN foundation.
Change of topic:
What mean by "SOVRIN is an identity network" at a high level.
Imagine that have an "identity" for Jane. There is no one real thing. It is in a ledger and distributed, etc. But Jane with think of these things as correlated with her.
Jane wants to create relationship with her bank Bank has set of keys.
Jane creates an identifier and gives the public part of the key pair to the bank. The ledger is helping Jane manage the PKI and what is happening there. Jane can have the banks key so that she knows when talking to the bank, all within normal public private key pairs.
When Jane has relationship with state government, Jane create separate key pair for the government. Create different key pairs for each entity that Jane interact with. Even if they wanted to correlate the key pairs, they cannot.
Jane can iterate those key pairs multiply.
Q: If Jane is human rights worker in Cambodia, but need two identities. Can manage two key pairs for each entity. There is no link other than Jane's linkage of the different relationships.
If Jane wants to get a job, and apply for work at employer. She may want to use claims that she has E.g., claims that are self asserted (from government, school and bank e.g.,) wants to tell them about bank, school transcript and state authority. They are all verifiable claims by the various entities with which she has the key relationships.

Jane creates a proof which she translates to the potential employer. That proof not provide all claims, just the ones that she want to share with the potential employer.
With proof, Jane can create proof that other organizations can use and rely upon.
Note that claims are all revocable.
Note that the employer got all the proofs.
She uses that address claim to show the employer that her information is provided to the bank.
There is a use ability to transfer claims to third party, based on relationships to the third parties.
User as the information arbitrage traffic cop.

Note that when written to the ledger – could be on the ledger, or off the ledger.
who controls the ledger. IT is distributed. Who controls what is written to them – stewards control what is written, SOVRIN cannot change the ledger.
Suggested enhancement to SOVRIN foundation would be to changes to code being in the changing pool.
Predictive market in front of an "actual" market.
Rules about how that happen.
Governance process can be deployed here from other conflict of interest contexts to mitigate the risk of code change control.
Why do you need a distributed ledger? Premise is true – Distributed ledger is a solution, but expensive one. Without distributed ledger, what is the way that I can have a self sovereign identity?
Precondition of this system is robust key matching. If have good private key management, cant you do this separately.
Do you need self sovereign identity or not. What do you mean by self sovereign identity?
Not need bind the concepts this way.
Decentralized ledger "own" the identifier"
DMV issues you a drivers license number, thing they are binding you to is the identifier.
How do this without your own hardware.
I have no pieces of paper – restore identity – no standard for identity.
Possibility of the confusion of my perception of me and your perception of me (external perceptions of identity and internal senses of self). I have ability to reassert external perceptions of me in the SOVRIN context, which is a new authority.
Social login and reusable identifiers. Claims are the transactions that drive this way past social login.
Banks and credit unions do KYC – they are interested in using claims more subtly and broadly.
How do you initialize this model – see next session.
What is the reason that it needs to be a ledger (like distributed hash tables, etc.). can it be distributed and not be a ledger.
Whoever has the power to pull the plug, creates a silo. If some other entity can pull the plug, then have silos, so not have user sovereignty.
One horizontal layer is me – person as the courier, holder of truths about the claims.. then the silos don't have to talk to each other.
Why need to be ledger – just accounts over time. Important if going to check time, auditability, immutability, etc.
Does this enable, pairwise, single sign on under user control.
People ask – why not use bitcoin, why not use ethereum – part of the answer is performance difference. Other issue is trust. Many are uneasy about a permissionless system. They want to know who is in the system.
Banks need the trust anchor – trust anchor opens up to questions of national sovereignty, etc. This is why there will be multiple ledgers and systems.
Private key management is a big problem. If lose the keys.
Big problem is the loss of the key. There are discussions going on about how to generate the key recovery.
Big problem is the UI.

Intro: User-Managed Access

Tuesday 4G
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:

Here are the slides I presented.
http://www.slideshare.net/CloudIDSummit/cis-2015-user-managed-access

Signed and Revocable Biometrics

Tuesday 4I
Convener: Jonathan McHugh
Notes-taker(s): Jonathan McHugh

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

Problem

- Easily pirated and/or stolen raw biometric data
- Inability to revoke data if breached

Definitions

- Template versus raw biometric data
  - Template - representation of biometric data
  - ??Raw - actual biometric data
- Identification versus authentication
  - Identification- confirming the person in front of you is that person
  - Authentication - confirming the entity attempting access is that entity

Discussion

- Defining whether we are talking about biometrics for identification versus authentication
- Whether biometrics are too easily breached or mimicked to be useful
- Methods for revoking biometric data
- uPort on Ethereum using smart contracts for revocation versus traditional methods mentioned as an alternative
- The mass breach at OPM was mentioned as an example of why this can be an issue
  - Those biometrics as well as a good deal of other PII is now in the wild without a means of revoking it

Conclusions

- Need for multiple factors for authentication
- Signed revocable biometrics are still untested and new
- In order to get highly reliable biometrics, use of retinal scans mentioned
  - Very expensive
  - Somewhat invasive
  - Technology not there yet

Security Event Token 101

Tuesday 5A
Convener: Marius Scurtescu
Notes-taker(s): Marius Scurtescu

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

Presentation link:
https://github.com/independentid/Identity-Events/raw/master/SecurityEvents101-IIW23.pdf

- clarification if SET only describes events or also deals with distribution
  - both, session for distribution tomorrow
- is JWT signature really optional? probably not
- query interface use case, around registration, pub/sub does not work
- account suspended event should also have a corresponding account restored event
- event order can be mittigated by adding event time stamps
  - VM time is not reliable
  - sequence numbers are not feasible with move towards decentralization
  - pointing to previous evnets when current one is issued is also problematic, leads to graph of events
- why numtiple identifier for user in password reset example
  - sub is in name space of issuer, other identifier nested in event sub-message
- is batching supported?
  - some changes could generate a massive ammount of evnets, this is when batching would be useful
  - batching at event level vs transport level
- logout example, nested iss
  - real world use cases
  - care with session identifiers, may not be useful
  - multiple devices use case
- why not nest event detaisl in the "events" attribute?
  - events could be an object, keys are event URIs, values are event sub-objects
  - events could be an array, each element is an event sub-object
  - current solution popular and inspired by SCIM
- what prevents these SETs from being used for authentication as Id Tokens?

Syntax change proposal from Justin Richer:

In the session at IIW yesterday, there was a discussion on the event syntax in the current proposed draft. A few of us (myself included) questioned the current structure which is something like this:

```
 {
  "jti": "3d0c3cf797584bd193bd0fb1bd4e7d30",
  "events":[
   "urn:ietf:params:scim:event:passwordReset",
   "https://example.com/scim/event/passwordResetExt"
  ],
  "iat": 1458496025,
  "iss": "https://scim.example.com",
  "aud":[
   "https://jhub.example.com/Feeds/98d52461fa5bbc879593b7754",
   "https://jhub.example.com/Feeds/5d7604516b1d08641d7676ee7"
  ],
  "sub":"https://scim.example.com/Users/44f6142df96bd6ab61e7521d9",
  "urn:ietf:params:scim:event:passwordReset":{
   "id":"44f6142df96bd6ab61e7521d9"
  },
  "https://example.com/scim/event/passwordResetExt":{
    "resetAttempts":5
  }
 }
```

To get the above information, I need to walk through the values in the “events” array and then look for those values as members of the root JSON object to see if they have data. Instead, I’d like to raise an alternative way to codify the same event in a way that I believe will be more easily understandable by implementors and easier to parse by both humans and code. Namely, skip the array definition and build out the event above like so:

```
  {
   "jti": "3d0c3cf797584bd193bd0fb1bd4e7d30",
   "events”: {
     "urn:ietf:params:scim:event:passwordReset":{
      "id":"44f6142df96bd6ab61e7521d9"
     },
     "https://example.com/scim/event/passwordResetExt":{
       "resetAttempts":5
     }
   },
   "iat": 1458496025,
   "iss": "https://scim.example.com",
   "aud":[
    "https://jhub.example.com/Feeds/98d52461fa5bbc879593b7754",
    "https://jhub.example.com/Feeds/5d7604516b1d08641d7676ee7"
   ],
   "sub":"https://scim.example.com/Users/44f6142df96bd6ab61e7521d9"
  }
```

With this syntax, I need to loop through the keys of the “events” object and don’t need to reference anything else in the root object. This is *much* easier to code, and it enforces that each event key appear only once. Plus it keeps event information out of the root of the JWT, which has been shown (with JAR, dynamic registration’s software statements, and a couple others) to be problematic at times.

An argument for the current syntax is that it can handle event types that don’t have any additional payload. While I don’t think I’ve seen a concrete example of one yet (I might just be missing it), we can still handle that in this syntax in a number of ways. First, we could just use an empty object when there are no arguments.

```
   "events”: {
     "urn:ietf:params:scim:event:passwordReset":{}
   },
```

Second, we could just use “null”, which OpenID Connect uses in the “claims” object:

```
  "events”: {
    "urn:ietf:params:scim:event:passwordReset”:null
  },
```

Or a stand-in value like the “true” boolean:

```
  "events”: {
    "urn:ietf:params:scim:event:passwordReset”:true
  },
```

I prefer the first as it doesn’t change the expected object model for all claims, and it also takes fewer characters on the wire (not by much, so that’s not a driving factor, but with a lot of these saving a couple bytes won’t hurt).

— Justin

Full thread at:
https://mailarchive.ietf.org/arch/search/?email_list=id-event&gbt=1&index=EZJO2uiOOF0MZgbLBzkUWuNITkE

Self-Sovereign Support Technology

Tuesday 5F
Convener: Adrian Gropper
Notes-taker(s): Vivian Shen

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

About Adrian: Full-time Patient Privacy Rights advocate for processes that preserve the self-sovereignty.
Try to apply the standards and policy in this context of technologies that is entirely own by an individual.
Definition of Self-Sovereign
1) an implant or defibrillator,
2) a bot that act on your behalf because you are paralyzed,
3) a robot in your house that have a lot of power over your aging mother
So who do you trust? Some of these things you don’t trust anyone or the person that recommends but it will not go to the Cloud where a Metronics. Technology that is so personal that it is completely owned by an individual.
3 kinds of SSS Technology:

- **DID – decentralized identifier** that not tied to a certificate authority instead it is tied to a blockchain, it can be associated with your reputation, tied to Blockchain. Not complete self-sovereign. Trust independent of DMV or Facebook. It enables SSS.

- **Mobile- Biometric and secure element** e.g. Apple Pay or Apple Healthkit. Apple will not see your data. Data on your mobile device but the Apple vendor does not see data, private key and it is link to biometric. Now you have a SSS. This authenticate your identity but also non-repudiable. Like Apple Pay because it is linked to your finger print.

- **Bot – authorization automation** – Now what can you do with DID and Mobile? You can have a Bot or delegation to act for you where you are asleep or out of range. An agent that is SS to you. It is non-repudiable or relatively non-repudiable. In the long run, the Bot will have machine intelligent. Sirius will manage how much it is to call home or does it on the phone. Alexa has different partition. The Bot represents that represent the thing that is online as a server but is linked to your Mobile for control purpose but it is not your mobile because it is offline. (**AI, Broker vs agent, policy source you inherit, policy UI)**

- **Reliance Documents** (birth, death certificate), Rights benefits Privileges (100 people can have the same birth record). -> Meaning, how do we properly notarize authoritative, or trust-anchor claims (repudiate or dispute)

- Ability to assert facts <u>without revealing the underlying information</u>

- **…. – what else?**

Is Bot a broker or agent?
Bot is a broker. In terms of AI, it is a broker. Traditional, it is a human broker, legal, financial. Tell the rule to give to people. If $300, fix it. Today, the Bot maybe sufficient but sometimes with self-driving, the Bot will inform human that it needs help. So it is a hybrid. Real-estate broker vs Doctor, lawyers are agent. Concierge is not a broker. It is an agent. I tell you what I want in simple language. I want certain job or opportunity. I want that within parameters.

Principles of Self-Sovereign Identity

Tuesday 5G
Convener: Joe Andrieu
Notes-taker(s): Garrett Schlesinger

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

Chris Allen's writeup here:
https://github.com/weboftrustinfo/self-sovereign-identity

Security

1. Protection
2. Minimization

Controllability

1. Existence
2. Control
3. Persistence
4. Consent

Portability

1. Interoperability
2. Transparency
3. Access
4. Portability

In Europe, there is the possibility of adopting these principles into privacy frameworks.

Goal: at least make this a pledge to define self-sovereign identity.

Joe Adrien: important aspects are: Control, Acceptance, and Cost/Access
Control: Self-generating, opt-in, non-participation, opt-out (remove my data or tell me why you can't), recoverable,
Acceptance: standard, simple, technology free, public ledger (alternatively: trust anchor/non-repudiable), reliable, substantially equivalent ("at least as good as what's already there")
Cost/Access: license + use, financial, cognitive (masses need to be able to understand why this is secure)

Question: what problem does self-sovereign identity solves? 1) administrative-issued identity (ex-employee disappears, refugee coming into a new country, no abstract representation of self in a lot of these instances), 2) Credentials can be held by an outside agent with no recourse to recovery. The most important thing: who is the authority/who controls our history and everything that we have done? Non-correlated identities: you should be able to not have links between your identities in different contexts unless you want them.

Can transparency sometimes be a bad thing?

Correlatable identities: multiple parties correlating partial identities. Non-correlatable is challenging if not impossible, but it is desirable. Best we can do right now is minimization.

Want to cross international borders without losing control.

Resilience
Stewardship/Custodianship
Non-correlatable identifiers
Purpose bindings
Contractual obligations

A big point: right now, the scales are so tipped in the direction that compromises user privacy that it is much better, in crafting an ideal identity management system, to err on the side of more user privacy.

Perfection can also be the enemy of the good. Can we make incremental steps toward identity sovereignty? Can we at least make this an expression of our goals and make the intentions clear?

Where is the business model? Really in the tooling that accretes identity information and handles identity claims.

What are the practical applications?
What is it, really? How does it fit? Reputation? How does it filter bullshit?
The simplest version is: if you control your private key, you can use that in other contexts and link it as you choose.

Self-Sovereign Digital Identity for Kids

Tuesday 5I
Convener: Shaun Conway
Notes-taker(s): Bryan Pon

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

Situation:

- Consent is trying to onboard large population for Barclay's in South Africa
- For government-approved subsidy claims
- 750k children that need records
- As a service provider, what is the obligation, what would be the right way to onboard these youth?

Challenges

- Custodianship
    - Kids under 18 (or legal age) can't legally sign off on T&Cs
    - Also seniors/elderly may need care
    - In Global South, fewer kids have custodians
- Biometrics are challenging—Consent has tested fingerprints, facial scan, both failed
    - Suggested ongoing biometrics at regular interval
    - Include a key along with the biometrics for increased correlation
    - Margin of error for biometrics
- Regulations around child protection
    - e.g., COPPA which precludes collecting any data on kids under 13
    - Onboarding -- age verification requirement; kids often lie
    - EU GDPR includes ideas of car-owner as parent-child relationship
- Safety -- interactions between minors and adults online, may need to scramble/encrypt identity to protect child
    - Need a mechanism to protect the most vulnerable kids; need to have checks in place so kids don't compromise themselves or their own safety
    - Need to bake in privacy-first, privacy by design
    - Online safety should be in context of other risks, and an empowered child is a safer child
- Role of digital literacy

- Once youth reaches legal age, how do you transfer complete control back to the youth
    - Youth might also want to delete old data
- Possibility of institutions--school, church, etc--could play a role custodial role
- Privo -- organization advocating for youth
- Who decides what data to collect?
- Can children manage a self-sovereign identity?
    - Maybe children can't be "self-sovereign" maybe it is a "collective-sovereign" or custodial-sovereign
    - Maybe custodians are required for some actions (onboarding) but youth can manage and perform certain actions without custodian
    - Sami has used a number of different identities signing up for different websites, services; says kids are already used to circumventing age controls
- Vulnerable populations
    - Challenge of LGBT or trans kids who find a community online might actually want to keep this "identity" private from their parents
    - Does this all apply just as much to other vulnerable populations? seniors? mentally disabled?
    - Should there be different needs for different ages or stages of vulnerability?
- Need to be cognizant of the Western perspective of our group in terms of views on privacy, safety, etc.
- Bill mentioned possible tie-ins to his session at last IIW on identity lifecycle
- More curators a child has, makes things more transparent, and limits the possibilities of bad things happening
- Child-centric identity!

Standards for Internet of Things

Tuesday 5K
Convener: Dave Sanford
Notes-taker(s): Dave Sanford and Ryan Page

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

Dave's Notes:
Session was called to explore the implications and possible opportunities caused by the recent DDoS attack on Dyn (and thereby Dyn customers) caused by a botnet of IoT devices. The sense is that this was so public that the long standing IoT device security problem may receive enough public scrutiny that regulatory responses are likely. Is there any guidance that we as a community can provide that could either a) avoid bad regulation or b) help fix the IoT space which is recognized as broken in terms of security and in other ways.

One of the motivations for the session was a well attended session on the use of OAuth to help integrate security in the IoT space that George Fletcher had in 2014. Dave Sanford posited that - OAuth use in this way could help heal the home IoT space.

Conversation turned to the critical role of routers as firewalls in the home IoT space - as a potential focus given the multitude of low cost IoT devices some of which are made by foreign manufacturers for which little regulatory pressure might be possible. There was some discussion of Underwriters Labs (UL) based security standards that could be used to support regulatory and import requirements.

It was expressed that more critical abuse cases than use of IoT devices for DDoS attacks are likely to cause regulatory response - particularly as the IoT ecosystem includes medical devices, cars, etc. DDoS may not be the inevitable event that will cause regulatory response.

One of the reasons that the IoT space is broken and it would be hard for smarter devices (routers, messaging hubs) in the home IoT space to protect the cheaper, dumber devices is due to lack of interoperability. There is little impetus for the various players that want to become the dominant IoT hub in the home to work together to create standards (including security relevant standards) by which all devices can be protected by all IoT devices.

There was discussion about the fact that devices are manufacturer vs. user centric, expecting to communicate directly with manufacturers. Also conversations about the need for automatic provisioning. David Fotland (Amazon) talked a little about Amazon IoT specifications and that Amazon already uses OAuth for all devices. Overall no conclusions that would lead to future actions - but great discussion.

Ryan's Notes:
We discussed methods of protecting against attacks using IOT devices. There were distinctions between super-dumb devices vs. devices that can be updated with software pushes, distinctions between devices behind consumer or industrial routers/firewalls, and devices in the wild or that have their own cellular connectivity.

