IIWXXVI

INTERNET IDENTITY WORKSHOP 26

ENDORSED BY HISTORY

Book of Proceedings

www.internetidentityworkshop.com

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

Notes in this book can also be found online at
http://iiw.idcommons.net/IIW_26_Session_Notes

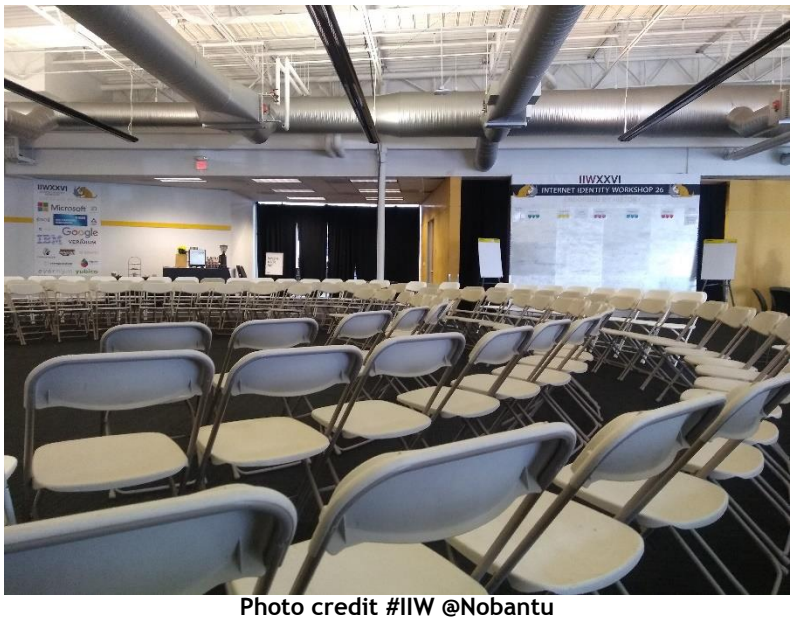


Photo credit #IIW @Nobantu

May 3, 4 & 5, 2018
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

About IIW

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

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

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

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

The event is now in its 13th year and is Co-produced by Kaliya Hamlin, Phil Windley and Heidi Nobantu Saul. IIWXXVII (#27) will be October 23 - 25, 2017 in Mountain View, California at the Computer History Museum.

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

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

Upcoming IIW Events in Mountain View California

IIWXXVII #27
Oct 23,24 & 25, 2018

IIWXXVIII #28
April 30 May1 & 2, 2019

Thank You Documentation Centre Sponsors!

Cirrus Identity

www.cirrusidentity.com/

Social to SAML gateway for universities and other higher education establishments.
Making **identity**management easier for your tech departments and your on-line community.

Internet Bar Institute

https://www.internetbar.org/

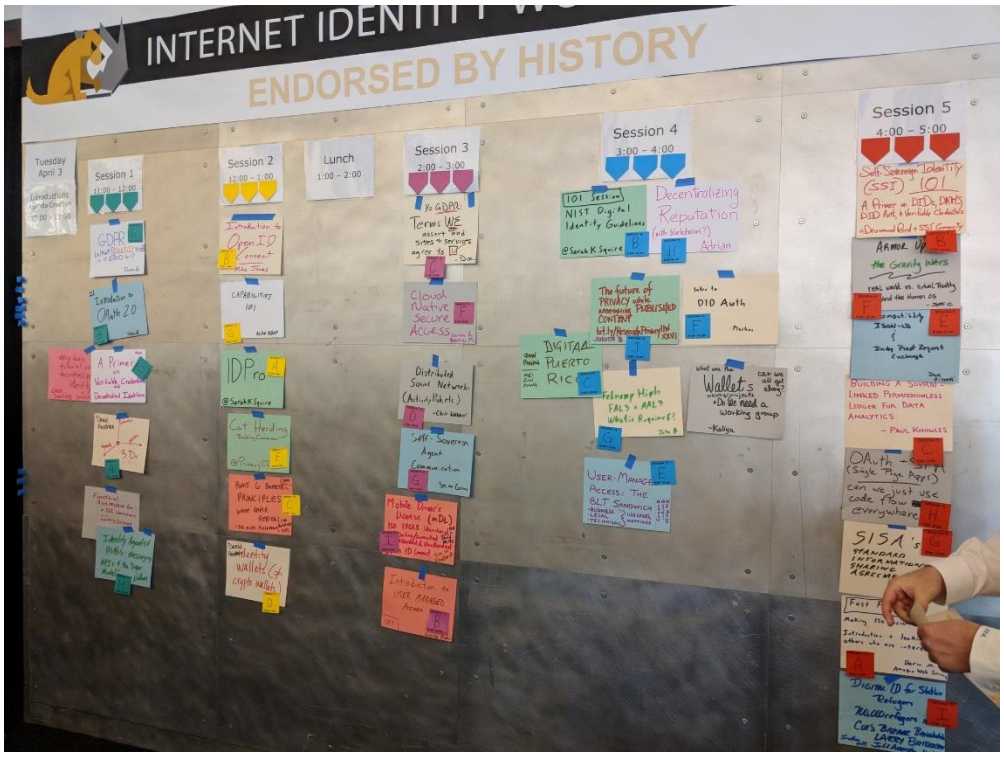
Internetbar.org Institute. Access to Justice Through Technology. Menu. Home · About Expand child menu. Building the Justice Layer of the Internet · Jeff Aresty on Shaping the Rule of Law Online, ... OUR MISSION : mission. To build the Justice Layer of the Internet as a community of equals.

Thank You Notes-Takers!

There were 118 distinct sessions called and held over the three days.

We received notes, links to slide decks, and/or white board shots for 102 of these sessions

IIW 26 Session Topics / Agenda Creation



Sarah Squire @SarahKSquire Apr 3 Ever wonder what identity experts would talk about if they could create their own agenda? Here's your answer. #iiw

Tuesday April 3, 2108

Session 1
1A/3D's of Identity (agents, relationships, ATTR's)
1B/ 101 Session / Introduction to OAuth 2.0
1D/A Primer on Verifiable Credentials and Decentralized Identifiers
1F/GDPR What (Identity Stuff) is it GOOD for?
1H/Identity Agents & HUBS: Messaging API's & the "Layer Model" & Functional Architecture for S.S.I. Blockchain – working session

Session 2
2A/IDPro Organization
2B/101 Session / Open ID Connect
2C/RWOT 6 Biometric Principles White Paper Review
2D/Identity Wallets are not Crypto Wallets
2F/Cat Herding – Building Consensus
2G/Capabilities 101

Lunch
Lunch B/Functional Identity 101
Lunch H/Use = Self Sovereign Bill of Rights = To Update Real Estate Consumer Bill of Rights

Session 3
3A/Self-Sovereign Agent Communication
3B/101 Session / Introduction to UMA = User Managed Access
3C/Yo GDPR: Terms WE Assert and Sites & Services Agree to Check
3D/Distributed Social Networks (Activity Pub etc…)
3F/Could Native Secure Access
3I/Mobile Driver's License (mDL)

Session 4
4A/What Are The 'Wallets' visions/projects – Do We Need a Working Group?
4B/101 Session / NIST Digital Identity Guidelines
4C/Digital Puerto Rico (part 1)
4D/User-Managed Access: The BLT Sandwich – Business, Legal, Technical – Use Cases Mappings
4F/Intro to DID Auth
4G/Fedromp High FAL3 + AAL3 What is Required?
4H/Decentralizing Reputation (with blockchains?)
4J/The Future Of PRIVACY While Accessing PUBLISHED CONTENT

Session 5
5A/Fast Fed – Making SSO Easier to Set Up. Intro and Looking for Others Who Are Interested
5B/101 Session / Self-Sovereign Identity (SSI) DID's, Verifiable Claims etc…
5C/Building A Sovrin Linked Permissionless Ledger for Data Analytics
5E/Compatibility JSON-LD & Indy Proof Request Exchange
5F/ Armor Up – The Gravity Wars ~ Real World vs Virtual Reality and the Human OS
5G/SISA's = Standard Information Sharing Agreements
5H/OAuth + SPA (Single Page Apps) Can We Just Use Code Flow Everywhere
5I/Digital ID for Stateless Refugees

Wednesday April 4, 2108
Session 1
1A/What is Sovrin? How to become a Sovrin Steward. Self Sovereign Identity 102
1C/WebAuthn + DID Auth
1E/Agent/Wallet? What is Agent? What is Wallet? Are They The Same?
1F/Decoupled Flow for OAuth (AKA CIBA)
1G/Zero Knowledge Proofs 101
1H/Native SSO for Mobile Apps
1I/Agent Communication Message Types + Names Spaces

Session 2
2A/DKMS Demo
2C/TheOrgBook / Permitify – Bootstrapping SSI Using A Gov DID/Ver Cred Workflow Implementation
2D/DID Ledger Lightening Talks
2F/What Do You HATE about OAuth?
2G/Publishing & /Advertising After 25 May ADPR Day
2I/Consent As A Service: Making Consent Compliant & Effective
2J/MyCUID/CU Ledger Update & Workshop
2K/Path To Adoption for Self-Sovereign Identity & An Idea For Soverin / Use Cases For
2L/Digital Puerto Rico (Part 2)

Session 3
3A/Quest For The Mnemon Seed #1
3C/Bringing The Best of IIW to India / Making IIW a Global Decentralized Community
3D/Open ID Foundation – Fast Fed & DIDC Federations = Enough Similarities to Share/Merge?
3E/Philosophy of Conscious Body w/Tech, ID Experience & S.O.U. Sovereign Ownership Under Law Prize 10M
3F/Saving Democracy What Could Happen
3G/DID Auth Workflows (Part 2)
3I/ IaM and Iot
3J/Digital Guardianship
3K/Outsourcing GDPR Using UMA
3L/IAB Transparency and Consent Framework
3M/Sovrin – Exploring Building an Alliance Wants & Needs (especially if you aren't Evernym)

Session 4
4A/The Business of Self-Sovereign Identity
4B/Kantara Consent Receipts – Communicating User Consent Between Data Controllers
4C/The "ID" of KIDS
4D/Expanding Language = The Identity of Words ~ Amebic / Shape Shifting
4E/Discussing + Examining CULTURAL BIAS In Specifications and Other Technical Documents
4F/An Analysis of S.S.I. Using Appreciative Inquiry
4G/Mobile APP - APP OAuth
4H/SAML Interoperability Deployment Profile
4I/DID Resolvers & DID JWT
4J/Easy POST Quantum Signature with Block Chain
4K/Separable Identifiers & Intersectional Collaboration
4M/Do-It-Yourself password free! – Cryptographic Authentication for Web Apps

Session 5
5B/Indy 301: Attribute Based Credentials & Zero Knowledge Proofs – Secret Contracts Private Computation
5C/Secure Elements DICE & TPM
5D/Communications Words Storytelling For Humans
5E/GDPR AEORR (requirements + capabilities) Interactive Design Session
5F/Consequential I.D. – How Not To Reinforce Power Imbalances in the Systems You Implement
5G/Phone # Global Identifier
5H/ORCID: What Should It Be Considering?
5I/Veres One (DID Ledger) Deep Dive
5J/Open ID v. FIDO v. SSI
5L/TLS Flex Expanded Library Support For Alternate Certificate Sources
5M/How Are You Making Money In The Sovereign Ecosystem?