Potential avenues of remediation:
- pushing software remediation to devices, either to limit points of communication or pushing use of a specification like OAuth 2.0
- updated firewalls or routers restricting protocols or frequency of traffic
- regulatory regime requiring minimum security controls and/or behaviors on regulated devices
- implementation of interoperable standards for device communication
- use of contact based authorization or de-provisioning for devices in the home (e.g., NFC)
- regulation or liability for carriers who fail to intervene in managing traffic (but see "there goes net neutrality")

Wednesday October 26

SMS for 2-Factor Authentication

Wednesday 1A
Convener: Sean Brooks and Jim Fenton
Notes-taker(s): Tom Brown

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

NIST - part of Dept of Commerce
Broad adoption outside of government (nonprofits, academic institutions)
So, important to get public feedback

NIST SP 800-63-3 https://pages.nist.gov/800-63-3/sp800-63-3.html

In new version, deprecating SMS for out of band authentication mechanism

Deprecation - when we released public draft, lots of articles about "NIST banning use of SMS for authentication"

Not saying that fed agencies can't use - just trying to signal to market that we don't see SMS as a reliable option for 2nd factor

Not forbidden from using it

In the technical standards space, it is always a surprise when the media picks up anything at all

NSTIC wrote a clarifying blog post

The idea was to give the marketplace a heads up

SMS is cost effective for many orgs

SMPP (peer-peer) widely used not particularly secure

SS7 - designed w/o particular security, used among carriers, not accessible to as many potential attackers as internet

social engineering attack on carrier:

"I lost my phone & need to buy another one"

sales person motivated to sell phone but not particularly skilled at verifying identity

FTC: in 2013, 1083 reports of this attack representing 3.2% of identity fraud attack

reported attacks doubled since then. (actual number of incidents unknown) high profile victims of this attack:

1. Deray McKesson via Twitter
2. Ladar Levison

phishing ("verifier impersonation attacks") is not at the same assurance level.

Document recommends that relying parties check to make sure it is a mobile phone rather than voice-over-ip

we are not singling out sms. document also nixes knowledge based authentication (kba) (e.g. what is the name of your dog?)

we cannot necessarily point private entities to any specific technologies but do mention five or so other mechanisms

Ubiquity and familiarity make SMS attractive. just because someone has a smartphone doesn't mean they understand it.

SMS is not 100% accessible, especially in rural areas

deprecating something isn't meaningful unless there is an alternative

deprecation in the document means: if you can find a better way, you should consider doing it.

if iphone is on, phone will forward message to the icloud

eurograbber malware snagged sms message on phone and sent it off to attacker who could front-run authentication

phone is intended to be "something you have". we've been using sms to prove you have the phone

alternatives: 1 time password device, crypto token

signal messaging service will detect if you move account to different device by checking device's fingerprint

some carriers have apis to determine how long a telephone number has been associated with a specific device.

providers can integrate with carrier apis to verify IMS (sim card) and IME (handset)

PIP standard for fed employees instead of sms

duo, fido tokens, google authenticator

webauthn in w3c to integrate fido in browser experience

federal gov & innovative technologies don't always mix as things take a while

Tutorial PBFT

Wednesday 1B
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:

Slides are at:
https://github.com/SmithSamuelM/Papers/blob/master/presentations/Distributed%20Consensus.pdf

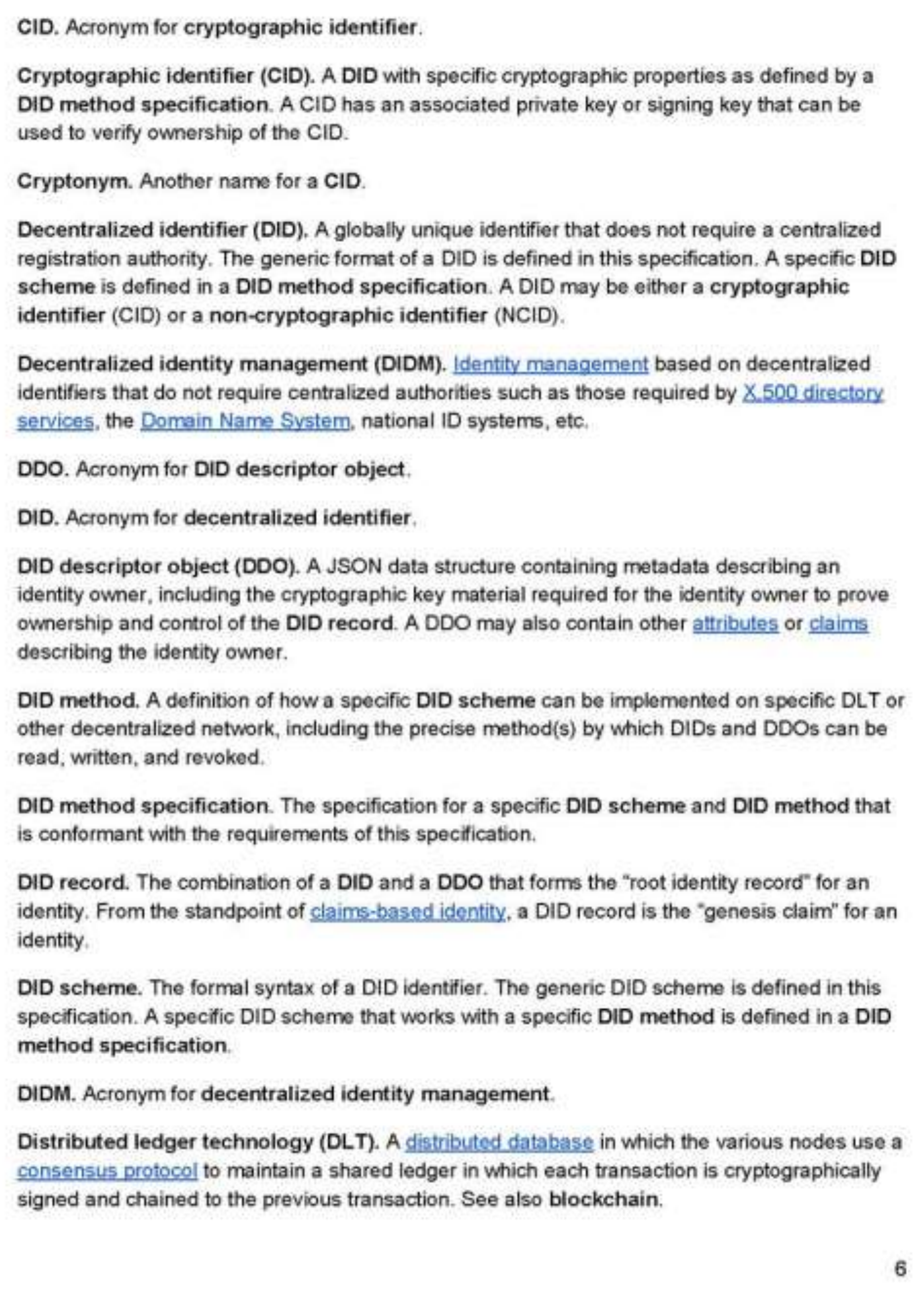
Decentralized Identifiers Spec

Wednesday 1C
Convener: Drummond Reed
Notes-taker(s): Jonathan McHugh

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

- Some endpoint terms
  - URL - Uniform Resource Locator
  - URI - Uniform Resource Identifier
  - URN - Universal Resource Name
    - Persistent but Non-referenceable
- DID solves these problems
  - Persistent but referenceable
  - Decentralized Registration
  - Cryptographically verifiable
  - Thought: Self-sovereign not possible w/o above
- DDO - DID Descriptor Object
- DID can refer to anything
  - People
  - Organizations
  - IoT
- Why not URL
  - Possibly not reliable
  - Owned and controlled by an entity
- Zookos triangle
  - Human readable | Unique | Decentralized
  - Holds that only two of these can be satisfied
- DID Naming layer is still up in the air if it will be included
- Example DID and DDO
  - Sovrin | Bitcoin | Ethereum (uPort)
  - Done via methods
    - "did:sov:{26 characters}"
    - "did:btc1:{record block and transaction id}"
    - "did:eth:{smart contract id}"
  - EquivID
    - Reference to other DIDs

Extras – Link to Draft and Glossary of terms - Below
Link to draft: https://github.com/WebOfTrustInfo/rebooting-the-web-of-trust-fall2016/blob/master/draft-documents/DIDSpecificationWorkingDraft04.pdf



CID. Acronym for **cryptographic identifier**.

Cryptographic identifier (CID). A **DID** with specific cryptographic properties as defined by a **DID method specification**. A CID has an associated private key or signing key that can be used to verify ownership of the CID.

Cryptonym. Another name for a **CID**.

Decentralized identifier (DID). A globally unique identifier that does not require a centralized registration authority. The generic format of a DID is defined in this specification. A specific **DID scheme** is defined in a **DID method specification**. A DID may be either a **cryptographic identifier** (CID) or a **non-cryptographic identifier** (NCID).

Decentralized identity management (DIDM). Identity management based on decentralized identifiers that do not require centralized authorities such as those required by X.500 directory services, the Domain Name System, national ID systems, etc.

DDO. Acronym for **DID descriptor object**.

DID. Acronym for **decentralized identifier**.

DID descriptor object (DDO). A JSON data structure containing metadata describing an identity owner, including the cryptographic key material required for the identity owner to prove ownership and control of the **DID record**. A DDO may also contain other attributes or claims describing the identity owner.

DID method. A definition of how a specific **DID scheme** can be implemented on specific DLT or other decentralized network, including the precise method(s) by which DIDs and DDOs can be read, written, and revoked.

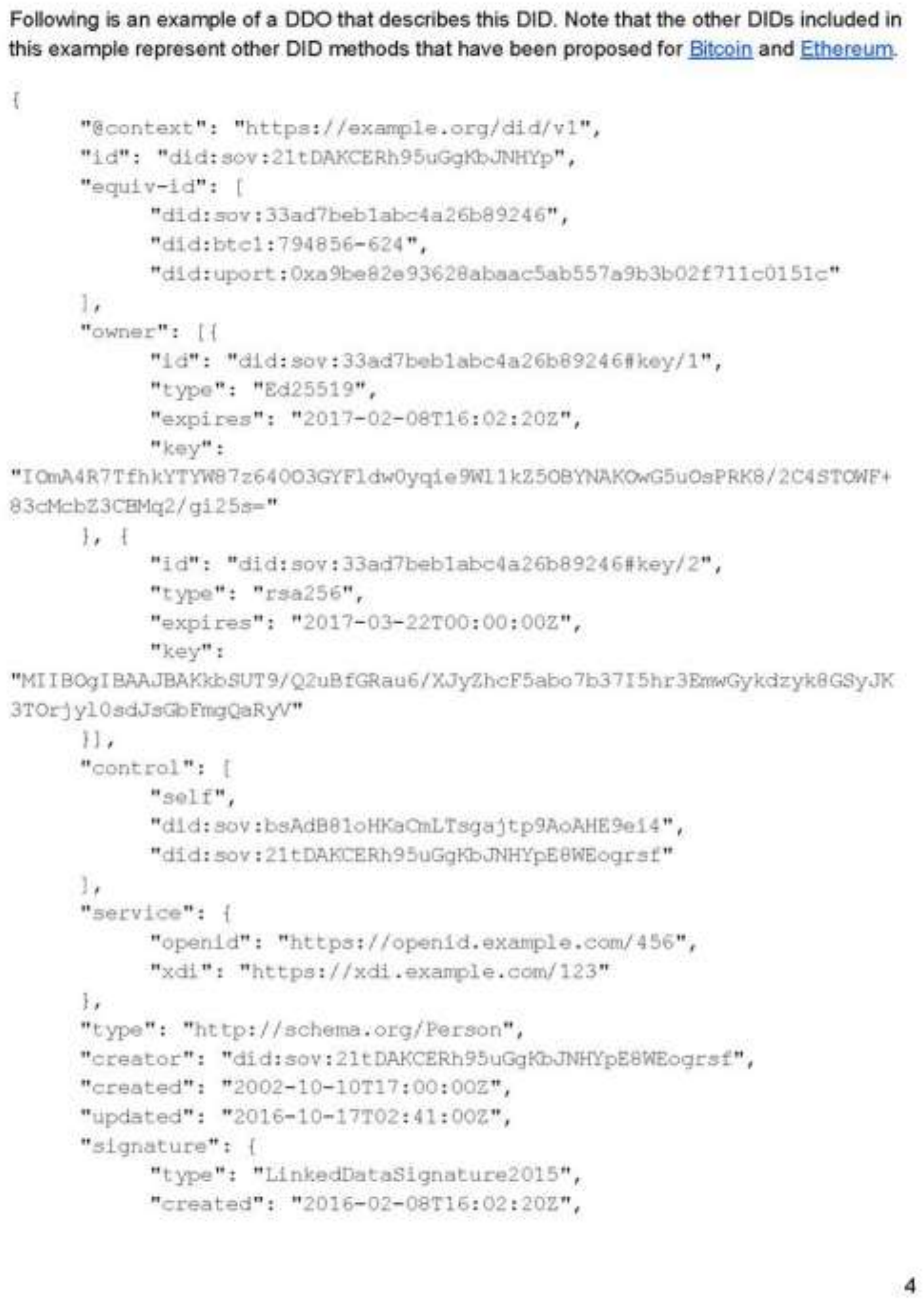
DID method specification. The specification for a specific **DID scheme** and **DID method** that is conformant with the requirements of this specification.

DID record. The combination of a **DID** and a **DDO** that forms the "root identity record" for an identity. From the standpoint of claims-based identity, a DID record is the "genesis claim" for an identity.

DID scheme. The formal syntax of a DID identifier. The generic DID scheme is defined in this specification. A specific DID scheme that works with a specific **DID method** is defined in a **DID method specification**.

DIDM. Acronym for **decentralized identity management**.

Distributed ledger technology (DLT). A distributed database in which the various nodes use a consensus protocol to maintain a shared ledger in which each transaction is cryptographically signed and chained to the previous transaction. See also **blockchain**.



Following is an example of a DDO that describes this DID. Note that the other DIDs included in this example represent other DID methods that have been proposed for Bitcoin and Ethereum.

```
{
      "@context": "https://example.org/did/v1",
      "id": "did:sov:21tDAKCERh95uGgKbJNHYp",
      "equiv-id": [
            "did:sov:33ad7beb1abc4a26b89246",
            "did:btc1:794856-624",
            "did:uport:0xa9be82e93628abaac5ab557a9b3b02f711c0151c"
      ],
      "owner": [{
            "id": "did:sov:33ad7beb1abc4a26b89246#key/1",
            "type": "Ed25519",
            "expires": "2017-02-08T16:02:20Z",
            "key":
"IOmA4R7TfhkYTYW87z640O3GYFldw0yqie9Wl1kZ5OBYNAKOwG5uOsPRK8/2C4STOWF+
83cMcbZ3CBMq2/gi25s="
      }, {
            "id": "did:sov:33ad7beb1abc4a26b89246#key/2",
            "type": "rsa256",
            "expires": "2017-03-22T00:00:00Z",
            "key":
"MIIBOgIBAAJBAKkbSUT9/Q2uBfGRau6/XJyZhcF5abo7b37I5hr3EmwGykdzyk8GSyJK
3TOrjyl0sdJsGbFmgQaRyV"
      }],
      "control": [
            "self",
            "did:sov:bsAdB81oHKaCmLTsgajtp9AoAHE9ei4",
            "did:sov:21tDAKCERh95uGgKbJNHYpE8WEogrsf"
      ],
      "service": {
            "openid": "https://openid.example.com/456",
            "xdi": "https://xdi.example.com/123"
      },
      "type": "http://schema.org/Person",
      "creator": "did:sov:21tDAKCERh95uGgKbJNHYpE8WEogrsf",
      "created": "2002-10-10T17:00:00Z",
      "updated": "2016-10-17T02:41:00Z",
      "signature": {
            "type": "LinkedDataSignature2015",
            "created": "2016-02-08T16:02:20Z",
```

Wells Fargo: Never Again

Wednesday 1F
Convener: Marc Hochstein
Notes-taker(s): Karin Marr, John Best

Tags for the session - technology discussed/ideas considered:

Wells Fargo, UMA, SOVRIN

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

Marc Hochstein - Editor American Banker
Using identity to prevent this from happening again.
Not don't do evil / CAN'T BE EVIL
What are the three things that should've caught this and how did they fail.

- Explicit Consent - formal process that is enforced
- Notice - Gave consent
- Audit - Making sure consent was given to the right Explicit consent

Follow HIPAA (in writing and signed)?

Was there a comparable law that was violated?

- Issue was an account created and on behalf of customer that CC was created with digital signature (based on account). When customers got card the recommendation was to ignore the card or just hang onto it. So customers were notified.

ISSUES/Solutions?

  - INFORMED - lack of information until after the card was established
  - SUCCINCT push notification - on the phone.

Problems:

  - The information is overwhelming when you get a new card
  - We don't have market by market privacy policy standards
  - Structural change in the legal structure??

This was a sales incentive gone wild - so do you create a different incentive that can't go down this road? They counted on the customer confusion.

Consent was "falsified", the notice was overwhelming and the audit favored the sales incentive.

Call centers were also incentified… and a part of this

Was there a mechanism to legally obtain a digital signature - not really - but the call center, drive-throughs, etc. all had these initiatives

Should there be parameters that are affiliated with an account? Besides UN/PW or email address where my relationship is controlled by self. Today all my accounts are not displayed on the first page but rather all over (indicating some are buried). Do we know anything other than UMA that can do this? Who provides these services? FDIC (for banks)? Loss was trust but also may have affected credit score.

- Model: Don't make the whole thing pivot on alerts - so that I inadvertently select
- Revocation is something that exists - maybe have it as "ACCEPT"

- (Justin) - authorization server has opportunity to query the consumer - OAUTH - but then the alert situation is possible but if can then later revoke, that option should be doable
    - UMA solves half the problem (2 pcs)
        - User Interface - that is consistent - check
        - Resource scopes - NOT - are not uniformed (mechanism allows (in OAUTH) limited right of access (subset of rights rather than all or nothing)

What's toted as a feature (Blanket open to any and all types of accounts) is actually not and the solution would be to require consent for all types of accounts

Is revocation (UMA) the solution? (Adrian) - UMA allows for revocation - but does have a UX standard in the implementation (doesn't have to be implemented). Maybe works at the implementation but not at the consumer level.

"Docusign" - I give it digital signature and then I can use for all financial "signatures"

UMA isn't the agreed upon solution though so should not move on. We can make some standard technology changes, but until we have some level of abstract at User level, it’s the same as the 10 page legalese issues. Technology cannot solve all of this

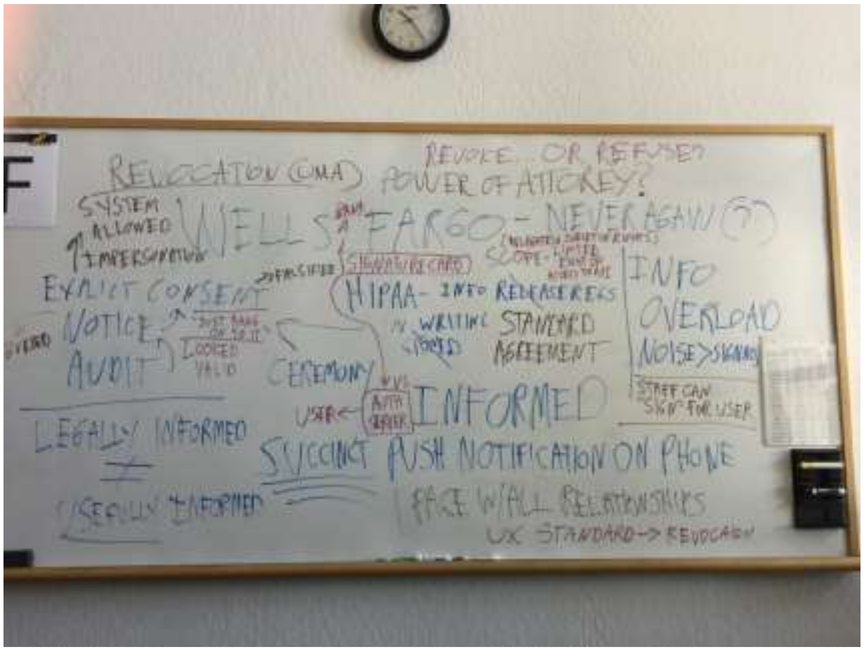
It’s the optimization (exploitation really) (see toted) - that went bad.
The issue is How they gained consent - by just getting one signature card. Revocation really says that "I as a consumer originally consented and now I want to revoke" rather than saying "I never authorized in the first place".

Should the consumer control the signature card? Institutes own the resource servers - so the institutes would own UMA - but UMA is a protocol - UMA tries to improve the relationship. Fiduciary information services - these services by law can only be responsible to the individual and not the institute.

(Justin) Everyone having an authorization server is not the solution? I can run my own, I can pay someone or pay in trade? UMA does not deliver this.

Some sort of legible agreement for consumer, outlining consent and options, and accounts. Should be similar to when you change password - you get notified that you did so after the fact.

Summary
The failure in the Wells Fargo system was related to not having a system with a clear notification process to inform the customer that a new account was opened on their behalf. The current system allowed staff to open accounts on the behalf of customers without their explicit consent. To auditors these accounts would look legitimate because of the controls in place had been satisfied.
Sovereign identity was also discussed, using the model of getting direct permission from the customer by getting their attention on the phone and having them agree to the opening of the account via Biometric.
All agreed that the breakdown in the explicit consent was the root of the problem. Also it cannot be ignored that inherent intent to do “bad” that was pervasive in the Well Fargo culture allowed it to grow to enormous proportions.
Picture of White Board



Ways to Use the Films

Wednesday 1G
Convener: Heather Vescent
Notes-taker(s): Joe Andrieu

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

Ways to promote the various IIW documentaries made by Heather.

0. Publish on Vimeo/Youtube
  SEO
  Canonical URLs

1. Press Release
Target anyone who has written about digital/online identity

2. Personal sharing announcement: Here's my movie
  ID Commons
  Project VRM

3. IIW Community Outreach
  Website
  Email 1: Here's the movie we made
  Email 2: A month later, Phil/Kaliya "For those of you who have been to IIW, Here's a great way to reach out to folks who might be a good fit for coming to IIW"
  Email 3: In promo for next IIW, Kaliya/Phil "If you know anyone considering coming to IIW or who SHOULD be considering it, point them to Heather's documentary."

Unconferences in More Fields

Wednesday 2A
Convener: Kaliya Young and Bill Aal
Notes-taker(s): Kaliya Young

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

Kaliya hosted this session to share with folks considering what would be involved to convene an IIW like event for their industry.

The session started with a review of who was in the session and why:

- wanting to learn more about how to do it…
- Transdisciplinary Research Teams
- Artificial Intelligence and Machine Learning - Ethics of the Algorithm
- IoT those ID's are in Finish Unconference
- Patient ID Debates
- First Experience with an unconference and have a backgroundd in ID& Health in the context of the theater of war.

When we work with clients starting to plan an unconference we begin with questions including:

What are/is the goal of the organization(s) hosting?
What are the goals of the proposed convening/
Who is coming - what are their needs/interest / profile.

What are the needs of non present stakeholders (could be sponsors, constituents).

Then working with the client's initial answers to questions around

How many people?
How much time?
What space/facility (both city, and location specifics, types of rooms, layout etc).
What are the time availabilities of the attendees (weekend/weekday, etc)
Are there any special characteristics of the population?
What are the existing relationships between people coming?
What are any hot button or tension issues?

There was two charts I drew:
 * One was explaining that I think of Unconfernece methods as everything more organized then a cocktail party and less organized then talking heads on a panel or a keynote.
* The second was talking about drawing on Organization and Community Development methodologies and bringing them into Conferences for Professionals.

I also talked about growing your event from a small energized event to a larger bigger event in time.

We then went on to explore a case study with the beginning of Outlining a Health Care and ID convening.

Health ID

Potential Co-Conveners that were brainstormed.
ONC at HHS, Patient Privacy Rights, AMA, Trade Organizations, Industry Groups, Technology Standards Groups

Those with an interest in the topic include

- Payors
- Providers
- Patients
- Population/Health/Public Health Studies
- Government (National, State HIE
- Providers of EMA

when asked about the potential time/length
Two days and One Hundred People

Community Development and Management will be key to helping this come together.
Really engaging with participants ahead of time and making sure the whole range that needs to be there is in the room.

So the question of going directly at the challenge of Health Care ID is to hard a challenge. ONC actually did a good job of listening to a whole range of stakeholders and wrote a whole report but progress was not made out of that effort.
Patient Identification and Matching Final Report, February 7,2014
https://www.healthit.gov/sites/default/files/patient_identification_matching_final_report.pdf

The v1 potential framing that came out of the conversation included

What do you consider success (relative to patient identification)?
What is the problem that needs to be solved for health care ID?
What are the constraints?

There is a group moving this forward as a potential event to convene.
Please contact Kaliya if you are interested   kaliya [at] identitywoman [dot] net

MFA 3.0

Wednesday 3C
Convener: Robert Lee
Notes-taker(s): Robert Lee

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

Deck use in the session:
https://www.dropbox.com/s/qmpi3f57oag3k76/Account%20Take%20Over%20-%20oct%2026%202016.pptx?dl=0

Identity Professionals Association

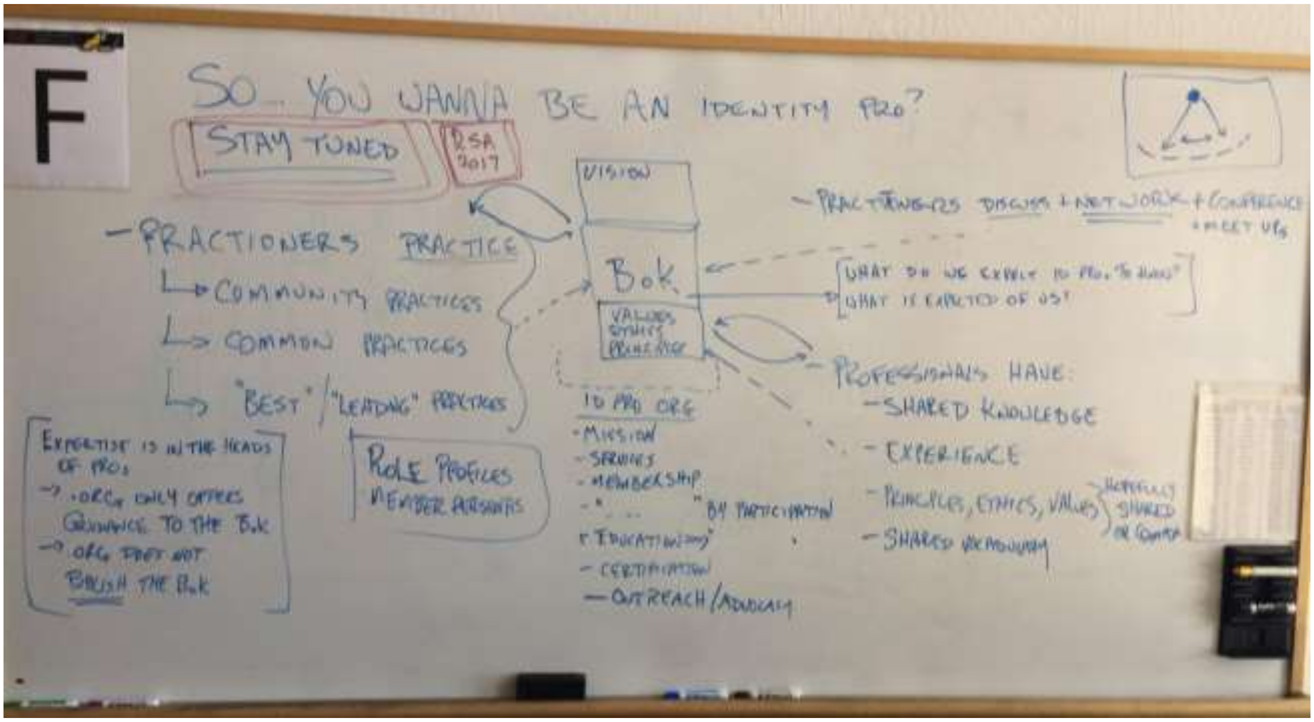
Wednesday 2F
Convener: Andrew Hughes
Notes-taker(s): Andrew Hughes

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

ID Professional Association - introduction and overview AndrewHughes3000@gmail.com

Kantara Initiative is incubating the formation of a new ID Professionals Association. The group discussed what the association intends to be, common body of knowledge, who members might be, and current timelines.
Pre-formation meetings are happening weekly as a Kantara Initiative Discussion Group. We expect to have announcements ready in February 2017.

The whiteboard picture captures the topics discussed.



Identity Verification Flows and Machine Learning in Fintech

Wednesday 2G
Convener: Maxwell Blumenfeld
Notes-taker(s): Garrett Schlesinger

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

Problem: credit bureaus are authorities for which identities on file, but how, given a consumer file, can we determine that the actor in a browser actually is the identity on file.

Potential flows:

- Prove that a person owns a mobile phone (challenge/response) registered to an entity with the same name (using data from telecomm companies on that phone number).
  - Issues: stale/inaccurate data. Family/company plans.
- Email verification
- KBAs from some authority
  - issues: "Google-able" answers
- Physical ID verification
- Human labeling

Proposal: 90/10% operational/experimental split with ID verification flows. 10% experiment gets random assignment of verification flows at the time of requesting a loan.

There will be some drop-off. Need to measure at each flow. Important to do in an a/b context. Ultimately, you want to get an idea of which verification flow will have the best ROA, conjoined with intuition around what provides a friendly user experience.

Would success in KBA boost our confidence enough to approve a loan? Does the cost of KBA lead to negative expected ROA?

In the photo id space, more interesting signals exist. E.g. *liveness* (turn 25% and take another photo).

Based on historic drop-off labels, you can then sort ordering of verification flows to actually make a difference in the outcome of fraud labeling.

Other things to look at: UK verify. Does it purely based on online behavior. https://www.gov.uk/government/publications/introducing-govuk-verify/introducing-govuk-verify

https://www.digidentity.eu/

Social/location-based data (localized photo tags) –
Raytheon riot http://www.zdnet.com/article/raytheon-riot-defense-spying-is-coming-to-social-networks/

Impermium

On the physical id front: MorphoTrust and AssureTec are the two working from source. No direct interface to government. Summary: keep expectations low until there's good government interfacing (~7 states have these already).

Huge body of research form google on effectiveness of UX flows for verification, recovery, etc. https://sites.google.com/site/oauthgoog/

Security Event Distribution

Wednesday 3A
Convener: Phil Hunt
Notes-taker(s): Marius Scurtescu

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

Presentation link:
https://github.com/independentid/Identity-Events/raw/master/SET-Distribution-IIW23.pdf

- how does this relate to OpenID RISC?
  - OpenID RISC can use this, same for SCIM, each can profile SETs for their own use cases
- email header deliver was also proposed, this presentation focuses on HTTP POST
- what does an accepted message mean?
  - that it was parsed
  - provisioning needs guaranteed delivery, for example
  - acceptance also means the right message was delivered to the right endpoint
- who is the publisher and the subcriber? IdP to RP?
  - depends on the context and profile, could flow both ways
  - abuse signals may go from RP to IdP
  - logout signals mostly from IdP to RP, but depends, up to OpenID Connect to define
  - 80% IdP to RP, 20% RP to IdP
- event specifies a state change, which can come later than the user action that triggered the state change
- no event specific error messages
  - "no account for this user" might be an example of event specific error code
    - a SET message going the opposite direction (if both channels are set up) could convey the same information
- how to show interest in a spcific user account (register to receive events for that user)?
- error handling difficuly with batching
- we should keep distribution simple, no batching, unless there is a real need for it, can be revisited in next version
- can this be extended to other use case, like sending a logout event to an IdP based on hardware proximity?
  - CISCO had a similar use case for WebEx, feed definition is complex in this case
- should we anticipate both way communication
  - well known endpoints would help automate this, there could be different well known URLs for RISC and SCIM
- some notifications, related to registrations, may work only with a query interface and not pub/sub
- don't accept email address without verifying it, as an RP

Virtual Universities and Student Profiles

Wednesday 3B
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:

http://www.windley.com/archives/2016/05/building_a_virtual_university.shtml

http://www.windley.com/archives/2016/10/when_people_can_share_verifiable_attributes_everything_changes.shtml

Verifiable Claims Deep Dive

Wednesday 3C
Convener: Manu Sporny
Notes-taker(s): Manu Sporny

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

It is currently difficult to transmit banking account information, proof of age, education qualifications, healthcare data, and other sorts of verified personal information via the Web. These sorts of data are often referred to as verifiable claims. The mission of the Verifiable Claims Working Group is to make expressing, exchanging, and verifying claims easier and more secure on the Web. The Credentials Community Group and the Verifiable Claims Task Force of the Web Payments Interest Group at W3C have extensively researched the problem and proposed an architecture and specification to enable the interoperable expression and verification of claims. The narrow scope of work in the draft Verifiable Claims Working Group Charter proposes that the first step toward broad interoperability is standardizing a data model and syntaxes for the expression and verification of verifiable claims.

Specifically, the Verifiable Claims Working Group will Recommend:

- a data model and syntax(es) for the expression of rich verifiable claims, including one or more core vocabularies.

- a note specifying how these data models should be used with existing attribute exchange protocols, a suggestion that existing protocols should be modified, or a suggestion that a new protocol is required to address the problems stated earlier in this document.
- The Working Group will NOT define a new protocol for attribute exchange or JavaScript browser APIs. These work items may be proposed at a future date if there is support for them, but are not necessary to successfully achieve the first step of interoperability.

Session Slides: https://docs.google.com/presentation/d/1BsGY6YOlkfTQQyxm0jJadxBhJwBCE3QLDoyRENzhS0k/edit

Verifiable Claims Architecture: https://w3c.github.io/webpayments-ig/VCTF/architecture/

Use Cases: https://w3c.github.io/webpayments-ig/VCTF/use-cases/

Primer: https://w3c.github.io/webpayments-ig/VCTF/primer/

More supporting information (W3C charter, due diligence documents, etc.) can be found here: https://w3c.github.io/webpayments-ig/VCTF/

Blockchain Family Values

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

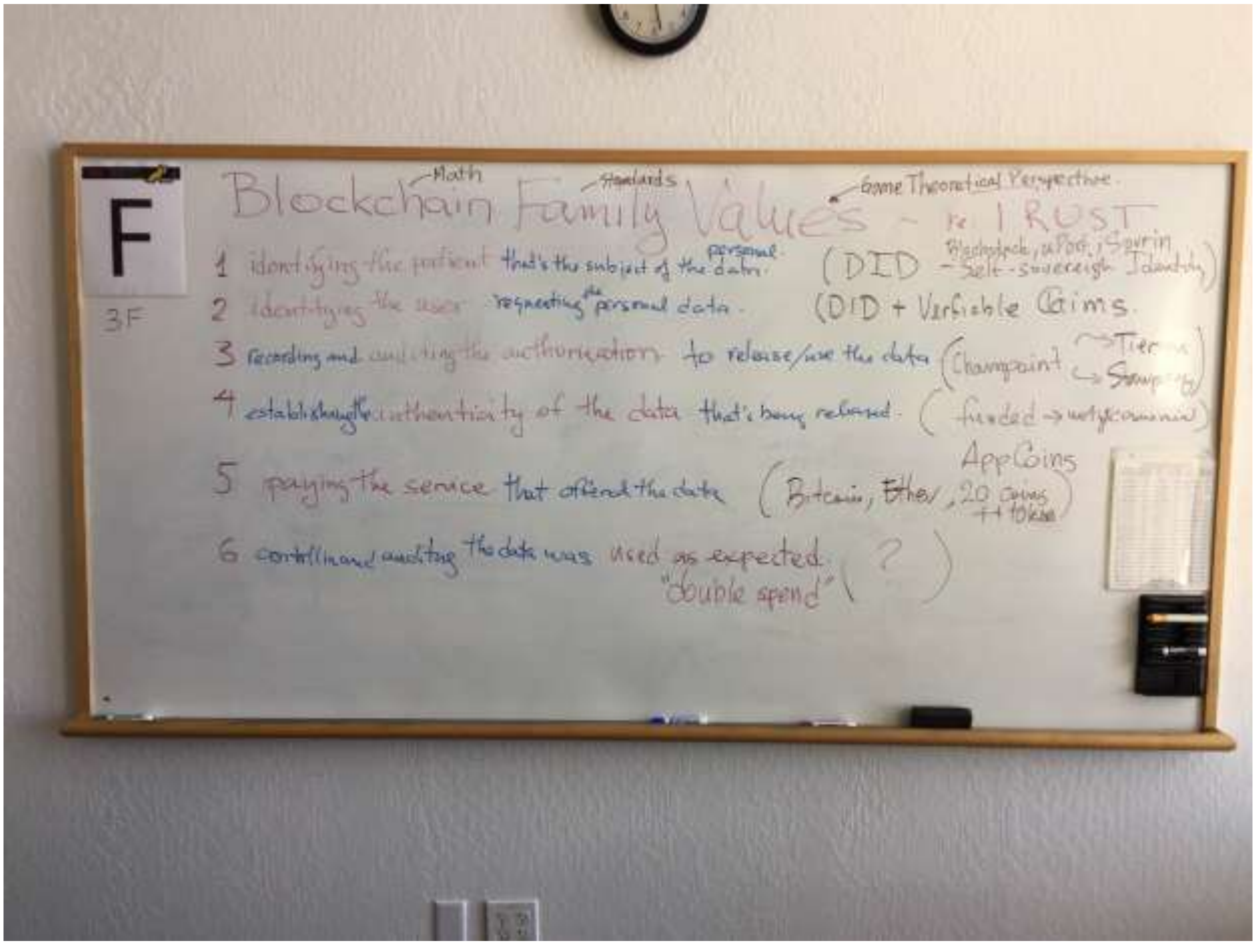
Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

When it comes to getting and using personal health data, trust is involved in:

- identifying the patient that is the subject of the data,
- identifying the user requesting patient data,
- recording and auditing the authorization to release the patient data,
- establishing the authenticity of the data that is being released,
- paying the service that offered the patient data,
- controlling and auditing that the shared data was used as expected.