Thursday April 5, 2018

Session 1
1A/Solving Professional Credentialing – A Dialogue w/Projects & Companies
1C/Soliciting YOUR Input (help a newbie!) How do You Want To Wield Your Data To Get Things Done? Commerce & ID
1F/Zero-Knowledge Prof's 101 ENCORE – Only High School Math
1G/User-Controlled GDPR Consent Cookies
1H/Cooperation Among Our Communities Owning Interoperable Identities. A Cooperative?

Session 2
2A/InSide Out SID's (Standard Immutable Delegation) & Trustless Distributed Computing
2C/Future of SSI: Tech Scalability & Onboarding Issuers & Identity Holders to Identity Blockchains
2D/REAL Federation
2E/PDX – Personal Data Exchanges – Possibilities Why/What
2F/Addhaar Pros + Cons
2G/Contributing to W3C Standards
2H/Comparing Info Without Revealing It
2I/Agent-Centric v Data-Centric Reality
2J/Digital Puerto Rico – Part 3 of 3
2K/Beyond Early Adopters – Getting the World to Inform What We Build!
2M/Identity Hub Personal Data Store – Soverin Agents – The Grand Unification

Session 3
3A/Mydata Movement – Looking at Identity from the Perspective of Human Centric Personal Data Management.
3C/eIDAS & SSI
3D/Self Sovereign – Reputation – Radical – Disintermediation + 2 Sided Networks
3E/Using Identity Tech To Keep People Safe in the Real World
3F/How Agents + Decentralized Interfaces Help The De-Siloazation of IoT
3G/Designing Ourselves Into The Future & Humanizing DID's + VC's
3H/Hyperledger – Who/What/Where/Why Open Source
3J/Breaking Digital Gridlock – Banking and Identity

Session 4
4D/Massively Multiplayer Online Secure Environments (Games!)
4F/Who Am I? (story time with Marcus)
4G/A Self Sovereign Technology of Stack HIE of ONE
4I/Digital Divide & Gender Equality in Indian Emerging Markets
4J/Value Network Mapping Market Models 4 Self Sovereign Ecosystem
4K/A Conversation About RECOVERING…. A Forgotten Credential Security

Session 5
5A/CRBAC An Introduction
5B/The Sovereign Web-Of-Trust Model / Dynamic Web of Trust?
5C/ID & Connected Vehicle
5F/"Machine Readable User Asserted Terms for Privacy" An IEEE Standard Working Group
5G/Delegation of Authority for Organizations + Services w/DID's + VerfCreds
5K/WHAT IS YOUR PROBLEM? (Bring Me Research)

Tuesday April 3

3D's of Identity (agents, relationships, ATTR's)

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

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

https://docs.google.com/presentation/d/1F3VCYdV3mKwMkeOvojGwHaH9YA0GMblB2MK_B3e9NQw/edit

A Primer on Verifiable Claims /Tutorial on Decentralized ID & Verifiable

Tuesday 1D
Convener: Dave Sanford, Manu Sporney
Notes-taker(s): Dave Sanford, Manu Sporney

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

Dave's slides are here:
https://drive.google.com/open?id=1kJCDF_JcRihUQ5uRFbo47dEJPFsQB7FD

Manu's slides are here:
https://drive.google.com/open?id=1GMQy4rI093c_9zojwLRgp2r-fTscpDUSfX-wqwBk4j4

Verifiable Credentials and Decentralized Identifiers IIW XXVI April 3rd-5th 2018
W3C Verifiable Credentials
What do we mean by Credential?
The mission of the W3C Verifiable Claims Working Group
Express credentials on the Web in a way that is cryptographically secure, privacy respecting, and automatically verifiable.
Anatomy of a Verifiable Credential

- Credential Identifier
- Credential Metadata
- Claims
- Issuer Signature

Verifiable Credentials Ecosystem

- Issuer (Website) - Government, Employer, etc.
- Issue Verifiable Credentials to Holders
- Holder (Digital Wallet / Personal Data Store) - Citizen, Employee, etc.
- Issue Credentials
- Send Presentations to Verifiers
- Verifier (Website) - Company, Bank, etc.

Verifiable Credentials Status

- WG Launch (May 2017)
- FPWD, WDs (Aug 2017-today)
- Implementations (Nov 2017-today)
- Complete Test Suite (Jul 2018)
- CR (Oct 2018)
- PR (Jan 2019)
- Spec/Issue Regular Contributors: 15
- Weekly WG Participants: 12-18 / 50
- Known Corporate Implementation Commitments: 10

Questions about Verifiable Credentials?

Anatomy of a Verifiable Credential

- <IDENTIFIER> <--- this is an issue
- license: I1234562
- hair: BLK
- name: ALEXANDER JOSEPH
- address: 2570 24th STREET …
- date of birth: 08/31/1977
- issued by: California DMV
- digital signature: MIIB7ZueKqp...

Which identifiers do we use today?

- jdoe@bigcorp.com
- https://flitter.com/jdoe

Why is this a problem?

Equifax

The Web's Identifier Problem

To date, every identifier you use online does not belong to you; it belongs to someone else. This results in problems related to cost, data portability, data privacy, and data security.

Web Identifiers Today

Domain Name System (Identifiers are leased to individuals)

What is missing?

Many portable identifiers for any person, organization, or thing that does not depend on a centralized authority, are protected by cryptography, and enable privacy and data portability.

Decentralized Identifiers

A new type of globally resolvable, cryptographically-verifiable identifier, registered directly on a distributed ledger (aka Blockchain)

What does a DID look like?

- did:example:123456789abcdefghijk
- Scheme DID Method
- DID Method Specific String
- Example: did:v1:nym:DwkYwcoyUXHNkpj3whn4DgXB4fcg9gj95vKxYN2apkZD
- DIDs Resolve to DID Documents which hold

1

Decentralized Identifiers

- Decentralized Identifiers (Identifiers are owned by individuals)
- Blockchains / DHTs (Decentralized Ledger)
- Veres One, Sovrin, Bitcoin, Ethereum, etc.

Decentralized Identifiers Status

- Technology Incubation (May 2014 - today)
- Specification and Implementations (October 2016 - today)
- W3C DID WG (Dec 2018-2020)
- Spec/Issue Regular Contributors: 12
- Weekly Community Group Participants: 15-28 / 161
- Known Corporate Implementation Commitments: 13

Implementers

Method DID prefix

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

Get in touch

Manu Sporny | CEO | Digital Bazaar

- Co-Inventor of Verifiable Credentials & Decentralized Identifiers
- Co-Inventor of JSON-LD
- Co-Founder of Veres One
- 10+ Years in Web Standards
- Customers in Finance, Government, Education, and Healthcare
- Email: msporny@digitalbazaar.com
- Twitter: @manusporny
- https://www.linkedin.com/in/manusporny/

GDPR – What [IDENTITY stuff] is GOOD for?

Tuesday 1F
Convener: Dazza G.
Notes-taker(s): Tiemae H. Roquerre and John Fontana

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

Tiemae's notes:

GDPR Session Report Out:

Tip – Skip the first 38 pages ☺

Website: gdpr-info.eu

Interesting App to Use - EDPS

Key Roles: Data Subject, Data Controller, Data Processor, DPO, DPA

Who does this apply to – Any person or any organization

Privacy vs. Data Protection

Key Takeaways:

- Article 7 - Will be as easy to give / revoke consent
- There are many layers to what consent is –must prove that the consent was intentional [clarify]
- Plain language requirement to make all relevant info to data subject easily understandable (Article 12)
- When Data Controller (party who determines the purpose and mean of processing) outsources the role of Data Processor then the accountability changes
- Article 13 – put a lot of the values of the HUE report into practice – pretty much whatever is done to personal data has to be communicated to the data subject by the data controller
- Article 13 (cont.) – Data controller must facilitate how the data subject has the right to request a copy of their data, correct their data, delete their data, and restrict the processing of your data
- TBD – trust services
- Paypal has published paper on what our data is used for and someone has made a map of this
- Article 14 – Data subjects must be notified when data provided by third-parties is used
- Article 15 – one of the most important mechanisms for a fair ecology for use of personal data
    - You can ask a company if they have your data and ask for the company to provide it
    - Huge Issue: A gaping hole is that the company needs to make sure that an individual proves that the data subject is who they say they are – there are easy endpoints now for identity thieves to access personal info from GDPR compliant companies
- Lots of opportunity to facilitate notification requirements for GDPR
- Article 20 – Right to data portability – data subject has the right to move data around to other providers
- Sensitive personal data – very careful management about how this type of data is displayed

    - There are layers of rules around different data categories
- Article 21 – Shifts burden of proof to prove necessity of algorithms onto the controller and changes income model of the commercial internet (point 2)
- Article 22 – Profiling happens only if the data subject consents to it and is made clear to the data subject
- Opinion – GDPRs purpose is to be a proponent of the data subject's rights and perspective
- GDPR provides the opportunity for companies to shift their business models to accommodate these new values
- Cloud Act??

Further Discussion Topics:

- What are the economic consequences for GDPR
- Who will be affected?
- Engineering parts of the GDPR

John Fontana's notes

Dazza - This talk is at a high level on how to scan the doc

What is the ID section?

Article 5 principals are about processing personal data.
Key things in GDPR
Data Subject
Data controller
Data Processor
DPA – Data Protection Act
DPO - Data protection officer
If you are controller of data, you have the data.

Connection point to GDPR is that if you are established co./org./etc.in EU you are subject to these rules.
If you have end-users in the EU.
Important concept: Profiling.

GDPR – citizen have a right to privacy, company has to fulfill those protections.
It is very broadly scoped.

Elizabeth: There is difference between privacy and privacy protection
Data protection is a specific type of privacy.
Part of motivation for GDPR was prior system..

See this page in Github (by
Dazza), https://github.com/PersonalDataFramework/DataProtectionLegalReview
Check out this URL: https://gdpr-info.eu/
One interesting thing on consent.
It is as easy to withdraw consent as it is to give consent
Here is a review of important articles for identity.

Article 7
1. consent. Processor must be able to prove the user provided consent.
2. it is clear that you can play more than role in GDPR.

Ken: there are six justifications for release data, consent is one.
Elizabeth: Consent is hard to rely on , it is hard to prove.
Skipping around…….

Article 12
Under law, in language of US, I would say, there is a plain language requirement in GDPR, dazza.
Data subject must be able to comprehend (the material).
Concise, transparent, intelligible, clear plain language.
Data controller has the direct relationship to subject
The processor is doing stuff on behalf of data controller

Article 13 discussion
There are many things here that those at IIW have yearned for.
Here you have right to request a copy of your data, can apply restrictions of processing data. (this is section 2b.)

Article 15
See 1.X section
Think this will be one of the most important mechanisms for this sustainable ecology for the use of personal data.
Legal name subject to access rules.

You can ask if an entity has personal data on you
Can get a copy, some nuance there.
Elizabeth: Before all of this, you had to prove who you are.
Dazza: processor has a duty not to give away you data to the wrong person.
Sarah: now all companies have to have an end-point that provides all your personal information. – this is gold mine for identity thieves
Dazza: …..or an opportunity for identity (and IIW)

Article 17
Right to erasure, aka right to be forgotten
We have limited right to request deletion of our personal data.
Right to restrictions are interesting. You should read these.