Prior to blockchain, all six of these separate trust issues involved one or more institutions.

Blockchain technology has already been proposed to replace all of these institutional trust roles with math.



Blockchain Family Values - re TRUST

Math
Standards
Game Theoretical Perspective

1 identifying the patient that's the subject of the personal data (DID - Blockstack, uPort, Sovrin Self-sovereign Identity)

2 identifying the user requesting the personal data (DID + Verfiable Claims

3 recording and auditing the authorization to release/use the data (Champoint → Tier [illegible] → Stamp [illegible])

4 establishing the authenticity of the data that's being released (fixed → [illegible])

5 paying the service that offered the data (Bitcoin, Ether, 20 coins ++ tokens AppCoins)

6 controlling and auditing the data was used as expected "double spend" (?)

My Data Technology Stack 101

Wednesday 3G
Convener: Harri Honko
Notes-taker(s): Harri Honko

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

The slides shown at the session are at: http://bit.ly/mydata-architecture-IIW23

Building a Secure Consumer Fintech

Wednesday 3H
Convener: Tiffany Jung
Notes-taker(s): Garrett Schlesinger

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

Old prototype:

- Unguessable URLs to Bookmark
    - SCoopFS: Simple Co-operative File Sharing (https://alanhkarp.com/scoopfs/index.html)
- Today: bake OAuth Token into the URL
- Declare to block chain that you are X. Uses an encypted, always incrementing nonce.
- Can set up many accounts against the same identifier for this.
    - register once per device: handshake period for identification.
- Another
    1. get claim on an email address (email verification) or other channel
    2. other identifying steps (e.g. KBAs)
    3. once this is done, register with PKI (register them with a certificate authority)
        - this can be a tricky UX
- Also are in the process of refining FIDO web-auth spec. It's currently per user-agent. Want to make that distributed.
    - Regardless, FIDO is important here since it standardizes the protocol.
- Important consideration in this: means of delegation and revocation.
- Also important: make it so that transactions are authorized by the user, not an impersonating agent.
    - At the very least, responsibility tracing.
- Web key generation. Public/private key generated in browser.
- Can also do some smarter device linking/cloud solutions.

Fast Fed Part 2

Wednesday 4A
Convener: Dick Hardt
Notes-taker(s): Sing Yoong Khew

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

During the session, Pam presented a list of attributes that may need to be part of the FastFed metadata document and we discussed whether or not it needed to be included.

Consensus was easily reached for most of the attributes. Below are some that were discussed further:

-Login URL: in a double federated scenario, may need to know where to send the user to after successful authentication. Pam has action item to provide a concrete example. Tentatively, this field is

not required.
-JIT provisioning/attributes dictating logic: spent a lot of time discussing this but did not reach consensus. Some thought that it should be part of the metadata so the IdP can implement specific logic to handle specific application tenants. Others insist on a simpler IdP setup and keeping FastFed more prescriptive, each application can interpret the standard user schema the way they need to.
-Provisioning/behavior on delete: did not reach consensus. Some applications suspend the user to keep historical context, while others can delete. Issues may arise when the same identifier gets resurrected.
-Provisioning/set password supported: some RP only wants provisioning and not federation. Is this a good idea?

Other interesting notes:
-Fields that doesn't affect the functionality of federation should not be included.
-Standard user schema will be part of the FastFed spec, explicitly mapping attributes in FastFed metadata document not required.
-In the lifecycle of a (SaaS) app, the FastFed spec should provide best practice for RP in migration from a system that does not support federation to a system that supports federation
-Spec should provide recommendation how RP should handle usernames, especially in a multi tenant service (e.g. Salesforce) where the same email cannot be reused in a different tenant.

Note: Pam Dingle will provide the spreadsheet that was presented.

Consent Receipts

Wednesday 4E
Convener: David Turner
Notes-taker(s): Scott David

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

Kantara Consent receipt introduced
Focus on what it is, not why it is.
Why? – GDPR is one of prime motivators
Regulatory motivation, but want to encourage the end user value proposition.
Spec doesn't define the consent process – those need to be done, but the spec is just the receipt.
Like a receipt at the store – record of transaction and method are not part of the receipt itself
End user gets a copy – they can keep it or not, but it is given to them.
The service provider keeps a copy. (for provenance and audit purposes
Three core parts to the consent receipt
Consent receipt fields
How they look to do the coding and
What mean to conform to the specification
Type of information included
Consent receipt fields that are addressed in spec is 18 fields.
Then map the fields to JSON
Conformance has 2 parts
1 – remind parties to give the receipt
must given in human readable – naturally or easily read by a person
Conformance part 2 – what are the musts and should for the given fields.

Schedule of the work – is described
Spec page
https://kantarainitiative.org/confluence/display/infosharing/Consent+Receipt+Specification?src=contextnavchildmode
Finalizing the specification by Nov. 3. Encourage folks to visit the site and provide comments.
Discussion ensued about the implementation of the consent receipt procedures and practices.
Other things like JLINC and others that are producing something like this.
The Kantara standard helps to normalize the activity in receipts.
Thoughts offered – If trying to deal with it on the phone – is there a phone ready version and what would be included and what not included. How present the balance of the terms. Can there be a "slider" that shows the sliding scale of rights, and can drill down to find out more about the decisions being made.
Might be a value proposition to an application provider – reason to implement using the process able formats. Being able to tell difference of different levels of the accounts. Consent management system – easier once have standard format to process the data.
Secondary markets in data generated in the consent receipts can lead to secondary markets in the insights generated by the data.
What if stream of income is basis for secondary model.
Behavioral analytics as reputation –
Value in personal data in market.
Still a floor, not a ceiling. Need standardization to get the receipt. This is a floor and goes much more granular. Relative value compared to the inferred arbitrages.
Bigger needles and smaller haystacks to identify the good information.
Find value proposition to make this attractive to businesses.
Looking for comments to get the maximum value from the spec as currently presented.
Description was given about some of the inputs into the current version of the specification

Self-Sovereign Identity: What's Different

Wednesday 4F
Convener: Joe Andrieu
Notes-taker(s): Dave Sanford

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

Joe called the session to address how the thinking brought in with distributed ledger technologies has change the aspirational goals (i.e. perception of what is possible) by the IIW community.

Old:
1) Individuals control* how we are correlated across interactions
2) Individuals control* the attributes and claims used to provide services
New?
3) Individuals can selectively assert verifiable and self-asserted claims without dependency upon any central authority
4) That independence is created through free, open standards for cryptographically signed claims (non-repudiability) public ledgers for distributed storage and access control
5) Everybody is a peer, everybody can do all the functions
Much of the below are comments attributed to Joe Andrieu and Christopher Allen, however other unattributed comments are also interspersed:

Chris - If everybody is a peer, everybody is a root (side comment - DNS root, 7 keys which 14 people have, 3 keys needed to make a change)

Joe - What we may have buried is the concept that we don't need a central authority.

Chris - It may be worth a look back at history to understand why and which of Kim Cameron's "Laws of Identity" failed. Need to update the "Self Sovereign Identity Principles"

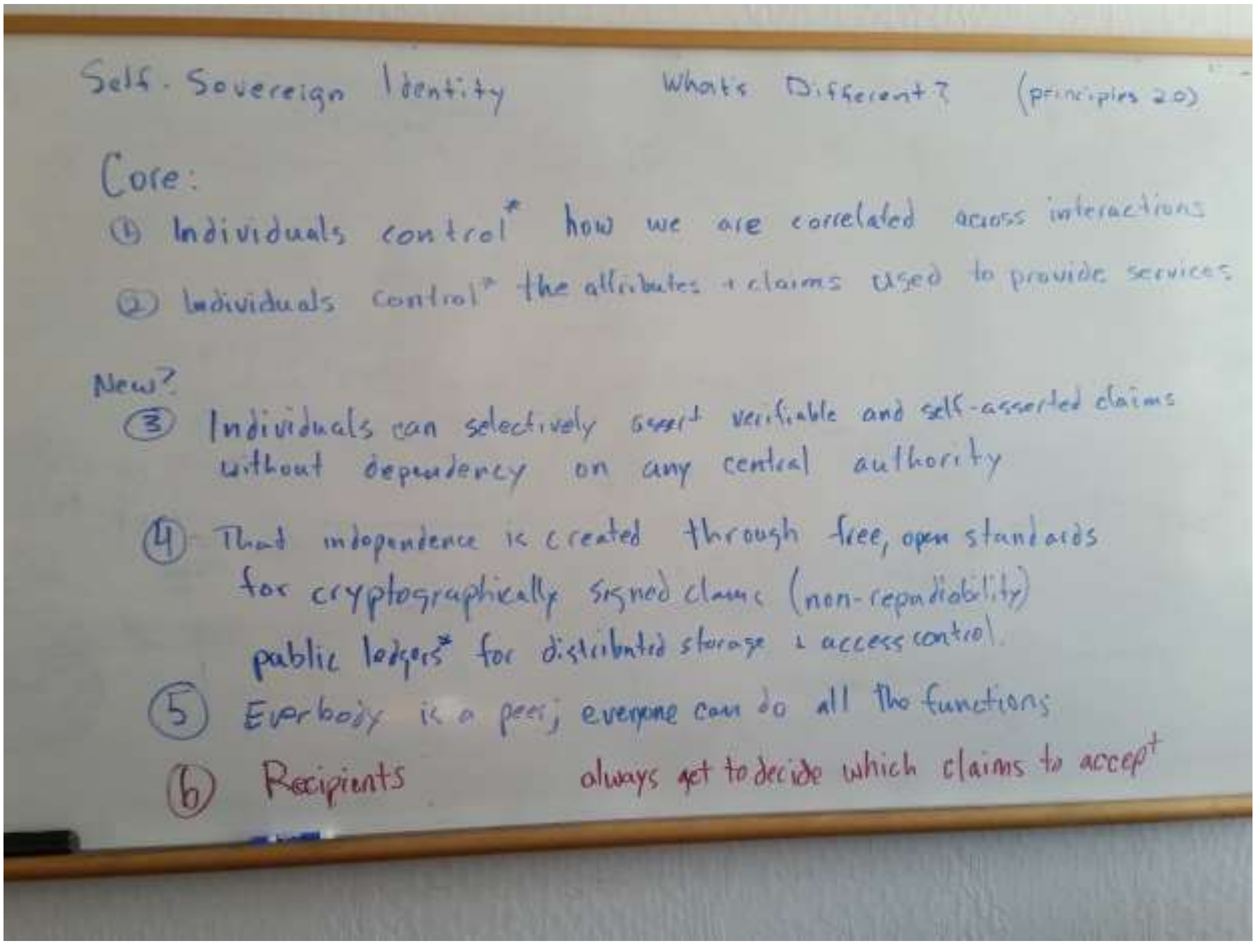
(https://github.com/WebOfTrustInfo/self-sovereign-identity/blob/master/self-sovereign-identity-principles.md).

Joe - Sovereignty is never absolute - it is always a basis for negotiation of boundaries.

6 - Relying party gets to decide which claims to accept

Chris - Administrative IDs will still exist - but there will be alternatives.

May need to go to an issuer to validate a claim or it might be validatable by information (hash, pointer, actual claim detail, ?) on a distributed ledger. ~ Issues were raised with respect to the right to be forgotten with respect to permanent information on the blockchain. The response was that this is a data minimization problem - with respect to use of the blockchain to be able to verify vs. making information permanently visible.



Self. Sovereign Identity What's Different? (principles 2.0)

Core:

① Individuals control* how we are correlated across interactions

② Individuals control* the attributes + claims used to provide services

New?

③ Individuals can selectively assert verifiable and self-asserted claims without dependency on any central authority

④ That independence is created through free, open standards for cryptographically signed claims (non-repudiability) public ledgers* for distributed storage + access control.

⑤ Everbody is a peer; everyone can do all the functions

⑥ Recipients always get to decide which claims to accept+

Chris - Up until 50 years ago in West Virginia, two town elders vouching for someone was the basis of claims, this is the historic norm, such 'socially grounded' systems - which we may be returning to in some ways with 'web of trust' type systems. ~

Chris - Timestamps mean that we can provide continuity over time, which we didn't have as comprehensively in older systems.

Picolabs

Wednesday 4G
Convener: Bruce Conrad
Notes-taker(s): Bruce Conrad

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

A pico is a "persistent compute object" and they've been available for about a decade. We are working now on an easy-to-install pico engine running in node JS, as an open source project located at github.com/Picolab/node-pico-engine for which documentation can be found at picolabs.io which will lead to the wiki page at https://picolabs.atlassian.net/wiki/display/docs/Pico+Engine+re-write

We had a great discussion, with Phil describing a live and functioning applications implemented with picos, and Bruce demonstrating the node pico-engine and showing how a registration system could be constructed, that would scale into thousands of picos with hundreds of thousands of interconnecting channels.

Some basic description, including: Each pico persists it state, and provides lock-free concurrency. It is a "first-class" Internet citizen, receiving and processing events which may affect its internal state and/or cascade to further events, and responding to queries about its internal state. When an event arrives for a pico, the pico engine selects the rules which apply by using declarations called event expressions. Rules may conditionally take actions and update the state of the pico.

Several application spaces were discussed. Objects which don't have any silicon at all can be represented by a pico in the cloud, as a kind of disembodied, state equivalent surrogate, allowing that object to participate by proxy in the IoT.

The question came up, "why have a new programming language for picos?" which Phil answered with something like this quote from his blog post, "to get pico functionality, you need to add event expressions, persistent data, a runtime environment, accounts and identifiers, channels, and the ability to manage the pico lifecycle dynamically, including the JavaScript installed in each one. By the time you're done, JavaScript is a very small part of the solution." (http://www.windley.com/archives/2015/11/reactive_programming_with_picos.shtml)

We invite contributions, consumption, and/or competition.

OTTO: Open Trust Taxonomy for Federation Operators

Wednesday 4H
Convener: Mike Schwartz
Notes-taker(s): Mike Schwartz

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

Federations: an central organization that lowers the cost of collaboration by providing standard security policies and practices, providing standard legal agreements, and technical schema. A good example of a multi-party federation in the higher education industry is InCommon: https://www.incommon.org/

OTTO is a working group at Kanatara that is leading an effort to define API's and data structures to enable federation operators to support new protocols like OpenID Connect and OAuth 2.0. It builds on the experience gained by operating SAML federations, and tries to better address requirements like:

- making the federation metadata more searchable
- better scaling inter-federation
- providing more flexibility for schema extension

OTTO defines a few actors:
Registration Authority - the organization that provides the tecnnical administration (i.e. hosts the database and web servers) for one or more federations
Federation Operator - the organization that is responsible for making the rules, setting the techincal standards, and vetting members.
Organizations - the legal entities that join Ffederations
Federation Entities - the services operated by an organization that are listed in a federation.

The "standard," which really needs official formatting, can be found here:
https://github.com/KantaraInitiative/wg-otto

There is a test federation generator here:
otto-test.gluu.org:8080

A test implementation of OTTO has been completed by Gluu. The code is here:
https://github.com/GluuFederation/otto-node
The API's have been deployed, and can be tested live here via Swagger UI:
otto-test.gluu.org/swagger

The test implementatoin showed that the approach defined by the WG is feasible. Specifically, the idea for querying the underlying metadata, and for browsing the data was shown to scale.

There is also a Presentation on OTTO from EIC here: https://prezi.com/vbh50clio1h7/eic-kantara-otto/

Ecosystem Maps

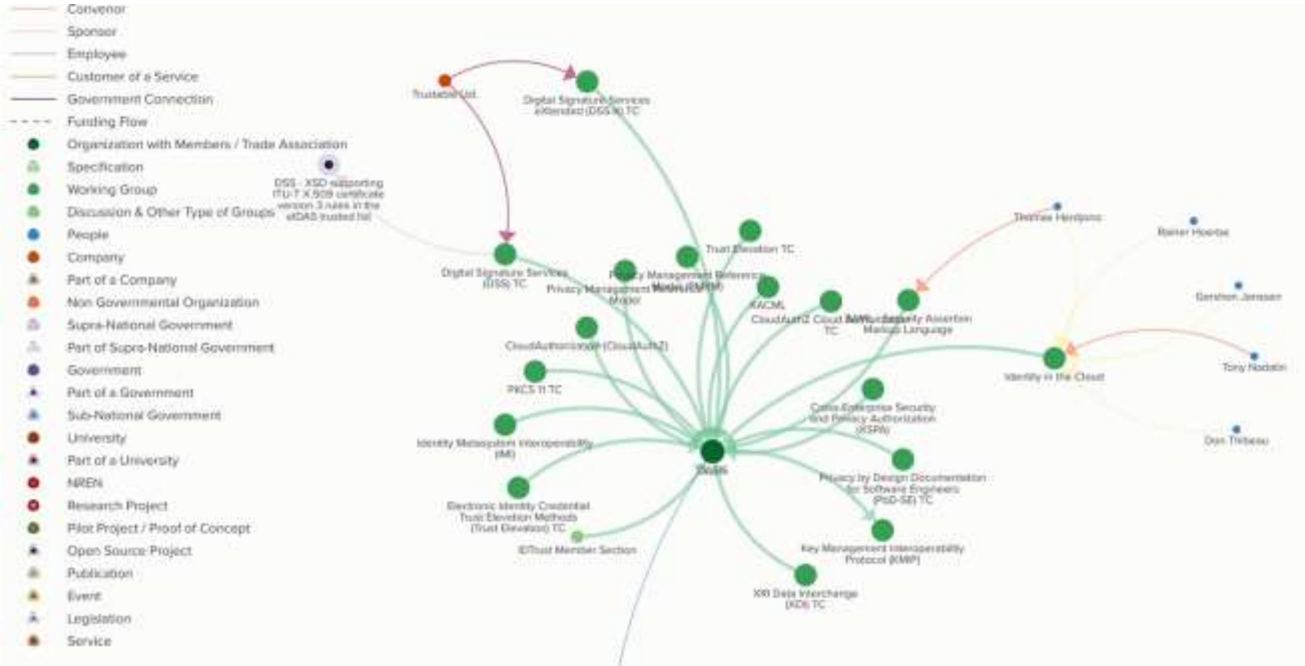
Wednesday 4I
Convener: Kaliya Young
Notes-taker(s): Kaliya Young

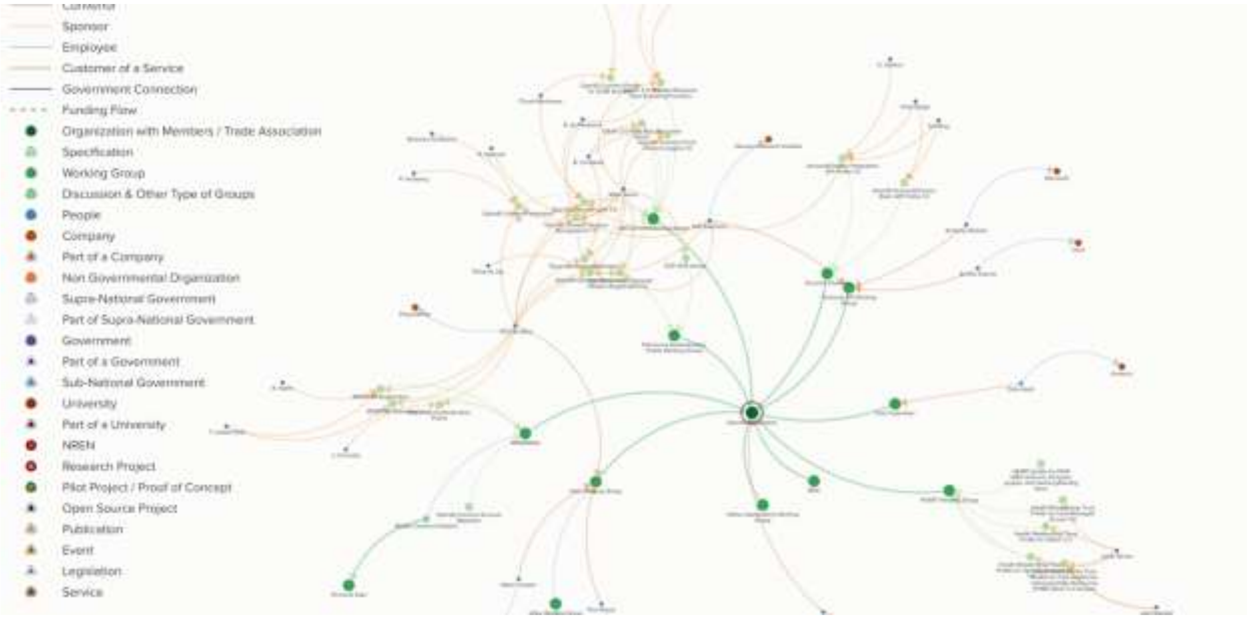
Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

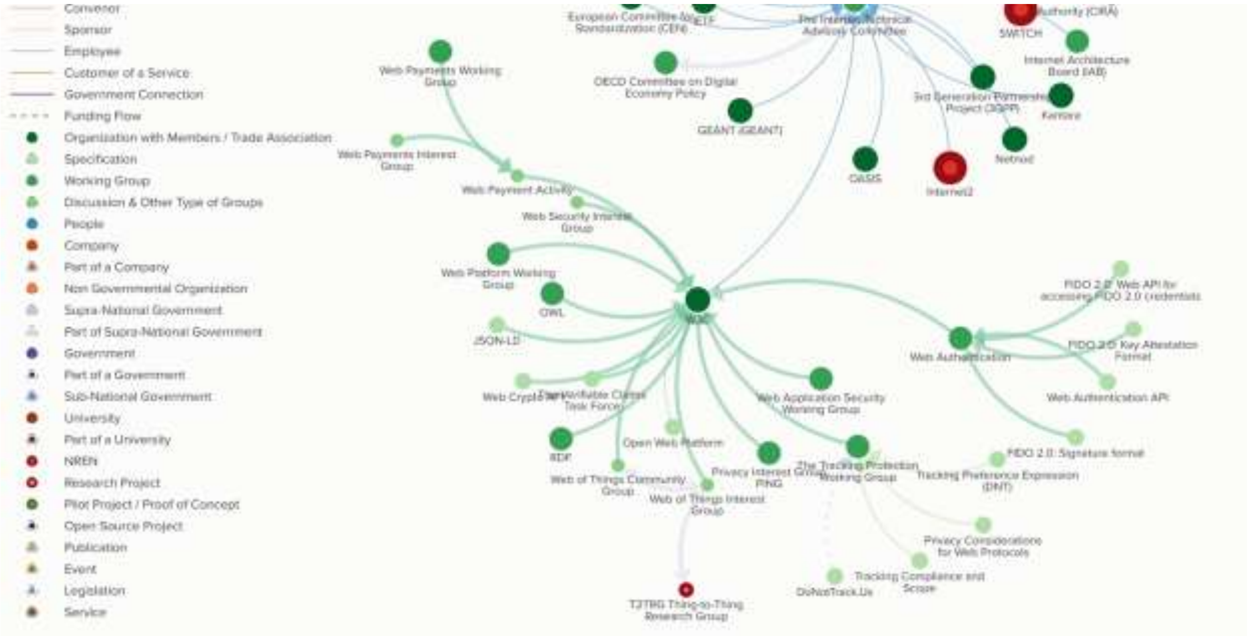
I presented about the ecosystem maps that I am being resourced to create of the ecosystem. Right now they cover all the major standards bodies and their efforts in digital identity.

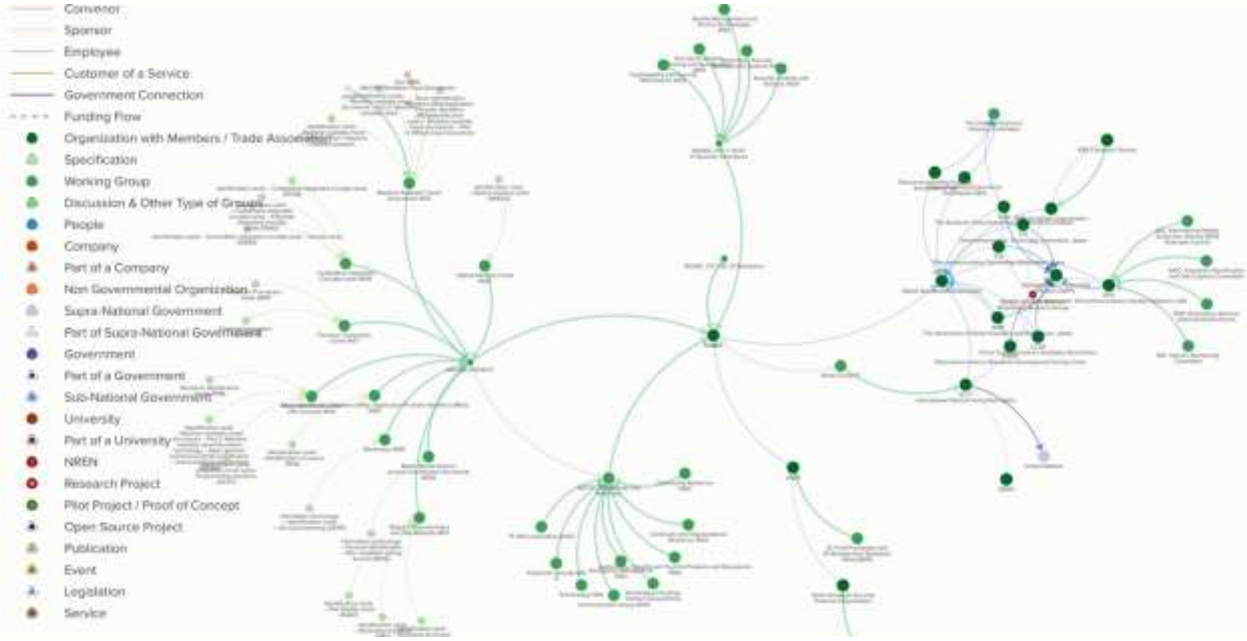
The work is just beginning. I shared several map snap shots.

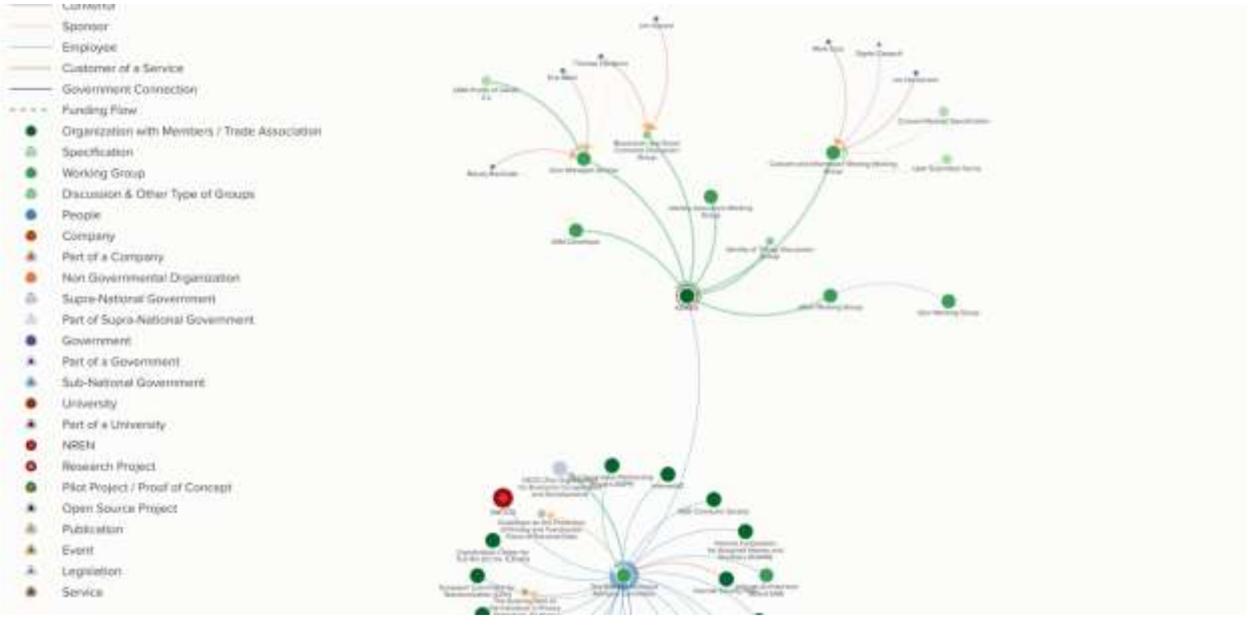
If you would like to contribute to the map or get progress about its development please contact me kaliya [at] identitywoman [dot] net

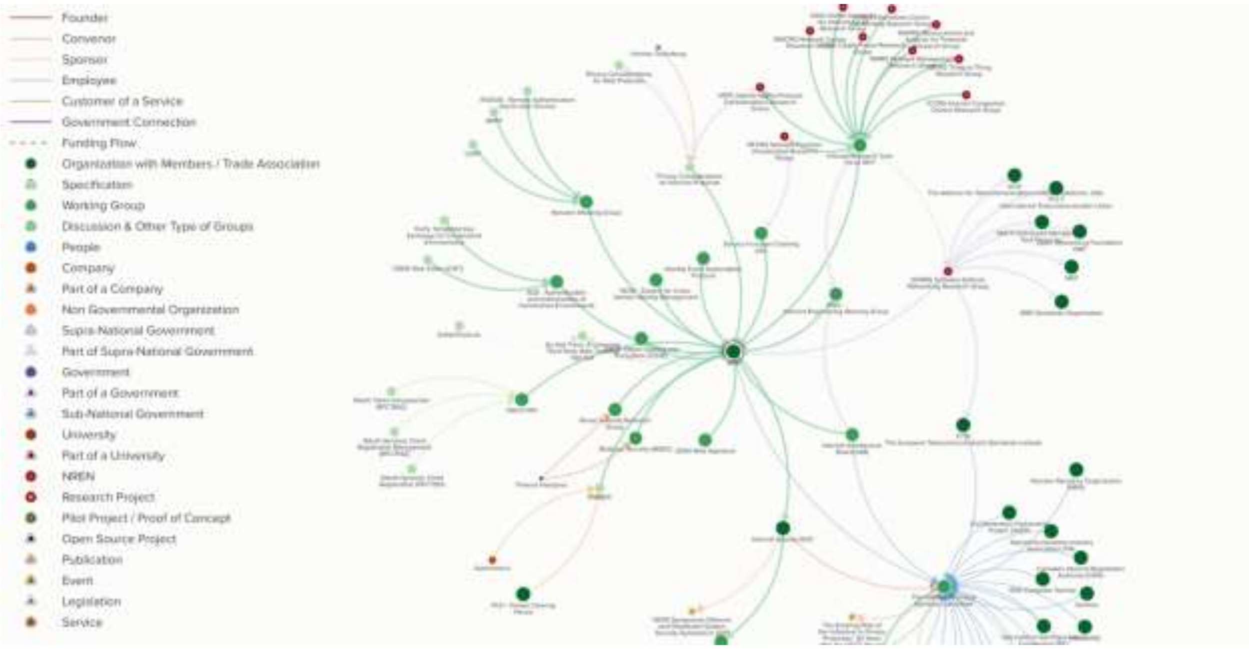

Convenor
Sponsor
Employee
Customer of a Service
Government Connection
Funding Flow
Organization with Members / Trade Association
Specification
Working Group
Discussion & Other Type of Groups
People
Company
Part of a Company
Non Governmental Organization
Supra-National Government
Part of Supra-National Government
Government
Part of a Government
Sub-National Government
University
Part of a University
NREN
Research Project
Pilot Project / Proof of Concept
Open Source Project
Publication
Event
Legislation
Service
Trustable Ltd.
Digital Signature Services eXtended (DSS-X) TC
DSS - XSD supporting ITU-T X.509 certificate version 3 rules in the eIDAS trusted list
Digital Signature Services (DSS) TC
Privacy Management Reference Model (PMRM)
Privacy Management Reference Model
Trust Elevation TC
XACML
CloudAuthZ
Cloud Authorization TC
Security Assertion Markup Language
CloudAuthorization (CloudAuthZ)
PKCS 11 TC
Cross-Enterprise Security and Privacy Authorization (XSPA)
Identity Metasystem Interoperability (IMI)
OASIS
Privacy by Design Documentation for Software Engineers (PbD-SE) TC
Electronic Identity Credential Trust Elevation Methods (Trust Elevation) TC
IDTrust Member Section
Key Management Interoperability Protocol (KMIP)
XRI Data Interchange (XDI) TC
Thomas Hardjono
Rainer Hoerbe
Gershon Janssen
Identity in the Cloud
Tony Nadalin
Don Thibeau


Convenor
Sponsor
Employee
Customer of a Service
Government Connection
Funding Flow
Organization with Members / Trade Association
Specification
Working Group
Discussion & Other Type of Groups
People
Company
Part of a Company
Non Governmental Organization
Supra-National Government
Part of Supra-National Government
Government
Part of a Government
Sub-National Government
University
Part of a University
NREN
Research Project
Pilot Project / Proof of Concept
Open Source Project
Publication
Event
Legislation
Service


Convenor
Sponsor
Employee
Customer of a Service
Government Connection
Funding Flow
Organization with Members / Trade Association
Specification
Working Group
Discussion & Other Type of Groups
People
Company
Part of a Company
Non Governmental Organization
Supra-National Government
Part of Supra-National Government
Government
Part of a Government
Sub-National Government
University
Part of a University
NREN
Research Project
Pilot Project / Proof of Concept
Open Source Project
Publication
Event
Legislation
Service
European Committee for Standardization (CEN)
IETF
The Internet Technical Advisory Committee
Authority (CIRA)
SWITCH
Internet Architecture Board (IAB)
Web Payments Working Group
OECD Committee on Digital Economy Policy
3rd Generation Partnership Project (3GPP)
Kantara
GEANT (GEANT)
Nethod
OASIS
Internet2
Web Payments Interest Group
Web Payment Activity
Web Security Interest Group
Web Platform Working Group
OWL
W3C
JSON-LD
FIDO 2.0: Web API for accessing FIDO 2.0 credentials
FIDO 2.0: Key Attestation Format
Web Authentication
Web Authentication API
Web Crypto API
Verifiable Claims Task Force
Web Application Security Working Group
RDF
Open Web Platform
FIDO 2.0: Signature format
Web of Things Community Group
Privacy Interest Group PING
The Tracking Protection Working Group
Tracking Preference Expression (DNT)
Web of Things Interest Group
Privacy Considerations for Web Protocols
DoNotTrack.Us
Tracking Compliance and Scope
T2TRG Thing-to-Thing Research Group


Convenor
Sponsor
Employee
Customer of a Service
Government Connection
Funding Flow
Organization with Members / Trade Association
Specification
Working Group
Discussion & Other Type of Groups
People
Company
Part of a Company
Non Governmental Organization
Supra-National Government
Part of Supra-National Government
Government
Part of a Government
Sub-National Government
University
Part of a University
NREN
Research Project
Pilot Project / Proof of Concept
Open Source Project
Publication
Event
Legislation
Service


Convenor
Sponsor
Employee
Customer of a Service
Government Connection
Funding Flow
Organization with Members / Trade Association
Specification
Working Group
Discussion & Other Type of Groups
People
Company
Part of a Company
Non Governmental Organization
Supra-National Government
Part of Supra-National Government
Government
Part of a Government
Sub-National Government
University
Part of a University
NREN
Research Project
Pilot Project / Proof of Concept
Open Source Project
Publication
Event
Legislation
Service



Reputation Algorithms & Scoring for Curating Self-Sovereign Data

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

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

Slides at:
https://github.com/SmithSamuelM/Papers/blob/master/presentations/ReputationAlgorithms.pdf

Personal API Implementation

Wednesday 5B
Convener: Kelly Flanagan
Notes-taker(s): Kelly Flanagan

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

Kelly presented the attached presentation on Personal APIs and his implementation using AWS.