Article 20
Right to data portability
This is another biggie.
Data subject has right to get data in a machine-readable form.
There are security requirements that apply to this
Encryption?
These sections we are looking at are the basic rules.
You have to read deeper to get the layers of understanding.
There is s category called sensitive personal data - be careful what you are asking for and what you

collect on-screen. What is revealed?

Article 21
Right to object
Subject can reject based on there situation…..
Be aware there are some major loop holes and scope limitations.
Section 2 and 3. Are important
The two talk about data processing for direct marketing purposes.
I think 2018 will be remembered as the date of the great data purge. (re:Facebook, social)

Article 22
Talks about automated processing, including profile,
These rules require plain and intelligible language
GDPR does define "explicit consent" (Article 4 contains definitions).
Full focus of GDPR is about the subject.

Dave:
American subjects not subject to GDPR
Generally co. following US citizens will not be subject to these.
Euro. Company's servicing US citizens are not going to be able to make the money they are making on personal information.
This creates a space to find out if those using ad blockers are willing to look at alternative service profiles, then euro companies will start to gain US customers.

Elizabeth.
Any kind of person, server, boot on grounds. Count in context of activity, any services of goods and services.
Other thing that is big is monitoring, any big analytics.
On data processing, because service is data processing it provides the scope.

Identity Agents & HUBS: Messaging API's & the "Layer Model" & Functional Architecture for S.S.I. Blockchain – working session

Tuesday 1H
Convener: Nathan George
Notes-taker(s): Ed Eykholt

Tags for the session - technology discussed/ideas considered:

blockchain, self-sovereign ID, architecture

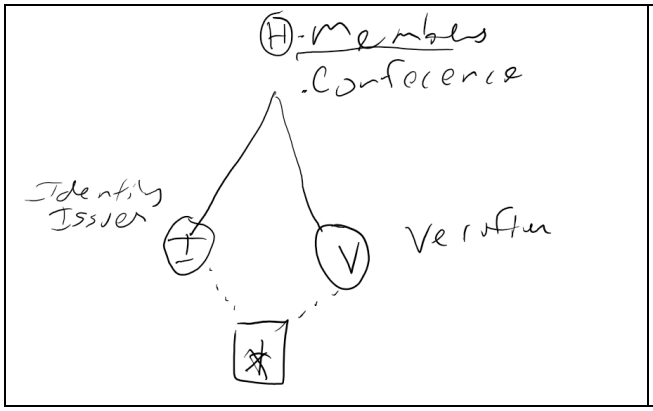
Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

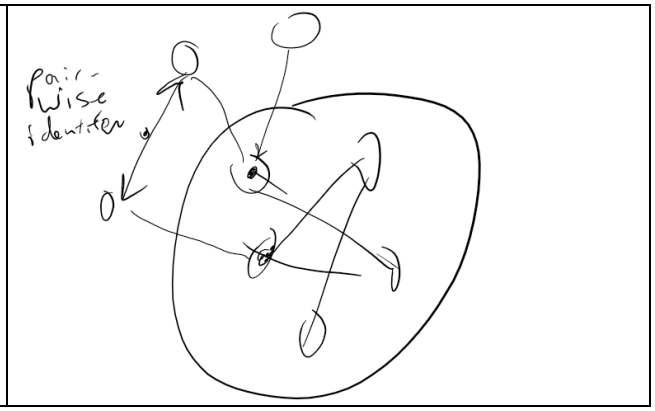
Better title: Functional Architecture and considerations for Identity on Blockchains

- Ledger Identity Models
  - What is a blockchain?
    - Proof of existence. We all agree
    - Proof of "before". "After".
    - "Trustless" system -- can use the crypto math to verify. Collectively we all agree.
    - Byzantine Fault Tolerant consensus
    - Often blockchains will have:
      - Smart contract layer
      - Consensus layer
      - Ordering layer
      - Distributed Smart Contract architecture allows for more validity.
    - Two basic models for blockchains UTXO (Bitcoin) and Smart Contract/State (Ethereum)
  - What do we want to do for Identity on blockchains?
  - An entity is represented by a cryptographic key. (Key management)
  - Identifier, Keys, Attributes (bind to keys and/or identifiers
- Why is a blockchain needed?
  - It's not, but it's a way that everyone can equally trust the root of trust.
- Is identity on the blockchain enabling the bad guys?
  - It could if verifiers must disclose those events. (making correlation easier).
  - SSI opposes implicit tyranny, but doesn't stop it.

- Risks of on-chain identity data is Correlation.
  - **"Keys constitute a unit of correlation". If you want something not correlated, you need to use another key.**
    - Anti-correlation is wicked hard: must Avoid ANY majority and Avoid ANY minority.
    - Sovrin calls these parties Trust Anchors, building out a web of trust.
    - Correlation is contagious!
  - Usability. E.g., to get around correlation? How much is enough, and how much is too-much?
  - Don't put too much on the ledger, since it can't be undone.
- **Patterns of interactions**
  - Most occurs off-chain (see below)
  - Initiated by Issuer

        - **When there are credentials issued there are B.L.T. (Business, Legal, and Technology) guarantees.**
    - **Initiated by Holder**
        - **The unit of interoperability is what the holder decides to tell someone else, not the issuer.**
        - Most selective disclosure should be based on ZKPs.
        - Identity Agent
            - An Identity Agent (software that control keys and can sign on behalf of the entity) is needed. … delegate responsibility to a key and later revoke it. In case an Identity Agent goes rouge.
        - Key Management
            - Other keys can be used for private, off-ledger interaction. For details, see DKMS topic/session.
                - See also Identity Mixer, U-Prove, Indy's Anoncreds.
                - Blinded Commitment / Petterson Commitment
            - You are self-sovereign over keys and identifiers; Data is about relationships, and you were never self-sovereign about that.
- On-Ledger Data (public ledger)
    - OK
        - Bootstrap consensus of ledger, establishing web of trust
        - Addresses of blockchain nodes
    - Not OK
        - Identifiers
        - Attributes (which bind to keys and/or identifiers)
        - PII, Biometrics
    - Concerns
        - What is "secure" now might be secure now, but it must stay secure on human timescales.
        - See magic penny video by Sam Smith. Not all the pennies are in one safe.
        - One can have a mountain of data, but they must not come along with the keys.
        - Equifax and others know more about us than we can remember.
- Off-Ledger Interactions
    - Exchange of Verifiable Information
    - Agent Messaging Protocol (for off-chain …)
    - One of challenges in designing an ecosystem is to enable Verifiers to pay Issuers.





IDPro Organization Roadmap

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

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

Exists Today

- Discussion and announce email lists
- Slack
- Newsletter
- Meetups
- Identity Event Tracking (https://idpro.org/events)

Soon

- RSA Meetup
- Enterprise Membership
- Job Board
- Speakers' Bureau
- Skills Survey

In the Future

- Body of Knowledge
- Certification

Potential Future Work (brainstormed ideas from IIW attendees)

- Global apprenticeship (hands-on experience as opposed to multiple choice test)
- Job classification
- Best practices around identity/security events (secevents)
- Promotion of human-centered architectures
- Student involvement
- Education of CMOs
- Identity Maturity Models
- University Outreach
- Clearinghouse for grad-student-appropriate identity projects
- Outreach to IEEE Young Professionals
- Highlight the potential for emerging markets to reframe identity assumptions
- Interdisciplinary/international programs
- Explanation of the value of identity proofing to those who take it for granted

OpenID Connect Primer – 101 Session

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

Tags for the session - technology discussed/ideas considered:

OpenID Connect based on OAuth 2.0, more specific
OpenID 2.0 obsoleted ~2015
question about multifactor authentication – not covered in the presentation – from Mark Rank of Cirrus Identity (mark.rank@cirrusidentity.com)

OpenID scope
Implementer's Draft for session management/logout; there are 3 separate methods, appropriate for different use cases (Session Management, Front-Channel Logout, Back-Channel logout)

Federation specification (InComon, nordunet, etc used in academic and research settings)
OpenID Connect Federation specification enables establishment and maintenance of mlti-party federations using OpenID Connect. Defines hierarchical JSON metadata for federation participants
How does DD relate to OpenID?
You could define a DID which triggers an OpenID login

OpenID Certification program
- Technical evidence of conformance resulting from testing
- Legal statement of conformance

Call to action to get your OpenID implementations certified, and to give feedback on the additional tests being defined now.
Invitation to join the mailing list (lists.openID.net/…/opened-specs-ab

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

Question: how do you know when you're done testing for security vulnerabilities, given that new attacks are being developed all the time
Good question. Some of the most important tests are negative tests. For example, one of the most important tests for a relying party is, 'Are you checking signatures at all?'
We are trying to cover all the MUSTS I the spec

Are there periodic updates to the certification process?
Yes – there are version identifiers that tie to version s of the certification test software version

http://self-issued.info/?p=1812

RWOT 6 Biometric Principles

Tuesday 2C
Convener: Jack
Notes-taker(s): Asem Othman

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

In this session, we discussed the six principles for self-sovereign biometrics.

Biometrics are already here, and they will be used on the internet, whether we like it or not. They are already are; a lot of the current practices are bad and the centralized hosts know it. We know that centralized repositories of sensitive information are highly vulnerable and present irresistible targets, but better solutions are not available to current practitioners; they're not even being considered. Fortunately, there are other fields that are already solving these problems, such as self-sovereign identity. We need to adapt their best practices to make biometrics safe and secure.

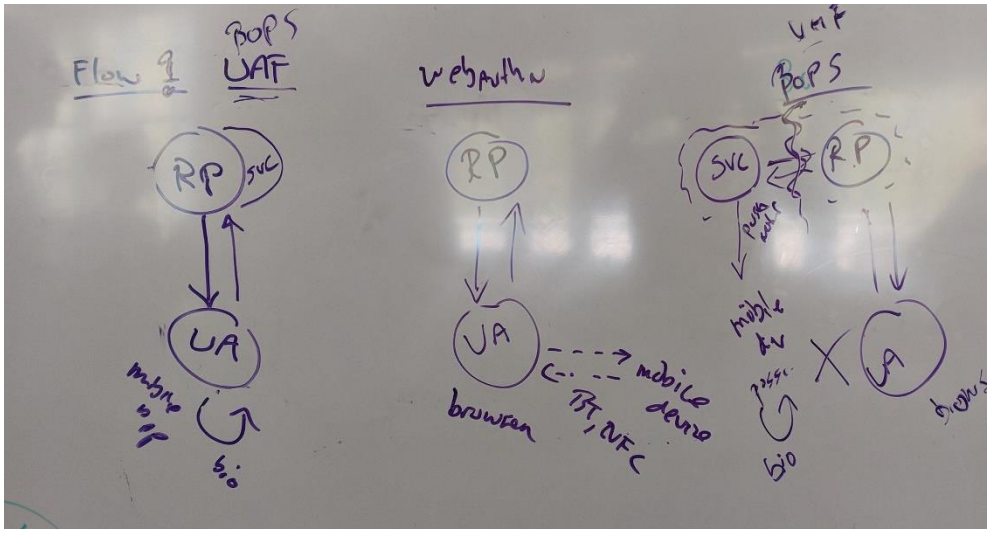
Therefore, during rebooting the web of trust workshop last month, a group start working on these principles (https://github.com/WebOfTrustInfo/rebooting-the-web-of-trust-spring2018)

The presenter discussed and enumerated the principles that have been detailed in the GitHub (https://github.com/WebOfTrustInfo/rebooting-the-web-of-trust-spring2018/blob/master/draft-documents/Biometrics.md)

One of the interesting suggestions is mentioning the different factors of usability of biometric traits and systems in order to be adopted in large scale.

Another suggestion is adding the concept of trust sensors similar to the Adhaar idea of registered devices that their identifiers should be added to the packet that will be sent along to the biometric data to the Adhaar database for verification of the data.

Finally, the presenter discussed few flows of using the biometric along with DID Auth. (check the picture)



Identity Wallets Are Not Crypto Wallets)

Tuesday 2D
Convener: Daniel Hardman
Notes-taker(s): Karan Verma

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

- What is an identity wallet?
  - Digital container belonging to a single identity owner that holds secrets, money, credentials, and miscellaneous related items.
  - Implement best practices and standards for distributed secrets and key management, for maximum security and privacy
  - Has an identifiable location on hardware
  - Unit of portability - mostly, move a wallet, move an identity.

- Question Why is it called a wallet?
  - Because of cryptocurrency wallet
  - Is there a better name?
    - Holder
    - Keychain

- What is and should be stored in an indy wallet?
  Bunch of different things that go into an identity wallet
  - Key pairs
  - Cryptocurrency keys and HDKeys indexes
  - Link secret
  - Policy address (and agency policy registry doc?)
  - Cred def keys
  - Credentials
  - Symmetric keys
  - Tails indexes, witnesses
  - Cache of other party's pub keys -> microliter
  - Tails file -> file system (not private)
  - Proofs from others?
  - Other identity info

- Cryptocurrency wallet != identity wallet
  - Cryptocurrency wallets just hold keys
  - How many things do you put in a cryptocurrency wallet
  - Some put your secrets in cloud, managed by another party
    - Identity wallet cannot be all in the cloud

- Vault != wallet
  - Vault is virtual construct — same boundary as a domain

- Includes data of all kinds, located in all places under owner control: wallets, proofs, genome, tax and legal records, private docs..
- Security and privacy of a vault is not standardized

Comment

- Identity wallet vs cryptocurrency wallet
    - Need to put lot of data in the wallet
    - Hardware to store symmetric keys
    - There are different requirement
        - There are different use cases and they are not exactly the same thing.

Questions

- Natural scope of a wallet is similar in the digital world and physical world
- Stateless refuge location
- Self sovereign identity for my connections
    - In a at risk situations, can I get to my wallet through biometrics? Is that somehow connected to the wallet?
    - Keys are tied to relationships, when you have a wallet you have your connections.
    - Wallet are set of things which are on a particular device.
- Curious about identity - people cannot take away from you - does self-sovriegn apply to wallet/ is it completely in users control?
    - Self-soverignity has to be a characteristic of the wallet.
    - There is difference b/w verifiable information and sensitive information.

  Browser Password Synch: sensitive data is never stored on the server, probably should have one wallet. Shouldn't probably make that distinction b/w cryptocurrency wallet and identity wallet
        - Distinction made for implementers not for users - Users get a unified experience.

Cat Herding – Building Consensus

Tuesday 2F
Convener: Phil Wunerlich
Notes-taker(s): John Fontana

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

Anybody who has been in org. of standards org.
To produce a report a project,
Sometimes it works
Sometimes NOT. This is most of the time.

How do you herd cats. Best you can hope for is to make everyone equally unhappy

God or evolution gave you two ears and one mouth for a reason.

I do want to not herd the cats here, but hear your rules of the road.

Doc: You have to start with will no do exactly what you want them to do.
The way we communicate , often people pickup their meaning and not yours

Wendall: Edmund Muskie reference.
Let people speak and be heard.
Hou hav eot let people be heard

Eve: thiat is part of Robert's rules of order.
Majority or consenssue
What do you prefere.
Voting is procedure to produce consensus.
Then you need

Justin: You need someone who takes responsibility for doing the driving.
It wasn't my job to drive those things, my job was to make the group decide.
Tools and techniques for making group make a decision
on thing that I did tow things
I did very clear lists of options to start a debate.
Let people vote on the option or no optiosn.
Or people did not want to vote, they just want a solution so they can get to there question.
The other thing was to put very clear time limits on discussions.
To drive things to a completion, give a time frame and then we will make a call.

??? the recognized driver has to facilitate the writing down on things.
A group does not write things. A person does, the group comments.

JohnW. For some groups, lug people tend to dominate.
So chair has to make sure peole that are not loud are heard
Sometimes you can use silence to make sure you draw out people

JohnP. Building alignment in advance, but if you know wher people sit already, that can help speed things up - be a facilitator.
You need the group to be diverse.
Is there wide enough support for something, or is consensus amnong all the people from certain company

??? I find having clear staremetn of work helps lwith diversity

JohnP: Decision clarity is important.

Wendall: For some groups, there is sunshine requiremments, all work has to hapend in group, you can't piece things off to side-alignment
Side-alignment can be counter-productionve

Eve: corporate politics.
We are talking about individuals, but the reasosn most of this activity gets done is biz.
Biz imperatives drive who is at the table or lack of biz imperatives.
The governance model under which yo labor determines al ot of your choices.
Around governance:
There can be people who do what amounts to a Ddos attack
They flood the group with various work.
Make them go off and do the work – in writing

John W. Rat hole diversion
Let some one propose a rat hole and ask they to explore and write it up
You get rat hole diversion

When consensus isn't working I call for votes. I becomes a road block
How do you deal with that person when it is happening?

Jogil: Consent over consensus.
It means is it OK to go one.
Everybody shows they are for it
Not against it – but want to voice….
If yo have objecdtion, you keep it , but keep it specified.
Not just objection for objection, you nedto expain and take to new level.
You can do this by hand gestures.

Eve: Knowing objections is important – if you wait you are asking for trouble.

Person 1 : Get to beliefs of the underlying assumption.

Justin : Can help to go balkc to clear startement of purpose.
If per son thinks ther are two ocmopetting ideas – what are you trying to solve, what is driving yo to this solution. – can't just say I like it bedause this is my way.

T: Sometimes communication is broken by symantecs. What are you getting at, don't listen to the words.

John W. cross cultural makes this difficult, you can have a level setting session at the bginning to try to understand how people communicate.

T: in China the word privacy has a different meaning than in the US

Roland: You have to level the playing field
Couple issues I had.
All these diff levels of understandings. Who read draft, who skimmed?
Cats, some are pumas, some are kittens.
People are typically in a group representing something and they can force their will on group.

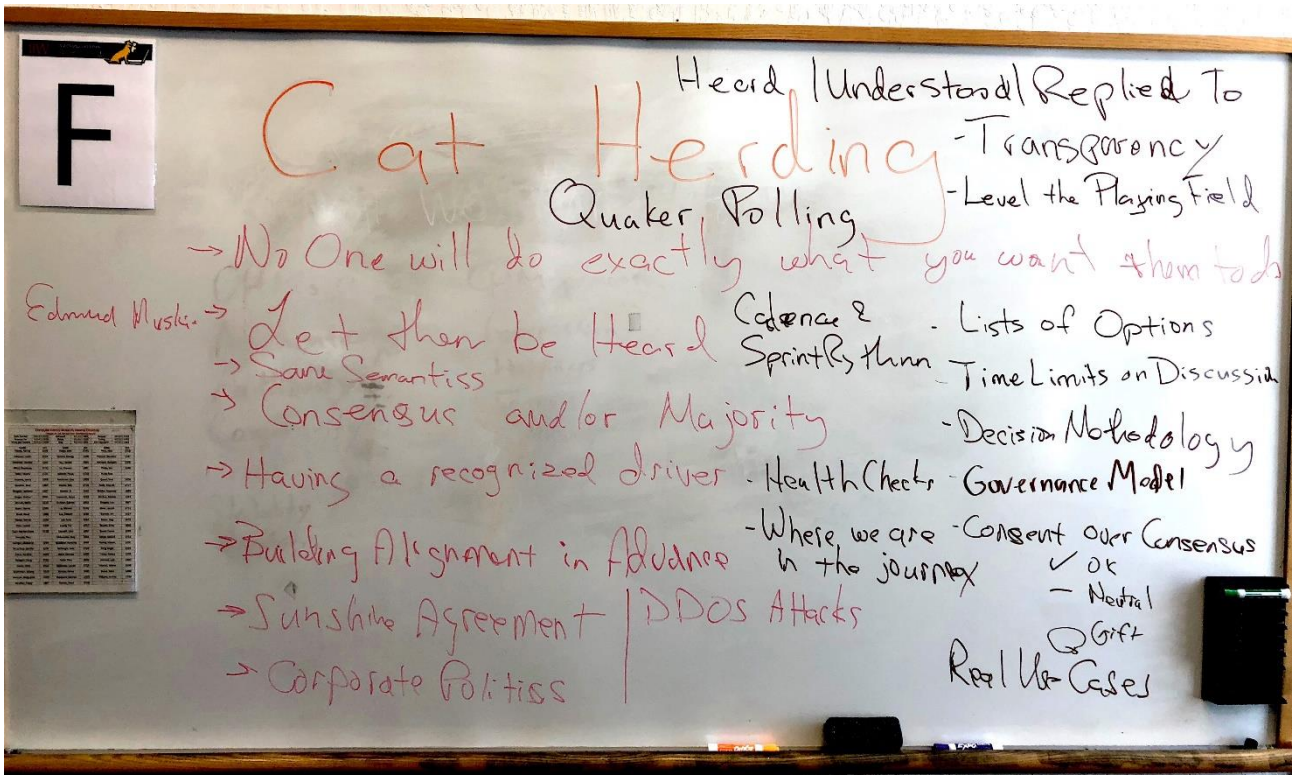
???? diversity matters.
You might not have ultimate control, but you can lobby for someone with a certain point to join the group, so that opinion is heaerd.

Jogil: If you force everyone to say something, it is good for the group.
Understand the silent ones.
If yo force evyerone to answer a question, you find out a lot. Like who doesn't udnerstnad the question.

Victor: Consensus, words mean different things to different people

Jiustin: isn some orgs. The IETF, someone can strongly disagree and consensuses can be called despite that objection
State why you disagree and acknowledge that things are moving on so it is written down

johnW – should there be a minority and majority report?
Is that a viable way out.
You can you discover divergent opinions and they are on the record.



Capabilities 101

Tuesday 2G
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:

Slides are at: https://www.dropbox.com/s/h73vltljkzoroob/Caps101.pdf?dl=0.