Essentially, Kelly has produced an API using AWS that allows other APIs and associated resources and methods to be installed without having to understand the complexities of AWS. The source code is available on Github. His Github user name is kelflanagan.

Here is a link to the presentation / notes.

https://www.dropbox.com/s/o7604m61e8imm4h/Personal%20APIs.pdf?dl=0

XDI Update

Wednesday 5C
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:

Markus gave a demo of an XDI application that enables individuals to connect to one another via link contracts, to share personal data, and to receive real time update notifications. The application also includes functionality to connect to non-native-XDI data sources such as the Meeco life management platform and a CozyCloud instance.

We discussed the following topics:
1. Synergy between XDI and the Sovrin distributed ledger,
2. Applicability of the technology (specifically link contracts and link contract templates) to finance use cases,
3. Transport protocols such as HTTPS, WebSocket, RAET,
4. Relevance of XDI to GDPR requirements.

Video of a demo similar to the one shown in this session:
https://vimeo.com/181896180

Access Control & Data Rights for the Industrial Internet

Wednesday 5E
Convener: Dario Amiri
Notes-taker(s): Dario Amiri

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

High level summary:

- No best practices or standards for solving common use cases in II access control.
- OAuth/UMA not sufficient on their own.
- Some problems are generic enough that there might be common answers.

How can you access control hierarchies of resources?

- Carry ids and coarse grained privileges in scopes.
- Export standards for permissions and policies to UMA aunthz serverXACML for central management?

How can you access control event streams by time of ownership (e.g. previous owner of a device can only see event stream during his period of ownership)?

- Many use case examples - no best practices or standards

How can you inject environment claims into the authz decision?

- Data correlation and pattern analysis
- JWS as a carrier of environment claims

Entitlement requests – Asks the question: “what are all of the resources I can access” rather than “can I access this particular resource”.

- No good patterns or standards for entitlements request at the REST level

There might be useful information for these use cases in the body of work produced by the IETF constrained device working group COAP &amp; ACE.

Dario Amiri
Principal Software Architect
GE Digital

Identity in Physics

Wednesday 5G
Convener: Paul Borrill
Notes-taker(s): Ryan Page

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

Paul's notes on topics discussed:

Identity in Physics: Steven French and Décio Krause. Identity in Physics: A Historical, Philosophical, and Formal Analysis. Oxford University Press, 2006 https://global.oup.com/academic/product/identity-in-physics-9780199278244

Identity in Philosophy: "The identity of indiscernibles".

Identity and Individuality in Quantum Theory: http://plato.stanford.edu/entries/qt-idind/ [Very important read — recommended you read it all]

"Those great principles of sufficient reason and of the identity of indiscernibles change the state of metaphysics. That science becomes real and demonstrative by means of these principles, whereas before it did generally consist in empty words."
~ Gottfried Leibniz

Philosophy teaches us that this problem is already wicked, and is related to the Identity of Indescernables. This principle states that no two distinct objects or entities can exactly resemble each other (Leibniz's Law) and is commonly understood to mean that no two objects have exactly the same properties. The Identity of Indiscernibles is of interest because it raises questions about the factors that individuate qualitatively identical objects. This problem applies to the identity of data and what it means to have many substitutable replicas, as much as it does to Quantum Mechanics.

This issue is of great importance to the complexity of humans interacting with their data, because it is unnecessary for a human to need to expend attention (or cognition) on any more than a single entity, no matter how many copies exist, as long has s/he can make the assumption that all the copies will eventually be made identical by the system.

See also: Katherine Hawley, How Things Persist.

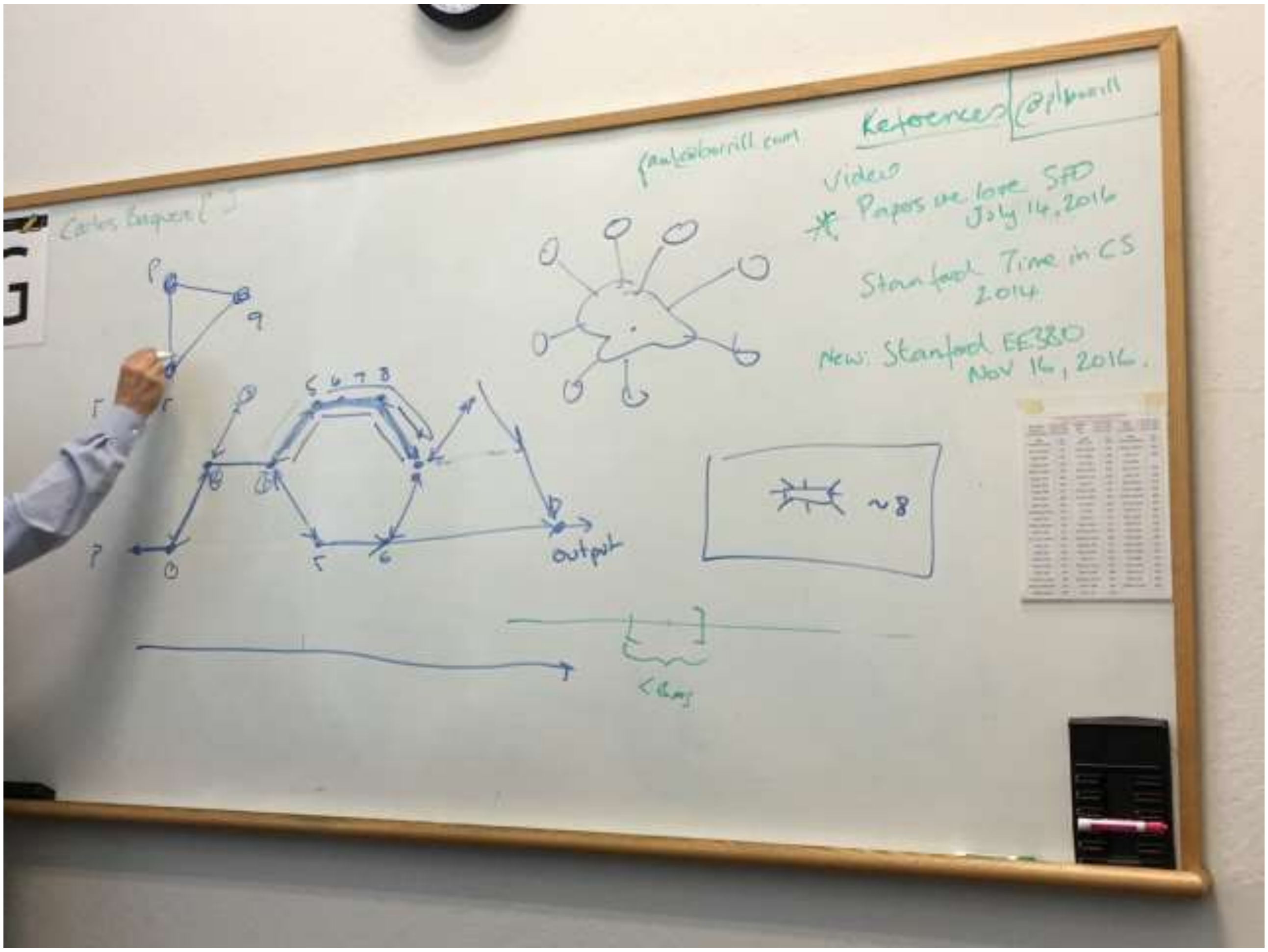
How do things persist? Are material objects spread out through time just as they are spread out through space? Or is temporal persistence quite different from spatial extension? This key question lies at the heart of any metaphysical exploration of the material world, and it **plays a crucial part in debates about personal identity and survival**. Katherine Hawley explores and compares three theories of persistence -- endurance, perdurance, and stage theories - investigating the ways in which they attempt to account for the world around us. Having provided valuable clarification of its two main rivals, she concludes by advocating stage theory. Such a basic issue about the nature of the physical world naturally has close ties with other central philosophical problems. How Things Persist includes discussions of change and parthood, of how we refer to material objects at different times, of the doctrine of Human supervenience, and of the modal features of material things. In particular, it contains new accounts of the nature of worldly vagueness, and of what binds material things together over time, distinguishing the career of a natural object from an arbitrary sequence of events. Each chapter concludes with a reflection about the impact of these metaphysical debates upon questions about our personal identity and survival. Both students and professional philosophers will find that this wide-ranging study provides ideal access to the lively modern debate about an ancient metaphysical problem.

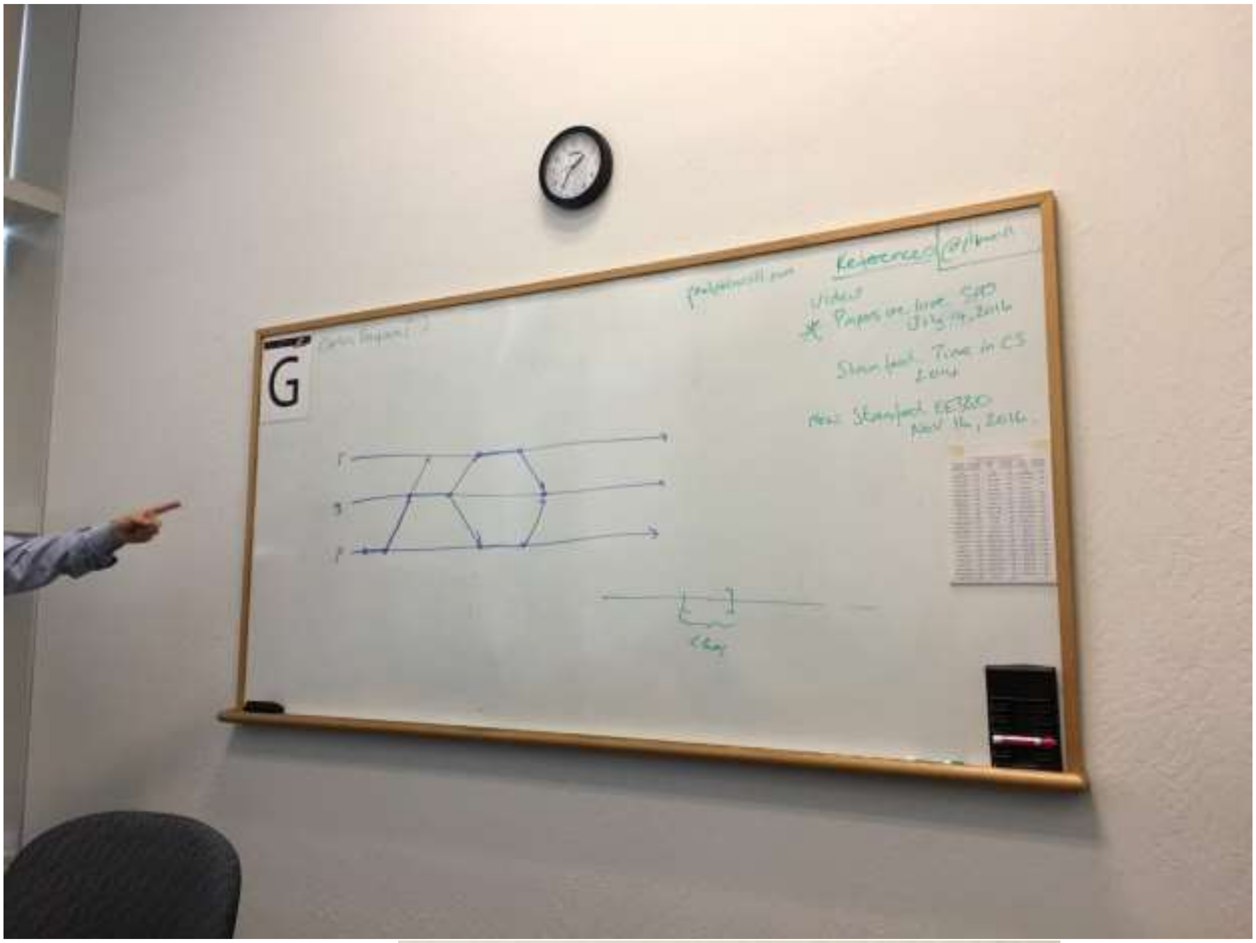
Time emerges from entanglement.
What is identity in physics – years ago moved to statistical physics – all particles are indistinguishable.
Thermodynamics is example
Indistinguishability goes all the way down.
All electrons are one electron – Feynman
Identity is at the heart of physics – Identity in physics book describes the heart of the problem.
Lee Smolin - Says it is a physics and philosophy problem.
Leibniz – the identity of the indiscernible. Insight into how know if something is the same as something else.
George Washington's axe – is it the same axe? Theseus myth – the ship story. The ship of Theseus: https://en.wikipedia.org/wiki/Ship_of_Theseus
IF replace all the planks of the ship, is it the same ship?
Deep philosophical problem that is at the heart of the reasoning in physics. Modern digital world, - can create exact replicas of the object.
Want to make the object distributed. Reality of the object exists as many different replicas. Need to consider how propagate the change to one, to another.
Lattice variables – to make sure that all.
Simons institute – Berkeley – course on consistency. Can make things consistent locally, and cannot make them globally.
Digital version of Ship of Theseus
Entanglement is next issue – no-cloning theorem – see Wikipedia page
Cannot copy a quantum state – can only steal it.
If try to observe an entangled system, change it.
Conserved quantities is related theorem – parity, momentum, etc. conserved.
Is information conserved – yes, but in interesting way. Shared information in quantum theory is where the information is. When make an observation, you
Entanglement: Nature of space time will change everything this year.
Google has 2 groups on quantum computers. Nobel prizes about quantum this year.
Quantum information theory – mutual information. It is a bipartite pair.
Entanglement is monogamous – only works between two parties (can compose that into larger objects, but idea is ripping apart idea about nature of space time.
After Einstein after general relativity – Murkowski space – space time is 4 dimensional.
How can you have these correlations between events that appear to happen faster than speed of light.
4 dimensional manifold challenge.
If I take a laser and shine it into object (parametric down conversion), and two photons get entangled.
Description of quantum entanglement apparatus. – called preparation of the measurement.
Information is negative of the entropy of the
Information is the answer to a yes no question. True in QM, true in Bayesian statistics, true for Shannon.
Bell states –
Einstein and Rosen paper – trying to resolve
Realizing that not living in 4 dimensional Murkowski space.
Back to apparatus description. Combine random generator number from two states.
Original Bell's paper – were seeing correlations that were faster than speed of light. (c)

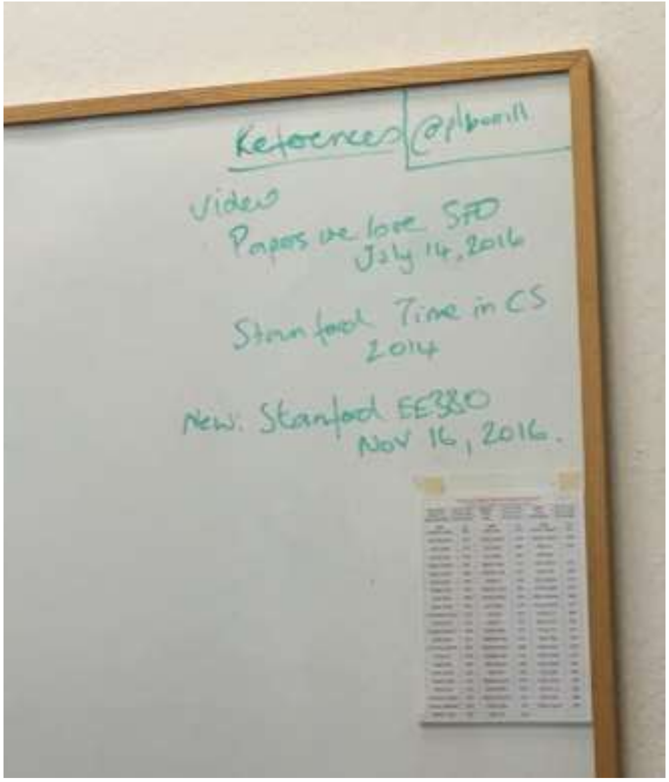
Puzzle of entanglement – Atoms are sending information to you in a spiral (described by Maxwell's equation). Electron spin can be measured, but when the electron is being exchanged back and forth, if had Murkowski background then would be able to detect time. There is no such thing as duration.
Biggest problem is the "Generals problem"
Computer science and physics – starting to see these deep problems of physics.
Exchange is lost of information (entropy).
Idea of speed, and that universe has a maximum speed is now being answered in terms of c, why is there a speed of light maximum.
Quantum provides random information. In electrical theory it is noise.
Photons and electrons are indistinguishable.
There is no such thing as single body.
When looking at stars – photon didn't leave the star until it knew that your eye was waiting for it.
Information is mutual
Not predetermination
Time emerges from entanglement. The universe is stitched together with entanglement. This means that, if that is true – can send information exchanged without timeouts.
Taken the mutual information and leveraged it to attach a payload. That provides a piece of information that can remain persistent.
Think about these problems.
Reversible entanglement issue discussed.
Can you entangle a particle and have achievable predictable space?
Quantum key distribution is related. Fiber optic is doing that.
When you ask the question in entanglement
Can you have indirect observation – can you have a measurement - weak entanglement is using statistic analysis.
Descriptions of the slit experiment. "at the same time" is raising the Murkowski space.
What is the flawed assumption of the Murkowski space – look at EPR experiment. ER experiments – one solution is that can get a wormhole. Susskind and others have speculative, but seems that ER and EPR are the same thing.
These are the same phenomenon, but Einstein and Rosen didn't recognize it.
The alternative to the slit experiment (going through both slits at the same time) is that time is going back and forth at the same time. It is the path of least action from Feynman diagrams. It is the same photon. Time is frozen in perpetuity between entangled
Can you entangle macro states? – Entanglement usually at atomic scales. What is really going on is that space time is stitched together by entanglement.
Coming to consensus – time emerges from entanglement.
What mean for computer science and identity and irreversibility.
Can make time go backwards on a single link. Time does not exist.
How does this correlate with the second law of thermodynamics? Thermodynamic arrow of time.
Issue. Lowest level thing is the simplest.