Functional Identity 101

Tuesday Lunch B
Convener: Joe Andrieu
Notes-taker(s): Joe Andrieu

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

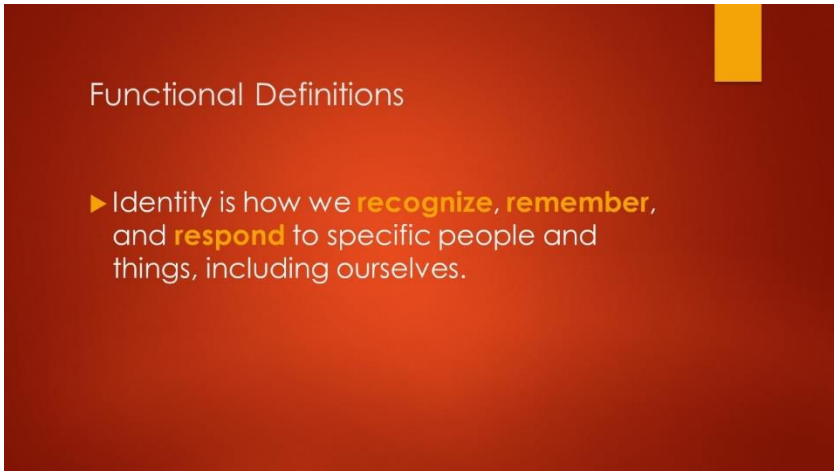
Functional Identity 101
Joe Andrieu, PMP
Internet identity workshop XXVI
April 2018
Functional Identity
Approach to understanding, discussing, engineering identity
HOW identity works
HOW people use it
NOT Functional Identity
Who you ARE? Who I AM?
These are philosophical, psychological, meta-physical, cultural, political questions

We are engineers & system designers
What's the function?
NOT Functional Identity
Compositional identity
Identity as set of attributes
"Identities" as digital assets
"Identities" as independent actors
Identity >> Digital Identity
We are more than our digital record
Digital Identity is a tool
Identities are cross-context
Stop treating digital identities in isolation

ISO/IEC 24760-1 got it wrong
"set of attributes related to an entity"
Functional Definition
Identity is how we recognize, remember, and respond to specific people and things, including ourselves.
Terminology
NOUNS
> Subjects
> Identifiers
> Attributes
> Raw Data
> Context
VERBS
> Acquire
> Correlate
> Reason
> Apply
> Govern

Alternative Terminology
> People
> Names
> Knowledge
> Observations
> Situations
VERBS
> Collect
> Relate
> Consider
> Use
> Control

--
Joe Andrieu, PMP joe@legreq.com
LEGENDARY REQUIREMENTS +1(805)705-8651
Do what matters. http://legreq.com



Use = Self Sovereign Bill of Rights = To Update Real Estate Consumer Bill of Rights

Tuesday Lunch H
Convener: Bill Wendel
Notes-taker(s): Bill Wendel

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

Thanks for your post IIW email. Responding to your invitation to follow-up re "Keep in touch if you are interested in participating in SSIMeetup in the future." Invite you to think about how to open this conversation via the SSIMeetUp network:

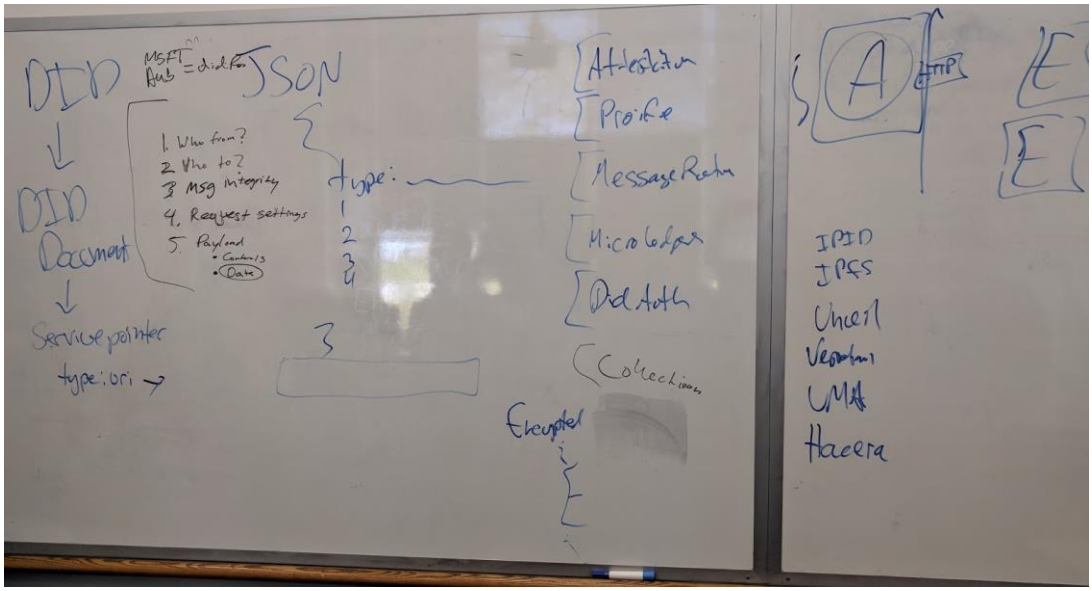
Notes referring to this session can be found here: http://bit.ly/ConsREvRights

Self-Sovreign Agent Communication

Tuesday 3A
Convener: Sam Cullen
Notes-taker(s): Sam Cullen

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

Good discussion of basic compatibility of hub communication. Another session will follow.



Introduction to User Managed Access (UMA) – 101 Session

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

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

Slide deck:
https://kantarainitiative.org/confluence/download/attachments/17760302/2018%20IIW%20User%20Managed%20Access%20v2.pptx?api=v2

UMA is based on OAuth. In OAuth, Alice shares access to resources "with herself" — to a service that she uses. George doesn't share access to a photo with Eve, but to an app he uses. In UMA, George can share access to the photo with Eve. In OAuth, the user experience requires George to approve access at run time. In UMA, he can also arrange to share access ahead of time, or after Eve attempts photo access, and can monitor access over time, and can withdraw access over time as well.

So UMA gives resource owner-defined control, dealing with access requests from arbitrary clients.

Why is this important? Evolution beyond consent, consent at times other than run time, audit and transparency, mutual consent between parties, IoT identity combined with human identity and consent, etc.

UMA is now at V2.0, which is improved. UMA V1.0 had to invent a bunch of technologies, which ultimately matured elsewhere. The two specs are now broken up into an OAuth extension grant and a "federated authorization" interface between the resource server (say, a photo service) and the authorization server.

This interface lets the photo server inform the AS about just enough resource info to let Alice express her resource-sharing wishes. The AS-RS loose coupling enables the resource owner potentially to manage sharing in a central way and enables the RS to offload management of policy decision-making.

Q: What implementations are there? ForgeRock, Gluu, RedHat Keycloak (partial), MITREid Connect (open-source project), more; see the Implementations page on the Kantara UMA Work Group wiki, for which the short link is http://tinyurl.com/umawg.

The UMA grant flow starts with requesting party's client making a request for the protected resource at the RS first, being told which AS to go to in an as_loc response, and being given a permission ticket. This structure is a means of saving state as the client moves to the AS and comes back to it possibly repeatedly.

Q: So I don't have to have the same company doing the auth as hosting the data? Correct.

Resource registration is the process that allows outsourcing of authorization policy of RS endpoints to the AS.

Q: Does this satisfy GDPR? You can use it to help prove certain GDPR compliance aspects. The "BLT sandwich" session in the next hour has some implications for that too. The RS is going to want to be quite certain about honoring consent and its withdrawal.

The motivation for the "Legal" work of the UMA Work Group is: How to ensure enforcement given that the harm for policy violation is real? If George lets Eve download a photo where Eve agrees to adhere to some usage constraints, and Eve violates the agreements, what is George's recourse?

Detailed use case using a calendar API: Alice first sets up a relationship between her "myCals" service (RS) to her "authZ4me" service (AS). This is achieved through a normal OAuth flow, and an access token (which UMA calls a protection API access token or PAT) is issued. The RS registers Alice's calendar-related resources and scopes at the AS. Alice defines an authorization policy. Alice sends Bob an email with a URL in it — a plain URL in the clear, pointing to a resource that is protected. Bob uses a calendar client, called scheduleMe, to try and reach Alice's calendar link. When it fails, Bob needs to prove who he is to satisfy Alice's policy (and an UMA permission ticket begins to flow through these transactions). Ultimately, his client app gets an access token (which UMA calls a requesting party token or RPT) and he can access the resource.

For those who love detailed, almost-curl-command-level sequence diagrams, please see:

- http://tinyurl.com/uma2grantwsd (for the UMA 2.0 Grant spec)
- http://tinyurl.com/uma2fawsd (for the UMA 2.0 Federated Authorization spec)

The grant has the client-centric perspective and the federated authorization spec has the AS-RS perspective.

Yo GDPR: Terms We Assert and Sites & Services Agree To Check

Tuesday 3C
Convener: Doc Searls
Notes-taker(s): Scott Mace

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

Something doable for GDPR sunrise day (punative), May 25, 2018

We are willing to be the second party

Customer Commons is based on Creative Commons. We have a collection of terms that people can assert.

It's an information sharing agreement.

Not sure what makes it a standard information sharing agreement.

If the first party proffers the term, Linux Journal calls Do Not Byte (Joyce's terms). Just show me ads not based on tracking me.

Old fashioned ads sponsored a publication. You know Rolex wanted to be in the New York Times. Today could be from any of the parties in ad tech.

We are not participating in the ad tech system. We want to show publishers the way. And a new revenue model.

The whole industry is drunk on digital and can't think of any other way. Most quoted line, Madison Avenue fell asleep. Direct marketing ate its brain.

Brand advertising, you didn't want or need to get personal. Direct response marketing is in fact a junk mail business and is a cousin of spam. Same model, just the numbers are a little different.

We're saying let's go back to what we had before as a model.

The customer will simply point as someone will point to Creative Commons on Flickr. Ours the same. Terms will be in legalese, in ordinary language and so machines can understand it as well.

We talked about doing this in the browser, maybe even hijacking Do Not Track. We decided against that. We're using Jlinc. My understanding of it, it happens out of band in a browser but through a UI or a thing that we haven't built yet.

Jlinc: It's cryptographically signed by both parties.

Two databases, recorded in both in a way that is auditable later.

Q: Can I sign a universal agreement. I dont want to do this with every source.

Jlinc: The one you sign with your health provider might be different. But might be standard for a given industry.

Q: I don't want to log into anything.

Doc: That's not what's on the table here. We're trying to do one doable thing.

Q: What if offer terms you don't agree to?

Simplest, we ignore them. You might see no ads.

Q: Tiered access?

I want the shortest distance. We will probably do this anyway. What we want to do is bring to the publishing industry the realization that there are advantages to listening to what readers want. This model starts with the reader.

Q [Oath]: Are you going to do IAB's transparency consent? Fixed permissions with extensions.

I have strong feelings about IAB. They paid me twice good money to come speak to them to no effect. They assume interactive advertising is best. But is there any agency on the reader side to what they propose?

Q: It's a set of permissions granted by the publisher. Not a free form set of permissions defined by individual consumer.

Joyce: That's not this.

Doc: It doesn't have to be complicated.

Q: You'll get a dialogue, do you consent?

Doc: I hate that. Having that regime defeats one of the purposes of the Web in the first place, and is for the convenience for interactive advertising that I don't want to participate in. Ideally it would be a Do Not Track with teeth. I could sue you if you agreed to this term. In a deeper sense we're trying to scaffold up private spaces in the physical world. The advertising world has said you are fair game. We can follow you everywhere. That is just so fucking wrong I don't know what to do with it. It's like negotiating with pirates. We're trying to do something simple.

Q: Contact for verifiable claims WG. Not much exploration around targeted advertising happening yet. Also started improving Web advertising WG at W3C. We're beginning to have conversations. Existence of ad block is a failure in that people are turning off part of the Web.

Doc: The notion that interactive advertising is part of the Web is fucked. It took off when publishers and the IAB stomped on Do Not Track.

Robert Steele: I might be funding a legal summit this summer that tracking and cookies are a form of stalking that is a federal felony. It is also unfair taking of computer resources, time and energy. We're not putting up with it anymore.

Doc: I would love the W3C to be involved.

Q: P&G pulled $200 million of ads from digital advertising. It was all bad spend. Another major institution pulled $100 million two years ago. It's an opportunity.

Doc: Compliant in spirit if not in letter to the GDPR. I'll never buy Geico. But that is a brand in my head. Geico didn't need to know who I was. That is the idea behind brand advertising. A trillion dollars has been spent on ad tech. How many brands have been created? Not one.

Q Oath: What's the difference between what IAB has done and this? We are using IAB in Europe.

Q: As soon as IAB starts honoring Do Not Track, we will believe you.

Doc: If the IAB can hear where a publisher or advertiser can hear a first party saying anything as an equal in the marketplace, we'll talk. It's the recordkeeping.

Joyce: We don't know what the IAB thing is. It's a menu saying decide. This is, this is me saying. You can agree to my terms. LJ we don't have any ads at all. The point is this is an illustration. Get something in somebody's hands to play with. Readers will see the popup, if you're interested in registering as a first person and saying this to advertisers, you are saying I want to support LJ and I am happy to see

interesting ads as long as they don't track me. It's an experiment to do the first party contract and get sponsors. 50% of all LJ readers have ad protection.

Q Oath [Wendell Baker?]: Where's the bright line?

Doc: Our counsel on this, Customer Commons, a California 501c3, Harvard Law School, contract is the oldest law in the world, only applies where there are disputes. No one has to be selling anything. This is totally not normative on the Web. It's been done in the world. We want to try this out. We having something going on with IEEE.

Q Oath: Only so many things can be done reading media. Given that, it seems to me IAB took that and put it into the standard. Why isnt that working for you.

Joyce: We don't know what it is.

Q: There's nothing on the side of the individual. It's the ad tech industry trying to get the publishers in sync.

Q Oath: Includes don't set a cookie. Trying to figure out for v2, v1 was rushed to get past GDPR.

Q Jim Jlinc: Doc has boiled this down to a particular axis that's about display ads vs. custom ads. We're providing technology to do that particular use case. The deeper philosophical case has to do with the sense of agency and control and empowerment on behalf of individual people. It's whether the viewer is the product. That's the model of Silicon Valley. It's led to a lot of problems. The question is whether we're going to go to something with a different business model. Different than the IAB. Not being spied on or turned into product.

Q: They're not ad blockers. They're tracking blockers. Advertisers changed the name.

Doc: Adblock Plus gets paid by Google, others. If you're trying to just show ads not based on tracking, it's hard to do. Go into Privacy Badger, others. It's a hard thing to manage.

Joyce: People are really very clever and they figure out how to do this new thing. If it doesn't serve, people are very creative. Think about it in a different way. There are two parties trying to get what's best for them. I used to be in the fashion business, a buyer for a large department store. A vendor would give me a printout sheet. Everything all written up perfectly, circle. I go back to hotel. I just went click click click. In my own business, I gave customers a pad a paper. Then I got orders.

Q Jim Jlinc: There is a philosphical point here. About a sense of end user volitional control. It may be some people are going to be find with what the IAB delivers. But what's still missing is the sense the end user is a first party. Not treated like something to work the buttons.

Doc: Take off the professional hat and look at the Web as you did when you first saw a browser and I had lots of agency. May be some overlap. The thing that makes it hard is we've been tracked for so long I don't know if you are ever willing to let tracking go. We need help with Customer Commons: funding, an executive director.

Q: You have no clue what interests me without tracking me.

Joyce: We know what Linux Journal readers are interested in.

Cloud Native Secure Access

Tuesday 3F
Convener: Sarah A., Rachel M.
Notes-taker(s): Rachel M.

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

What can we do to make sure developers can deploy to the cloud confidently? What are the requirements for tools for auditing policy in hybrid-cloud systems? Open Policy Agent (OPA) is an open source policy language still in development. We should all get involved, start hacking with it, and make sure it meets our needs.

Sarah A: The world is more complicated. When I started, security was all about the network boundary

Alan: Is this about Enterprise or individual developers?

Sarah A: The individual's problem is not the hard problem, but all the hard problems happen in the Enterprise

Alan: I think managing Enterprise developers in the cloud has hidden something important. So the enterprise case is easier.

```
   Cloud Provider
 ^          ^
 Enterprise    Individual
 ^ (trusted relationship)
 Employee
```

This simplifies the Cloud Provider's job.

Paul: Thinking of proposing a ledger that contains personal information.
The table would be held by cloud providers, but I don't want it to be owned by anyone
What kind of relationship would I have to cloud providers?

Alan: ?

Sarah: How is this GDPR Compliant?

Paul: There is sensitive and non-sensitive data, and the sensitive data is stripped out
Most people would probably be okay with posting sensitive data if it can't be traced back to a human. I'm also finding that any text field is sensitive data.

Ray: What is the GDPR's definition of sensitive data?

Paul: There is a definition but it's not as strong or as clear as it could be

Alan: How does this relate to the policies?

Paul: This doesn't have an owner. Sensitive information is

Sarah A and Rachel: The thing that we're building is that everyone who puts things on the cloud should be confident and understand what they're building and who has access to it

Alan: There are two different cases, what the developer standing up a cloud service is allowed to do and what the users of those cloud services can do

Denis: Should we be worried about irresponsible developers

Micah: Do we need to think about multi-tenancies and isolation?

Shantau: We must have thought of what the needs of fin tech, etc, and built tools for what compliance, and then the tools thats

Micah: And building tools that guide the developer, for example, to get a certificate, be HIPPA compliant

Chris: Having a WYSIWYG editor for API, and then applying UMA2 on top of that

Alan: So you're envisioning a standard

Sarah: We're thinking of OPA, so there's a common way of expressing policy. We created a policy language, and someone said "a policy language won't make you secure?"

Alan: You can't be security without expressing policy.

Sarah A: What else do we need?

Mark: You need a risk assessment. SOX, HIPPA, and PCI all now include a risk assessment.

Davide: You could build components. Edugain lets you say they're compliant with a CoC, and that requires an audit.

Micah: That's something cloud providers could do, so it's not up to individual developers to know what they need to have when it's time to go through a security audit.

Sarah A: One company has 10ks of apps

Alan: All we need to be able to prove is that we enforce any policy that is expressed in the policy And then we're decoupled from all the services offered on Google Cloud

Paul: I'd like a way of knowing what fields are considered personal, sensitive information that should never go out

Alan: That could be something you use as the developer.

Denis: GDPR requires expressing HOW you enforce policy

Alan: You can look at what each Cloud provider says

Chris: You could write a testing tool. Are there encrypted at rest requirements in GDPR?

Everyone: Yes.

Alan: If I say this is personal information, and this is the policy around it,
then the auditors only have to audit the policy, and how Google enforces the policy

Micah: GDPR is a a good case, where the app developers will be able to do all the best practices by default

Paul: <

Alan: I think the hard part is to make the policy language that all the cloud providers agree on.

Sarah A: Are people bought in to the idea of a policy language?

Seidev: I've used Amazon policy, and it was a good concept. It could be extended to many providers.

Alan: And we have the flexibility that policy could be expressed in many ways

Sarah A: Some things are not documented and are hard to discover, when is it
effective? And that's not part of the policy language. So what else

Micah: Is it centered around access?

Sarah A: Borrows from Xacmul, which has the concept of deligation.

Micah: Janrain is building policy language in Xacmul. Customers hate it, so they go back to XML.
Alan: It was so expressive, and we built a few checkboxes that generated the XML that no one would ever see.
Sarah: Can we express the policy across multiple providers, and in cases where it's more complicated.

Alan: I looked into limiting what parts of the database by making queries for things you're not allowed to make

Denis: You can do an interference attack

Alan: Instead we gave them a view of the database that only had what they needed. (We found out later?)

Sarah S: Why are you trying to do this? Making a infographic of the database?

Sarah A: Say I have a front end, back end, lots of services in different infrastructure. How do we reason about it and
understand the high level review. There's the problem of knowing what is correct, and there's the problem of implementing
what you've decided.

Denis: You'll want in some case to want to start checking the token, and additionally the region

Alan: As long as you allow delegation.

Mobile Driver's License (mDL)

Tuesday 3I
Convener: David Kelts
Notes-taker(s): David Kelts

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

Presentation can be accessed here:
https://drive.google.com/file/d/0B_luqCyRPBXjaDQtZ2QzWnpJQW1VNHpMTHRuQ3N4LW9MXzNz/view?usp=sharing

What Are The 'Wallets' visions/projects - Do We Need a Working Group?

Tuesday 4A
Convener: Kaliya @identitywoman
Notes-taker(s): Kaliya @identitywoman

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

Wallets we Identified

BlockPass https://blockpass.org Sovrin DID? (someone said this in the session)

QiyFoundation (Dapper) https://www.qiyfoundation.org Sovrin DID (someone said this in the session)

Veres One (server side) DID http://www.veres.one

Pillar Crypto 1st https://pillarproject.io

uPort DID http://www.uport.me

connect.me (Evernym) Sovrin DID http://www.connect.me http://www.evernym.com

Trusted Key https://www.trustedkey.com

BlockCerts DID https://www.blockcerts.org

LifeID https://lifeid.io

Blockstack DID https://blockstack.org

SecureKey https://securekey.com

Civic https://www.civic.com

ShoCard https://shocard.com https://www.diro.io

DigiMe https://digi.me

MSFT? (DID Auth)

HIE of One http://hieofone.org

Jolocom https://jolocom.com

Beyond the session

DataWallet - https://datawallet.com/index.html

One Pager - https://datawallet.com/pdf/datawallet_one_pager.pdf

What are the capabilities of Crypto Wallets? ID Wallets?

They all have Backup and can Sign Messages

This diagram was drawn during the session to articulate the overlap and the differences. Originally it was just a currency and an Identity Wallet but then it was clear there was another category of Personal Data Stores, Agents and Personal Information Management Systems that related to Identity aspects but didn't become crypto wallet.

The question is - does their need to be a wallet working group to ensure interoperability.