Carroll fond of notion of time.
Statistical question –
Space and time are the same thing –
1905 paper Einstein theory is about mirrors and clocks – one dimensional property.
3 dimensions may be
Emergent properties of systems are hard to consider.
Biology – notion of reversible differentiation,
How can we correlate – infinite dimensions that can explore. And some of those may be relevant to the workshop.
If these things are identical and can get information - how can things be hidden.

Dark matter and dark energy. What are they? We hide things now with quantum key distribution is a proven technology, but expensive. Once they are up and running they are secure. As soon as can move a key securely, can hide anything.
Speculation – if this is analyzed under the model of "no time" with photon going back and forth. If entangle photon – it is trapped. If given another photon – he and I are dark matter, but photon trapped in sub-time.
Tractor beam – cooling for electromagnetic cooling – if match frequencies and then raise frequency- it draws it toward. Closest to absolute zero with laser cooling.
Third thing to take from room – Entanglement is universal and substitutable.
Videos from Caltech – Stanford (Susskind), perimeter institute,
Starting thinking of time as a tree and be careful of how you establish the root (phase space issue).
Earth computing – How to distribute time and make sure that can be more resilient and using standard hardware.




G
References
@plbarrill
Video
Papers we love SFO
July 14, 2016
Stanford Time in CS
2014
New: Stanford EE380
Nov 16, 2016
r
g
p


References
@plbarrill
Video
Papers we love SFO
July 14, 2016
Stanford Time in CS
2014
New: Stanford EE380
Nov 16, 2016.

OIDC Identity Federations

Wednesday 5H
Convener: Roland Hedberg
Notes-taker(s): Roland Hedberg

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

Roland did a presentation of the basic pieces of the OIDC Identity Federation draft:

http://www.slideshare.net/RolandHedberg1/oidc-fed-in-picturesiiwxxiii

After which there was a discussion about the pros and cons. The overall designed was like by many. The potential problem is that parties of the system may have to manage a large number of keys.

Identity Without the Individual

Wednesday 5J
Convener: Andy Halliday
Notes-taker(s): Andy Halliday

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

Identity without the Individual: A Publishing Perspective

In the publishing industry (specifically scientific journal publishing), 90%+ of access to our content comes from sources where we cannot specifically identify an individual with a personal credential. This provides challenges in collecting information in order to provide personalised / improved services, for fraud detection, and mitigation of illegitimate use.

In this discussion, we talked about some strategies for incentivising users to provide personal credentials and allowing them to be linked to an institutional subscription. Some of the incentives we discussed were:

1. Offering 5 free paid-for articles per month before requiring a personal credential
2. Offering the ability for users to take their institutional entitlements with them for a pre-defined period – through linking a personal credential to an institutional account
3. Providing personalised homepage / recommendations based upon a personal credential
4. Reducing the length / complexity of registration – and potentially not requiring registration – by using social sign-on etc.

We also discussed the architecture for an IDP at the heart of a solution – based on OAuth2 and Open ID Connect.
The discussion provided some interesting food for thought, and ideas to test to move towards an improved solution.

Thursday October 27

Design of a Scalable Service Broker

Thursday 1E
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:

Hewlett-Packard Enterprise (HPE) has a product called Enterprise Services on Demand (ESO) that simplifies standing up large enterprise services, such as SAP Hana, and enabling external cloud services, such as Salesforce. ESO provides a catalog of services with a small number of preset configurations. Companies with contracts with HPE can order such services with a few clicks, and the service will be ready to run in tens of minutes instead of tens of days.

Other companies have such catalogs, so HPE also planned to offer differentiators, one of which was managing the Service Level Agreements (SLAs) that its enterprise customer have with their cloud providers. The problem is one of scale. HPE has several thousand such customers, each with tens of thousand to hundreds of thousands of employees, and each customer uses hundreds of services. I was given the task of designing the part of the service broker platform that mediates all request from those user to the services they use.

Conventional solutions could be used if all the services were hosted by HPE or if all requests came from inside the enterprise firewall. In the former case, a reverse proxy would guarantee that the service broker sees all requests; in the later case, a proxy running in the enterprise would do. Unfortunately, ESO has to deal with requests made to external cloud services from outside the corporate firewall.

I designed a platform with three key components. A User Proxy (UP) running in the enterprise, a Solution Broker (SB) running in HPE data centers, and a Solution Wrapper (SW) running either in the HPE data centers or in one associated with the external cloud service. This design meant that identities were relevant only outside the SB. Enterprise users would authenticate to their companies; the SW would authenticate as the users to the cloud service. The SB needed identities only for administrative users.

A user of a service would invoke it via the UP in the form of an app or a web page. The UP would retrieve a blob from the company's Active Directory (AD) or LDAP server. One component of this blob was an OAuth access token to authorize access to the SB. The UP submitted the request and the blob to the SB, which would decrypt with its private key an OAuth token authorizing access to the appropriate SW, and use it to invoke the SW, forwarding the blob. The SW would decrypt with its private key the user's signing key from the blob, verify the signature on the request, and then decrypt the user's login credentials from the blob and pass session requests/replies back and forth.

This approach had several advantages. There was no need for a CA in order to trust the signing keys. Neither the SB or the SWs had any permissions of their own, reducing the damage a successful attacker could do. Further, the SB and SWs were highly scalable because they were stateless, not even requiring a backing database. An employee's access to all services could be blocked by revoking one token, a company could block access to a particular service by revoking one token, and HPE could revoke an enterprise customer's access to all services by revoking one token.

This design was under review when the SB part of ESO was cancelled and all the people working on it, including me, were laid off. Hence, there's no guarantee that there weren't security issues with the design, nor is there a way to be sure of its scalability.

Federated/Decentralized Social Web

Thursday 1G
Convener: Kaliya Young
Notes-taker(s): Kaliya Young

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

Context History:
Geo-Cities
Live Journal (the home of the original OpenID URL)
My Space
WordPress and other Blog

Indie Web - Own do the main web site/hub - "this is me"

(With) Known - Ben Werd - https://withknown.com/

Microformats - http://microformats.org/

Distributed Social Web work at W3C
Social Verbs
https://www.w3.org/Social/
https://www.w3.org/2005/Incubator/socialweb/XGR-socialweb-20101206/
https://www.w3.org/Social/WG

Social Web Protocols
W3C Working Draft 02 November 2016
https://www.w3.org/TR/social-web-protocols/

Building Blocks:
PubSub - Publish Subscribe
pubSubHubbub
https://github.com/pubsubhubbub/

Next level of UX/UI was not there for RSS/Atom adoption across the web.
RSS - http://www.whatisrss.com/
Atom - https://tools.ietf.org/html/rfc4287

Google KILLED Reader.

OAuth 1.0 - https://tools.ietf.org/html/rfc5849

UMA - different access controls for different people

Self-Sovereign ID - DID
Existing CMSs Drupal and Wordpress

Patchwork - https://github.com/ssbc/patchwork

Terms Building Blocks by Customer Commons

End to End Encryption

Tor - https://www.torproject.org/projects/torbrowser.html.en

What we Need: We need payments systems eg/Patreon - Permission based advertising

Business Models that resource all aspects of the ecosystem

Group Chat —> Slack Plug In/Out
—-> Back channel for the network
IFTTT If this then that

Graph Database Tech
Apache
Constructing Graphs doing graph traversal
CounnDB

Centralized/Distributed How People Connected

PRODUCTIZATION GAP

- core distain of Normals by - Blocking functionality - Group Tools.

Opportunities:
Anti-GAFA (Google, Amazon, Facebook, Apple) sentiment in Europe
http://www.makeuseof.com/tag/gafa-eu-doesnt-love-large-american-internet-companies/

Media “industry” freaking out over future business models and the power of platforms

Data Broker Evilness has grown and includes device tracking

Democracy Machine - John Gastil, is working on it.
http://ash.harvard.edu/links/building-democracy-machine-toward-integrated-and-empowered-form-civic-engagement

Social Movement’s of Late including #ows, #BLM #teaparty

Brewster Khale
Reclaim the Web was expanded to Internet
http://www.reclaimtheinternet.com/

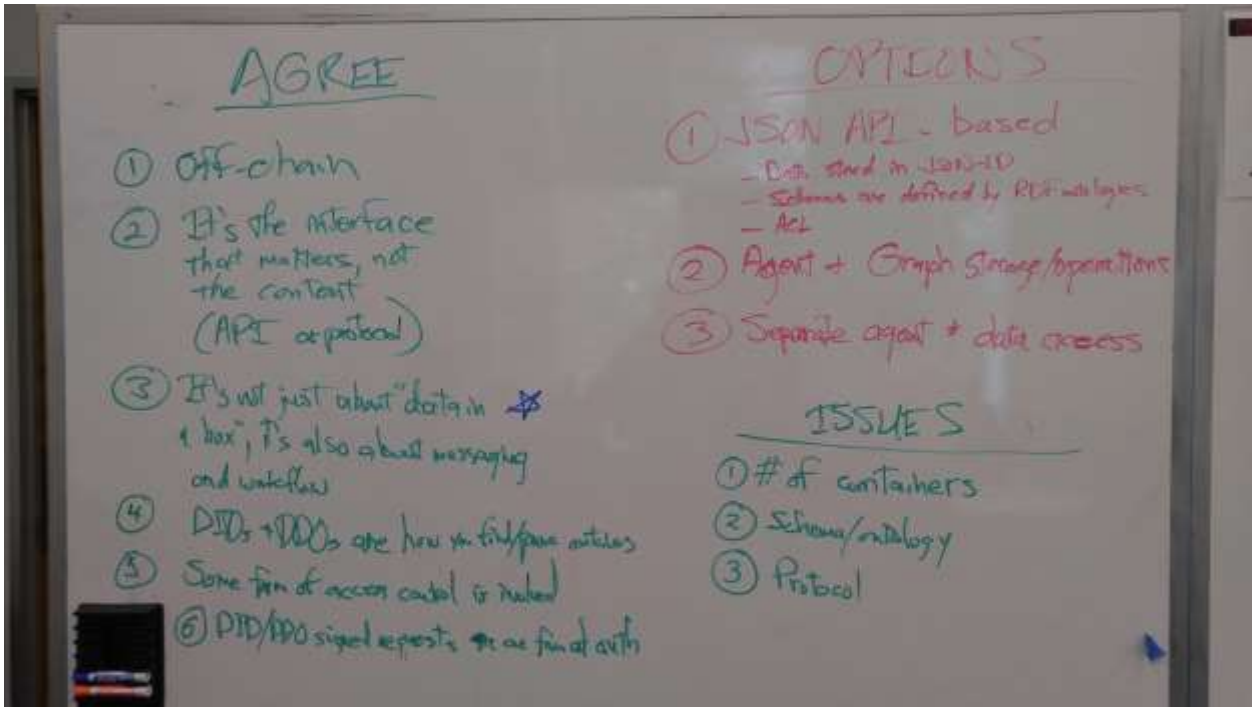
Platform Cooperative - http://platformcoop.net/
Indie by Aral Balkan - https://ind.ie
$ Not coming back infrastructure developments

Container Wars

Thursday 2A
Convener: Sam Curren
Notes-taker(s): Ryan Page

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

Whiteboard photos from the session:



AGREE

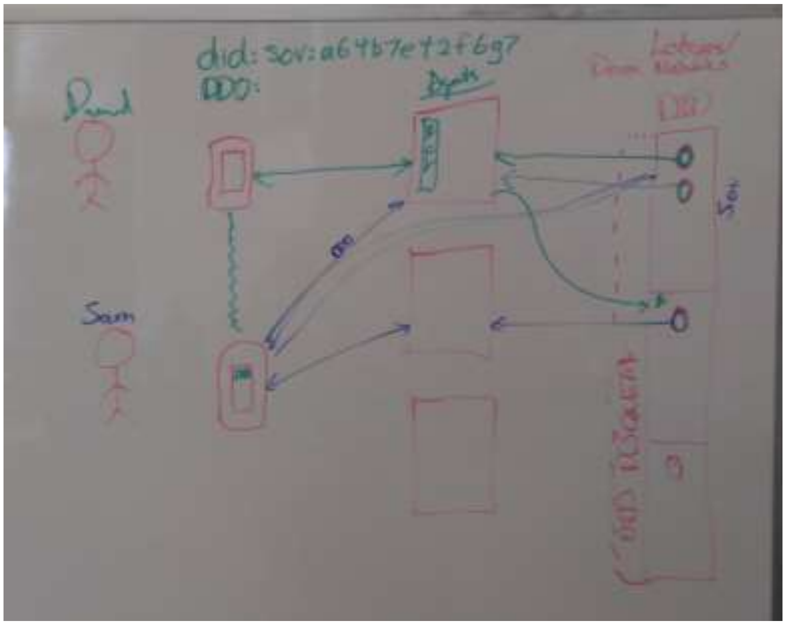
1. Off-chain
2. It's the interface that matters, not the content (API or protocol)
3. It's not just about "data in a box", it's also about messaging and workflow
4. DIDs + DDOs are how you find/prove entities
5. Some form of access control is needed
6. DID/DDO signed requests are one form of auth

OPTIONS

1. JSON API - based
   - Data stored in JSON-LD
   - Schemas are defined by RDF ontologies
   - ACL
2. Agent + Graph Storage/operations
3. Separate agent + data access

ISSUES

1. # of containers
2. Schema/ontology
3. Protocol



Sophisticated Ledgers and Smart Contracts

Thursday 3E
Convener: Bryant Gilot
Notes-taker(s): Bryant Gilot

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

'Sophisticated ledgers and smart contracts – are they useful?'
Bryant Joseph GILOT, MD CM DPhil MSc

A spectrum of ledgers exist including the paper ledger, simple database, distributed database, consensus ledgers with strong immutibilty and trust properties.

Which problems in the ID space are easier to solve with sophisticated ledgers (blockchains - the most robust being the bitcoin blockchain)

Samuel S. 90%+ prop usage of ledgers can be solved using a database.
Few need preventing double spending.

Properties intersting to the ID management (of blockchains/sophisticated ledgers)
Ledger - no intermediaries that can assert control or influence.

No need for trusted intermediaries
Allso possible to have diffused trust across distributred participants.
The governance can also be with a weakened intermediary, a distributed intermediary with an adaptive governance model.

Smart contracts - code, trust the process other than participants

Smart Contracts offer to the ability to automate, verify actions.
They may facilitate access control, granting of permissions.

Distributed, consensus based
Diffused trust, reduce risk
Ledger vs distributed hash table
Time ordered sequence - convenient way
Linerizable
Public disclosure (some information)

Blockchains/Sophisticated ledgers are most interesting for:
1) strong ability for robust timestamping and the ability to order transactions
The ledger is the common source for trusted revocation records.
2) The distributed nature of the ledger diffuses trust in a beneficial manner
3) the distributed nature of the ledger offers robust data accessibilty features.

ID Correlation Startup Architecture

Thursday 3G
Convener: Don Cameron
Notes-taker(s): Don Cameron

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

- a nonprofit legal entity assumes the architectural space to enforce a sociological relationship between the user and the website.
- the user selects a social media identity whose data footprint is mapped to a psychological representation
- the psychological representation is used as an avatar to portray the user's presence across websites they visit.
- the website may request this avatar (value channel) and target content to the dimensional characteristics that map from the avatar.
- the intended outcome is privacy preserving customization of online experience.
- the user is in a position to proactively derive value from data that is operationalized according to their ownership and control.
- a record of connection between avatar and website persisted as a public data point and used to map culture across the net (value channel).

Sovrin Trust Framework

Thursday 4A
Convener: Phil Windley, Drummond Reed
Notes-taker(s): Phil Windley, Drummond Reed

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

Here is the link to the Sovrin Trust Framework Working Group Charter and Workplan (anyone with the link can access):

https://docs.google.com/document/d/10fuBCLyTVXyrNsdODHtd90QnmmENGz5fzENhKEHNVac/edit#

Time and Identity in Physics II

Thursday 4G
Convener: Paul Borrill
Notes-taker(s): Paul Borrill, Andy Radle

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

Identity and The trouble with timestamps

References

https://www.youtube.com/watch?v=CWF3QnfihL4 (Paul's talk on Lamport's Seminal Paper is the main talk, starts 32:30 in — slides).

https://www.youtube.com/watch?v=SfvouFIVCmQ (Paul's 2014 talk, more on the physics intro. — slides).

Without getting into the Quantum Information Theory, the basic idea (for computer scientists) is that time is a 1-dimensional phenonemon (along a path of constantly reversing information and time between an entangled pair). Bell's inequalities have been telling us for a long time now that there is something wrong with Minkowski spacetime. Summary. The original paper is here.

Alan Karp and Paul Borrill are currently scheduled to do a further Talk at Stanford on November 16th,2016, where we will demonstrate a new link protocol with the property *"I know that you know that I know"* (IKTYKTIK), which allows us to replace failure detectors, timeouts and heartbeats in scalable distributed systems for datacenters.

We view time as Aristotelian: "change we can count". By change, we mean quantum information, subject to the Born squared modulus rule when observed *locally*.

The subtime conjecture predicts that: (a) time emerges from entanglement, and (b) entanglement is real, but quantum computing is an illusion. An experimental illustration that time emerges from quantum entanglement was published by Maccone, Lloyd & others. And benchmarks of the D-Wave Machine appear, according to Scott Aaronson, to show no evidence of *quantum* speedup. Checkout the Google hangout on November 8th: https://plus.google.com/+QplusHangouts/posts/EoCJW8wGrDi

While these results may be far from conclusive from a scientific perspective, if this insight turns out to be even partly correct, it opens up the **potential for a revolution in the computer industry** by transforming the way we incorporate the concept of time (liveness) in the design of hardware, software, networks, protocols and storage; and the potential to dramatically simplify the algorithms that govern consistency in distributed systems such as consensus, atomic broadcast and transactions.

This is why we (at EARTH Computing, inc) are looking at the fundamentals of communication between computers to create our company's mission of simplicity, resilience & security.