101 Session / NIST Digital Identity Guidelines

Tuesday 4B
Convener: Sarah Squire
Notes-taker(s): Kevin Trilli

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

- Updated after 10 yrs - Official June 2107, designed with govt' agencies in mind; done on GitHub
- Orignal version conflated ID proofing and auth; motivation to change this and unbind
- Authentication
    - Context: NIST in Commerce, so built to ensure fair commerce
    - def. making sure a person or a thing is the same person or thing (which is different than being who they say they are)
        - ID Proof doesn't matter, just that you are returning act holder
- 4 Levels of Assurance of Identity, based on threat modeling against:
    - Random input
    - Snoopers
    - Bots
    - Financial attackers

    - Nation States
    - Hacktivists
- Old model - levels of assurance - LOA
    - 1 - Little or none
    - 2 - Some
    - 3 - High
    - 4 - Very High (strong crypto auth, man-in-middle resistance, no bearer tokens, **in-person proofing with govt' ID)**
- Digital ID Guidelines (1, 2 and 3)
    - Identity
    - Authenticator
    - Federation
- Identity Proofing (Volume A)
    - Level 1- Pseudonymous
    - Leve 2 - remote or in-person proofing
    - Level 3- In person, biometric collection (non-repudiation)
- Auth (Volume B)
    - Level 1- single factor (know, have, or are)
    - Leve 2 - 2FA
    - Level 3- 2FA w/crypto (private key) + verifier impersonation (Phisher) resistance (e.g, same TLS Channel, token binding)
- Federation (IDP and RP are different) (Volume C)
    - Level 1 - Signed bearer assertion
    - Level 2 - Signed, encrypted bearer assertion
    - Level 3 - Signed, encrypted, holder-of-key assertion (not commercially available as of today)
- Password and MFA Policy
    - KBA is banned (fed agencies can't use— Yea!!)
        - Bad security and bad usability
    - OTP over SMS is restricted
        - Telcos vulnerability, SMS can be sniffed, easy to engineer phone number porting/device replacement
        - Not the same as App notifications
    - Passwords
        - Do
            - Allow very long pw's
            - Accept spaces and special characters
            - Compare to breach corpus (e.g Ashley Madison passwords published). (E.g, haveIbeenpawned)
        - Do Not
            - Require special characters (reduces possible set entropy)
            - Force rotation (easier for fuzzy discovery
- Questions
    - No inclusion of device fingerprint (but a known best practice)
    - Password Recovery - big back door.

User Managed Access: The BLT Sandwich

Tuesday 4D 1I
Convener: Eve Maler
Notes-taker(s): Scott Fehrman

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

The UMA work has business, legal, and technical aspects. That's what the "BLT sandwich" (business, legal, technical use cases mapping) is about. In this session:

- We reviewed how UMA works in light of OAuth and OpenID Connect (for more, see the UMA Introduction session notes).
- We presented the new draft formal model of UMA-related legal parties, such as Data Subject Agent, and Authorization Server Operator, and the way they can delegate and license abilities and rights to other such parties — we plan for this to drive boilerplate legal text that would be available through CommonAccord.org.
- We discussed real-life scenarios such as when mother Alice manages who gets access to newborn Johnny's medical records and then he goes through different life stages.
- The goal is to improve liability apportionment and individual empowerment through auditability and possibly even tools like smart contracts.
- This slide deck was presented.

Quick overview ...

- OAuth is for constrained delegation to apps .. the OAuth "dance"
- OpenID Connect does modern-day federation
    - OAuth protected identity API, plus a bit more
- User Managed Access is for cross-party sharing
    - Next-gen delegation and consent to OAuth

Organizations have Resource Servers and want them to be sharable
Multiple resource servers can use a single authorization server

It's now about Alice to Bob sharing

Think about Google Docs:

- setup what you want to share
- control who actually has access
- revoke access

Use Case: Origo ... implemented UMA 1.0, UK pensions dashboard (for more information, see this white paper, website, article, and video)

- Discover all the pension accounts
- Alice to Alice sharing, initially, pension dashboard client

- One Authorization Server
- Multiple Resource Servers
- Alice can share with financial advisors … the Requesting Party
- Selects what to share with who

Recently published, draft report, UMA 2 Proposed licensing model (see also the new draft report)
… Legal role definitions
Giving access can come with some usage constraints

Starting with legal relationship model

Common Accord model

UMA capabilities … align well to a "next-gem" permission taxonomy (for more info, see this talk):

- Modes
  - Directed, Reactive, Long-Term
- Methods
  - Concrete, Abstract
- Controls
  - Scope, grantee, environment, usage (constraints can only be legally enforceable), downstream (constraints can only be legally enforceable unless resource owner and requesting party share an AS)

Attempt at a formal legal model … legal relationships:

- Persons

- Delegation and licensing
- Devices and artifacts

Scenario: Parent-child resource management

- Stage One: Mother and newborn child, offline
- Stage Two: Child old enough to use on-line services
- Stage Three: Child no longer needs legal guardian (age related to resources)

Need for more Identity Relationship Management capabilities

Digital death … who has control of on-line data after biological death

https://youtu.be/LjWPyy94NgA

DID Auth Scope, Formats, and Protocols

Tuesday 4F
Convener: Marcus Sabadello
Notes-taker(s): Karan Verma

Tags for the session - technology discussed/ideas considered:
DID Auth, OpenID, OAuth

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

- DID Auth - what it is
  - Definition:
    - A ceremony protocol where an identity owner proves to a relying party that they control a DID
    - Are the subject of a DID document.
    - Example cases:
      - Login to a website, apps, services
  - There is a challenge and response b/w identity owner & Relying Party
  - Change in terminology Moving from Identity Provider -> Identity Owner

- DID Document
  - JSON-LD based format
  - Proof not only by digital signature but also biometrics (BOPS protocol)
  - Three relevant blocks
    - Authentication
    - Public Key
    - Service
  - Question: Is there a list of authentication methods?

- DID Auth: Flows
  - Mutually authenticated channels
  - Signed HTTP requests
  - Signed emails
  - Login to website
  - Login to mobile app

What people call DID Auth?

- Client calling a traditional rest API
  - Sign the HTTP signatures
  - did:sov:....
  - Resolver <-> DID Poc
- Person sending email with SMTP signature
  - did:sov:...
  - Resolve, DID Auth

    - Per message basis
- DID-TLS
    - One service connecting to the other service
    - Instead of signing the payload or the http service you have mutual authentication
        - Use the TLS handshake to authenticate
        - Each will have a DID and they invoke a resolvers
        - Comment: this is better to avoid denial of service attacks
        - Comment: DID auth = proving control of the DID document. In the above cases there needs to be a priori agreement.
    - Not all chains are created equal, sovrin chain will sign the DID document to establish trust, other chains may act differently. For sovrin there are additional state proofs.
        - Resolver should give you enough information that can help you validate that the DID document is authentic.
        - Comment: people will end up doing is using a system and trust it without using state proofs.
- Universal Resolvers: uniresolver.io

- Proving DID auth when we don't rotate public key Vs when there is key rotation
    - Needs state information
    - Comment: that is in the ledger

- Using DID to login into a website(everyday tasks)
- Credential handler API
- The website needs to know your DID
    - Typing your DID in the website
    - Javascript API for the browser
    - QR codes
- Websites looks up the DID document using a resolver
    - Website sends a challenge

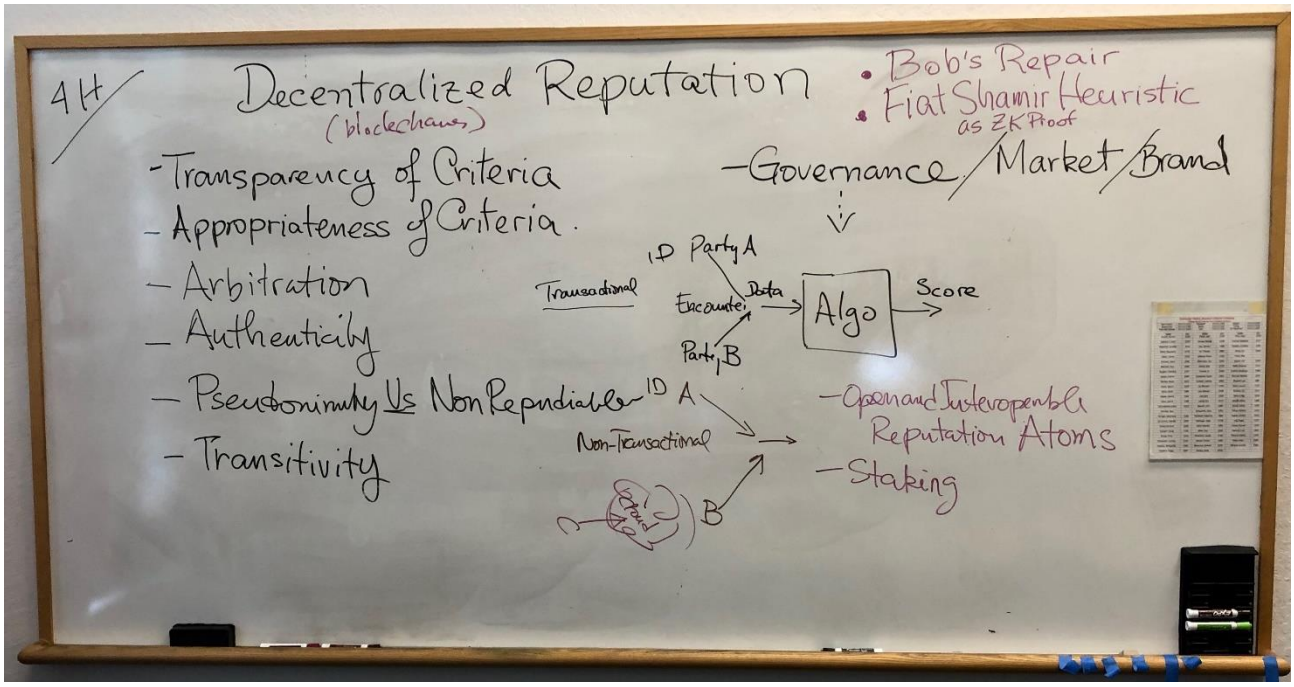
    - Agent Hub DID Auth asks to solve a challenge
    - User proves that "I am me"
        - Comment: The login button can ask more than just you "I am me" but also attributes/credentials about you.
        - Examples: Age, Driving License
    - What happens if the server is offline?
        - Answer: caching
    - Oauth and OpendID connect is applicable to DID workflow.
- Challenge can be delivered as
    - QR code
    - Javascript code
- Standardize: messages, protocol
- There are flows that overlap with Oauth and OpenID connect

Look at draft at weboftrust.info

Decentralizing Reputation (with Blockchains?)

Tuesday 4H
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:



The Future of Privacy While Accessing Published Content

Tuesday 4J
Convener: Judith Bush @judielaine
Notes-taker(s): Judith Bush

Tags for the session - technology discussed/ideas considered:
RA21, EZproxy

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

How can i access published content without surrendering all my relationships and my identity?