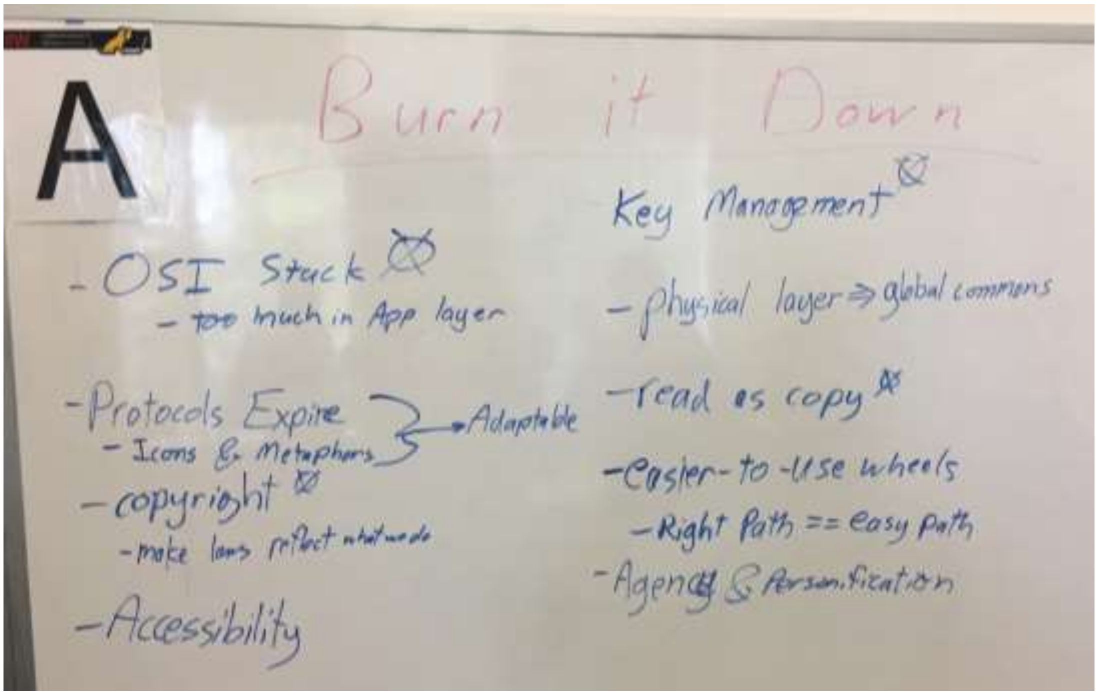
Burn it Down and Start Over

Thursday 5A
Convener: Justin Richer
Notes-taker(s): Andy Radle

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

Discussed items folks would like to really get rid of or change that cause various problems in the Internet world. Items with circled X are items to get rid of. Items without the circled X are things to create.

Everything is Shoes - The way it should be reflects how shoes were a step forward that allowed humans to do much more and travel further distances. They are nearly ubiquitous, easy to use.



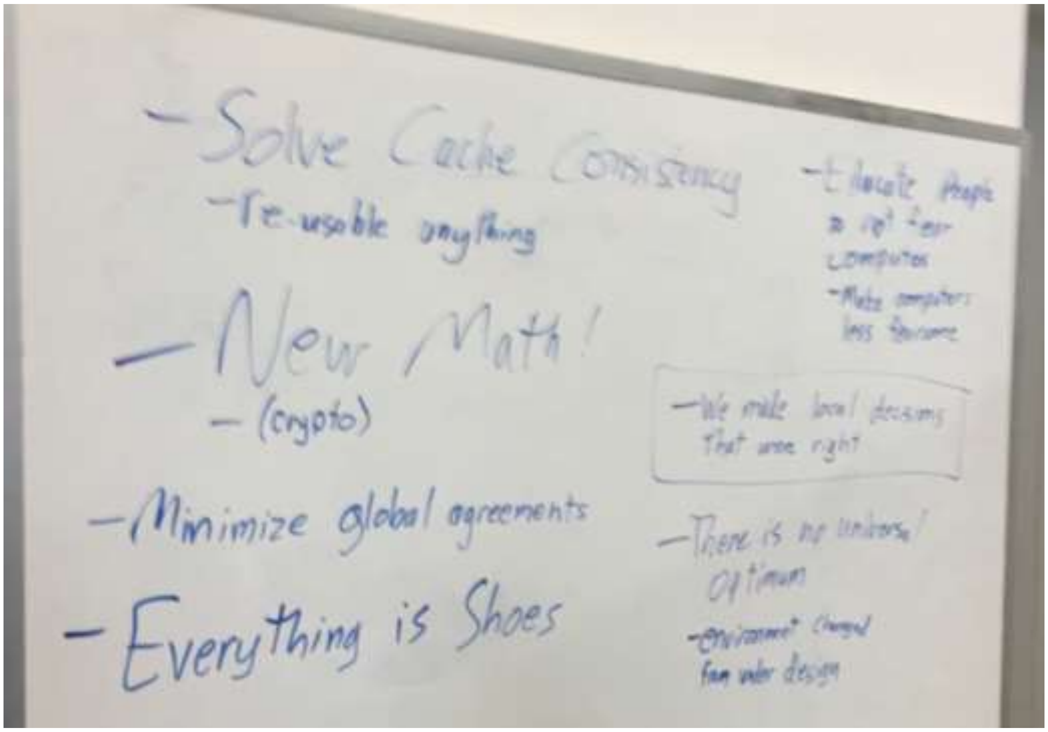
A

Burn it Down

- OSI Stack ⊗
  - too much in App layer
- Protocols Expire
  - Icons & Metaphors → Adaptable
- copyright ⊗
  - make laws reflect what we do
- Accessibility

Key Management ⊗

- physical layer ⇒ global commons
- read as copy ⊗
- easier-to-use wheels
  - Right Path == easy path
- Agency & Personification

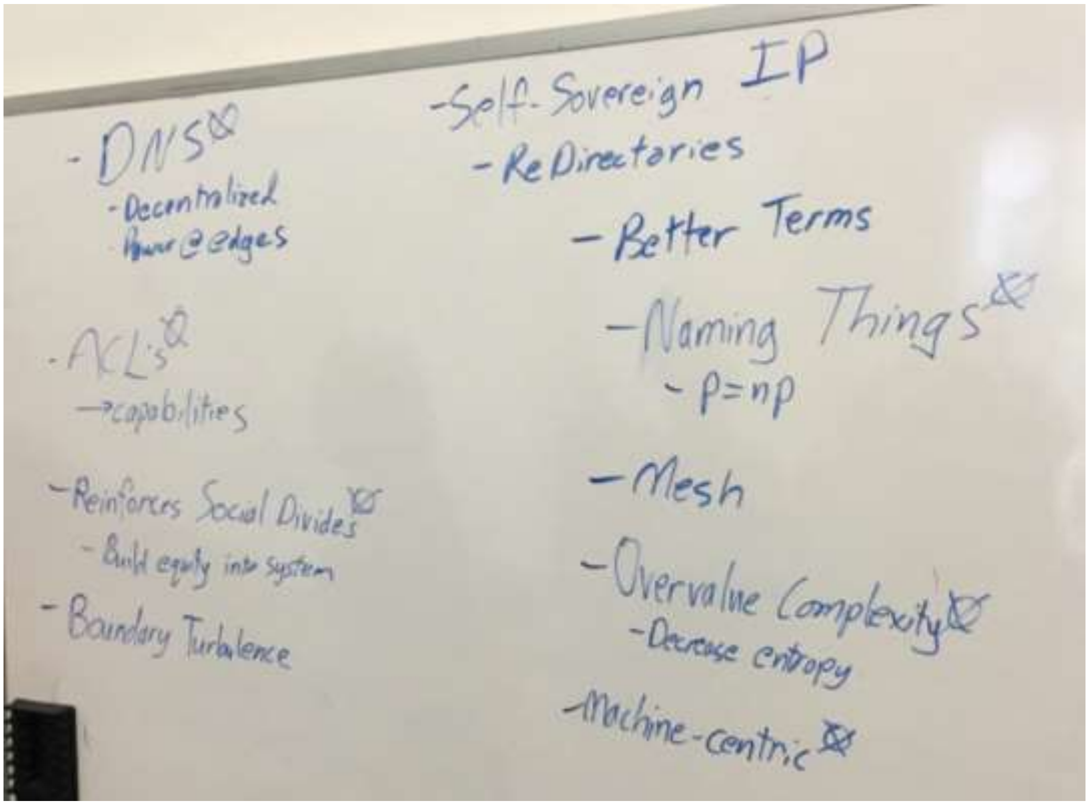


- Solve Cache Consistency
  - re-usable anything
- New Math!
  - (crypto)
- Minimize global agreements
- Everything is Shoes

- Educate people to not fear computers
- Make computers less fearsome

- We make local decisions that are right

- There is no universal optimum
- Environment changed from under design



- DNS ⊗
  - Decentralized
  - Power @ edges
- ACL's ⊗
  → capabilities
- Reinforces Social Divides ⊗
  - Build equity into system
- Boundary Turbulence

- Self-Sovereign IP
  - ReDirectories
    - Better Terms
    - Naming Things ⊗
      - p=np
    - Mesh
    - Overvalue Complexity ⊗
      - Decrease entropy
    - Machine-centric ⊗

Will Smart Contracts Drive Civilization Over a Cliff?

Thursday 5G
Convener: Kaliya
Notes-taker(s): Bryant Gilot

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

Smart contract are an interesting technology with potential dangers. Smart contracts function as autonomous agents. If not properly designed they can be dangerous.

A flawed smart contract deployed in critical settings will have serious negative outcomes. Safe deployment of smart contracts requires consideration of numerous factors.

The smart contract code must be bug free.

A flawed smart contract could execute in perpetuity with unintended outcomes if not designed with proper precautions. If the smart contract is deployed on an immutable platform, buggy code is unacceptable.

Immutable smart contracts should include certain design features. Specifically, smart contracts need to be designed with an escape hatch allowing an authorized entity to abort execution of the smart contract. Secondly, critical parameters should not be hard coded into the immutable smart contract itself. Mechanisms to modify the behaviour of the smart contracts must be incorporated into smart contract code. Safe design dictates that smart contracts must point to parameters and variables external to the smart contract code and modifiable by authorized individuals.

See the following links.
The Ethereum/DAO is an a demonstration of a smart contract gone wrong.
Code is Cruel - http://blog.cryptoiq.ca/?p=512
Code != Law - http://blog.cryptoiq.ca/?p=534

Demo Hour

IIWXXIII #23 Community Sharing / DEMO LIST
Wednesday October 26, 2016

Thanks to our Demo Hour Sponsor

LOGIN WITH amazon

1. **Verifiable Claims Ecosystem Demo:** Manu Sporny
   URL: http://w3c.github.io/webpayments-ig/VCTF/architecture
   See a demo of the Verifiable Claims Ecosystem in action. Part of this work is proposed for standardization at W3C. The 5 minute demo covers a self-sovereign verifiable claim being issued, stored, and used.

2. **YubiKey Demo:** Stina Ehrensvard, CEO and Founder & Chris Streeks, Solutions Engineer
   URL: https://www.yubico.com/products/yubikey-hardware
   We'll demo the versatile YubiKey, which supports open standards such as PIV, OATH, OpenPGP and FIDO U2F. Use U2F strong authentication to log into Gmail, Dropbox and now Salesforce among others. See PIV capabilities for MacOS Sierra log in. Use the same Yubikey with Windows Hello to unlock your Windows desktop.

3. **HIE of One, PBC and HIE of One:** Adrian Gropper
   URL: http://hieofone.org
   HIE of One is a proof of concept for self-sovereign support technology based on UMA. Using healthcare as the demo domain, Alice operates her own authorization server and manages policies re: OpenID Connect. Soon, we will also include blockchain standards for self-sovereign ID.

4. **Lumenous, the first credit "non-bureau,":** LaVonne Reimer
   URL: www.lumenous.net
   The first credit bureau launched in 1841. The model has not been rethought, until now. Lumenous puts business owners in charge of personal and business data used to verify identity and decide on credit terms, loans, and more. See how first user value will turn into trust graph.

5. **ÆVATAR , your Digital Companion:** David ROBERT President & Founder ÆTERNAM
   URL: www.aevatar.com   www.aeternam.eu   ÆTERNAM a “Common Interest Cooperative”
   ÆVATAR is the first self-Sovereign Identity management Companion offered to each EU Citizens, conforming to EU Privacy Regulation (GDPR, eIDAS) and UN ID2020 recommendations for Self-Sovereign Identities. ÆVATAR is govern by a Common Interest Cooperative (1 person, 1 vote).

6. **digi.me –current PC/Mac, iOS and Android version application:** Jim Pasquale & Julian Ranger
   URL: http://get.digi.me for product and https://blog.digi.me/2016/09/29/who-am-i-iamdata-a-new-digi-me-campaign/ for vision
   Demo shows what users can do when they own and control their own data on their own devices(s), initially with social data aggregation of different accounts, which is fully curated – providing peace of mind, flashback perspectives on social interactions with likes, comments and photos including meta data, universal search, customizable widgets for building collections, creating journals, empowering individuals to make better decisions.

7. **ONTY:** Simon Jones
   URL: onty.com
   ONTY – "a connected notebook for private sharing". ONTY is a new communication medium based on a concept of private matching / sharing. Think matching mindmaps mashed up with skype. The perfect VRM venue for your side of the intention market.

8. **Pico Labs at Brigham Young University:** Bruce Conrad
   URL: http://www.windley.com/archives/2015/11/reactive_programming_with_picos.shtml
   We show how the identity and life history of things in the IoT can be represented by picos. Each pico, hosted on a pico engine--local or in the cloud--uses the actor model to respond to events and queries; runs rules in a single thread; communicates through Internet-hosted APIs.

9. **Demos of current state-of-the-art of XDI:** Markus Sabadello
   URL: https://xdi2.org/demos.html
   Demos of current state-of-the-art of XDI, including: Use of XDI link contracts for GDPR-compliant sharing of personal data of a train passenger traveling through multiple E.U. countries ("European Passenger Record"). & Use of XDI connectors for interoperability and data portability between personal data stores (e.g. CozyCloud, Meeco).

10. **"What would you like in YOUR consent receipt?" :** John Wunderlich
    URL: http://kantarainitiative.org/confluence/display/infosharing/Consent+Receipt+Specification
    You've heard about consent receipts, but now we're going to show you some examples and ask for your feedback.

11. **Best Innovation Group (BIG) / Setit Credit - Updating consumer payment data across the web with a single click:** John Best, CEO of BIG
    URL: http://www.setitcredit.com/ Site will be completed this weekend
    The Setit Credit app allows consumers to easily push tokenized payment information to multiple sites at once. This is not just a convenience to the consumer, but resolves some of the challenges facing financial institutions every day such as expired cards and fraud.

12. **Evernym - obtaining and reusing verifiable claims on the Sovrin network:** Nathan George
    URL: http://sovrin.org/
    Associate verifiable claims with a self-sovereign identity. Present claims to relying party... trust becomes easy.

13. **TeamData: Shane Green**
    URL: http://TeamData.com
    Will show our mobile and web apps for collaborative data management, ownership & security in the workplace and teams of all kinds. Based on personal.com platform and data vault.

14. **inWebo Convergent MFA:** Didier Perrot
    URL: https://www.inwebo.com/how-it-works
    inWebo provides organizations with a platform and an API to bootstrap MFA with their VPN, applications, and SSO. *Convergent MFA* means that the easiest and most secure experience is proposed for any given transaction.

15. **Yoti:** Paco Garcia
    URL: https://Yoti.com
    A user centric mobile biometric identity platform with exchangeable identity attributes anchored on e-passports and/or issued by companies/institutions/organizations.

The IIWXXIII Demo List can also be found here
http://iiw.idcommons.net/IIW_23_Demo%27s

Photo Credit #IIW @Windley

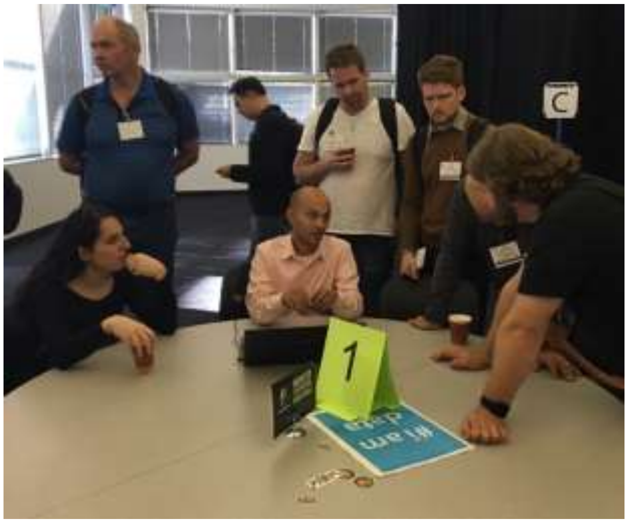


Photo Credit #IIW @JamieXML

Thank You Note -Takers!

There were 88 distinct sessions called and held.

We received notes and/or white board shots or links for 77 of these sessions.

Thanks to those of you who submitted notes and information.

This is the highest percentage of submitted notes to date!

Photo credit #IIW @justin_richer

Does any Canadian woman in London want to have a baby with me?

ONTY.com

IIWXXIII #23 Photos

All the Photo's in this document were posted on Twitter
Credit given at each image ~

WHOEVER COMES ARE THE RIGHT PEOPLE
WHATEVER HAPPENS IS THE ONLY THING THAT COULD HAVE
WHENEVER IT STARTS IS THE RIGHT TIME
WHEN IT's OVER IT's OVER
THE LAW OF TWO FEET
MOTION and RESPONSIBILITY
IF YOU ARE NOT LEARNING or CONTRIBUTING; RESPECTFULLY GET UP AND GO SOMEWHERE THAT YOU WILL!!
Thank You for Breakfast!
evernym

Photo credit #IIW @alain2sf

WELCOME TO THE

vmware

ESPRESSO BAR

V SPHERE
DOUBLE SHOT OF GOURMET ESPRESSO ... STRAIGHT UP

CLOUD CAPPUCCINO
ESPRESSO, STEAMED & FOAMED MILK

VIRTUALIZATION LATTE
ESPRESSO, STEAMED MILK TOPPED WITH FOAM

ENTERPRISE MOCHA
STEAMED COCOA & ESPRESSO

HOT COCOA
YUMMY HOT CHOCOLATE

IIW

Photo credit #IIW @nascarlogin

See you May 2,3 & 4 2017

for

IIWXXIV

The 24th Internet Identity Workshop

www.InternetIdentityWorkshop.com