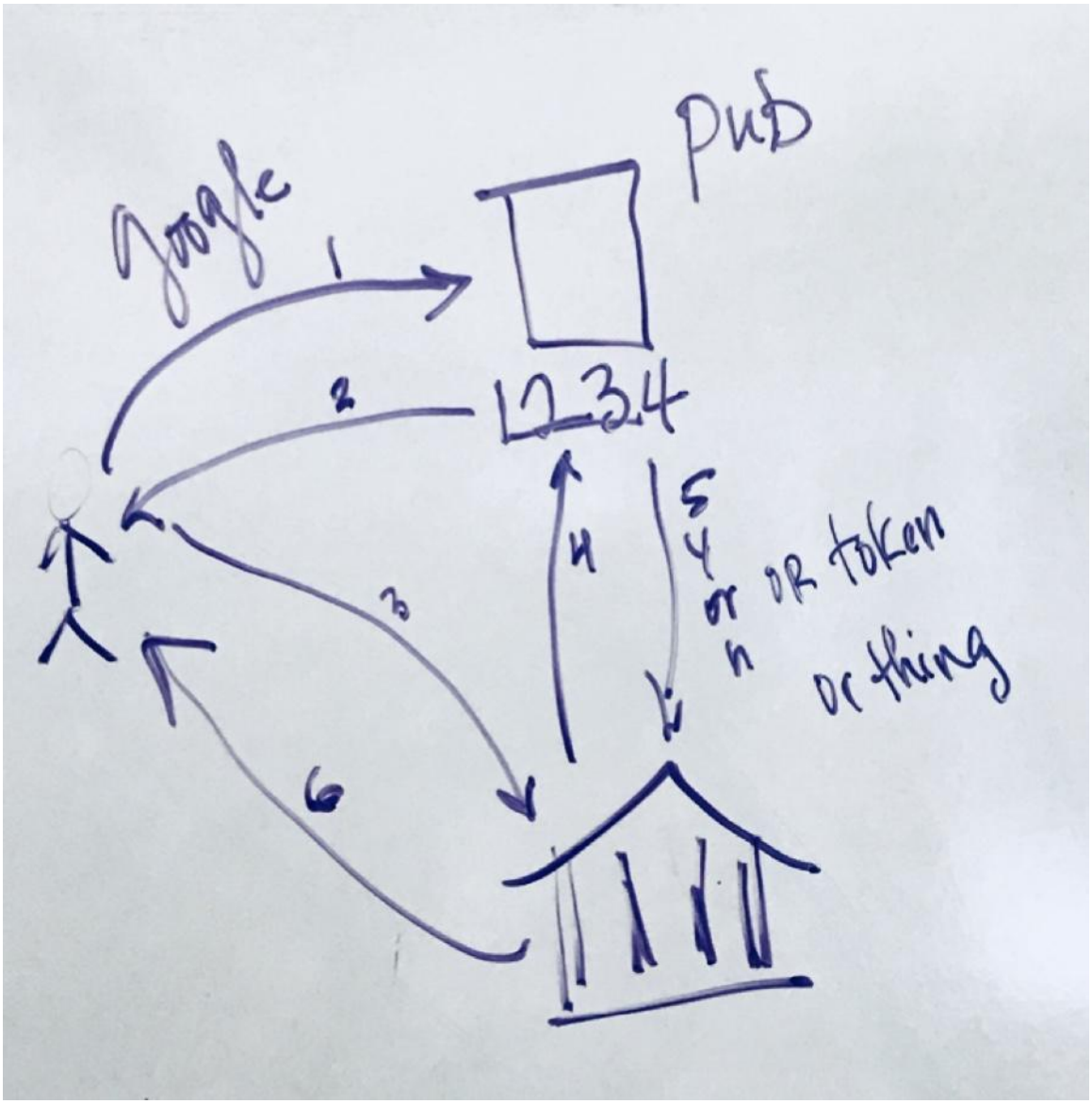
- Individuals want access with privacy (personally or due to intellectual property reasons)
- writers have an interest in demonstrating the reach of their work
- publishers have an interest in compensation for their content
- aggregators may act on behalf of publishers, collecting diverse publishers content in one platform.
- publishers & aggregators have an interest in usage statistics to improve their platform and content
- institutions have an interest in linking their members to licensed content
- institutions are interested in establishing whether subscriptions impact research and student outcomes

Scope setting
Published, licensed content mainly means journals and research papers — think humanities and sciences, health and hospitals, biotech research
Compensation has generally been per paper payments or institutional subscriptions: other compensation models that protect privacy (micropayments through an aggregator) are interesting to contrast with models that do not (targeted advertising)
Access includes authentication and authorization, establishing affiliation

Current state
Much of the access is currently mediated IP affiliation. Institutions assert the IP range they wish treated as their use. While there is some "on site" use, there is also considerable proxied use. Proxies usually interrupt TLS interactions, decrypting, rewriting, and then resending. Cookies may or may not be passed through. The proxies allow a great deal of usage statistics to be captured by the institution while obscuring individual users from the content provider.

Questions
RA21 is working with SAML because of the SAML deployments in higher ed. Is OpenID Connect a challenge for established SAML institutions?
What would user centric control of search stats across publishers look like, so that the research stats could be aggregated for educational outcomes studies for the user?
What can IDP systems do to help librarians confirm usage statistics at published resources?
How might affiliation be established with social identities once and used at publishers?
Given the friction points identified by RA21 — discovering if any of an individual's affiliations provide access — how might a sovereign identity with revokable or time bound affiliations be used in a way that by-passes the friction of the user testing affiliations until finding access and is privacy preserving (not handing over all "library cards")?

To help library patrons discover whether they have access through their library, processes beyond discovering the IDP in the publisher's list was discussed. Suggestions included introducing an authorization server used by the library as part of their licensing tool, and then if the AS returns a token if and only if there is access to the doi. Other channels between the patron and library, using a doi aware bookmark let were discussed.



FastFed – Making SSO Easier to Set Up. Intro and Status

Tuesday 5A
Convener: Darin McAdams
Notes-taker(s): Darin McAdams

Tags for the session - technology discussed/ideas considered: SSO

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

The FastFed problem statement was presented. The information is available here: https://bitbucket.org/openid/fastfed/src/4e4a20f183508fd34059de6b93b8bdf23e2e77f8/FastFedIntro.docx?at=master

The table of contents from the current draft specification was also shared. This is available here: http://openid.net/specs/fastfed-1_0.html

The discussion was about the intial feedback on the draft. In particular, the first draft attempted to define a FastFed experience for every common protocol including OIDC, SAML, and SCIM and the combinations of them. The result was essentially too big for anyone to fund and implement.

Therefore, the question discussed was "what not to do" if hard decisions were made on prioritization. In particular, should OIDC be prioritized ahead of SAML, even though most of the SaaS market uses SAML? In this approach, FastFed would become a nudge to move people toward OIDC.

There was little pushback on prioritizating OIDC ahead of SAML. Feedback from IdP and SP providers in the room: some customers are getting off it for security. XML bugs. Move to the future. Or, they want to use Google Logins. SAML is like mainframes - still used, but no one is rushing into it. RocketChat is an example of an app that implemented OIDC before SAML. People building new things are starting with OIDC.

Still provide an extensibility mechanism - not just for OIDC. Enable FastFed to be used for /SAML, of the next new protocol, if there is justification to do that work later.

In the academic space, 10's of thousands of IdPs. Most academic departments have moved to the cloud. The trend to hosted IdP is going way up.

If FastFed solves user deprovisioning, that's the key feature in academia. Pure university brings in 100,000 people every year. Don't want to get to 6 years from now and realize half-a-million people on a service license who are gone. Today, need an out-of-band process for that.

The typical deprovisioning flow is to block access to the app, not delete. Want to assign it to someone in compliance to determine what can/can't be deleted. One IdP vendor had APIs to support both modes (immediate delete vs block user and retain the data). Customers aren't choosing the hard-delete option.

Businesses want to preserve, or don't care until the bill reaches a limit. Business have regulations that make them want to preserve. Only recently have we seen customers start enforcing a higher degree of security and SSO.

In contrast, universities will tend to hard-delete accounts. With tens-of-thousands of students entering/leaving each year, impossible to examine each one. Seeing universities who put together an "update" spreadsheet. Graduating seniors and dropouts uploaded to APIs for deprovisioning. Don't do it day after finals. They have a flow and timeline.

Two concepts: preserving the data, and preserving the licensed seat. Are SP's differentiating these two? Not really. Most SP's have an export process. Workflow is to block user access, then export, then purge. Or, might assign that account to someone else. Some have an additional step of removing entitlements. Kill access, unlicense, but don't delete anything. Legal - retain documents for litigation and such.

Self-Sovereign Identity 101 Session

Tuesday 5B
Convener: Drummond Reed
Notes-taker: John Callahan

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

Drummond Reed (see slides here: https://drive.google.com/file/d/1uxIZkJpO02GJHkWWdS3R2heLAOALDiTg/view?usp=sharing)

3 Models of Identity:

(1) Sioled (Centralized) Identity

(2) IDP (Federated) Identity

(3) Self-Sovereign Identity

Four Emerging Open Standards for SSI

(1) DID (Decentralized Identifier)

(2) DKMS (Decentralized Key Management System) - KMIP compatible

(3) DID Auth

(4) Verifiable Credentials (a W3C Working Group)

What is Self-Sovereign Identity?

* DID = blockchain agnostic, prv/pub key pair

* Mobile Device = Identity Agent

* You will not have just ONE DID
* You will have 1000s of DIDs
* Each will give you a lifetime, encrypted channel with another person, org, thing (or can be highly emphemeral too)
* You will not just use this to prove your identity, but also credentials
* With no need to a centralized authority
* Every DID is registered on a blockchain or distributed process
* Self-sovereign Digital Identity = lifetime, PORTABLE, identity for any person, organization, or thing that does not depend on any centralized authority and can never be taken away

Decentralized Identifiers

* DID itself (for self-description)
* Set of public keys (for verification)
* Set of auth protocols (for authentication)
* Set of service endpoints

Decentralized Key Management System (DKMS)

* Offline recovery (paper wallet)
* Social recovery (trustee)

DID Auth

* Prove control of a DID

Verifiable Credentials (formerly known as Verifiable Claims)

* Issuer
* Holder
* Verifier

Building A Sovrin Linked Permissionless Ledger for Data Analytics

Tuesday 5C
Convener: Paul Knowles
Notes-taker(s): Paul Knowles

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

The presentation outlined the potential advantages of building a Sovrin-linked permissionless ledger to house "Ghost Schemas", GDPR-compliant versions of the original schemas. Any attributes constituting *Sensitive Personal Identifying Information* (SPII) would be omitted from the ghost versions at the time of schema creation using a *sensitiveAttributes* function. All non-sensitive data would be stored off-ledger in public read-only tables. The permissionless ecosystem could then be used to produce statistics and analytics on non-sensitive data.

The only real concern was how to prevent triangulation on non-sensitive attributes to unblind identification. Proposed solutions to prevent triangulation were (i.) to set an observation threshold so that tables were only published once they had grown to a certain pre-determined size, (ii.) to have a holding function so that tables were only published once the schema owners were content that they were suitably non-sensitive and safe for public consumption and (iii.) the community would be able to see if certain tables were being excessively used in conjunction to create analytics as this could signal that hackers were looking at certain data patterns and an investigation could then be triggered.

Having spoken to Timothy Ruff from Evernym, it was suggested that all of the functionality could, in fact, be built into the Sovrin framework without the need to create a separate linked ledger. That set the ball rolling in a different direction and we are now looking at how to go about that implementation.

On the last day of the workshop, Nathan George, Matthew Hailstone and Paul Knowles had a brainstorming session and decided that, rather than introducing "ghost schemas" into the mix, "overlaid schemas" would be a better solution. These acetate versions would enable sensitive attributes to be flagged throughout the schema lifecycle without having to strip them out.

A first draft of the new proposal can be downloaded via the following link …

https://we.tl/OvCRa0V9QV

Paul Knowles (data modelling expert) and Elizabeth Renieris (Global Policy Counsel, Evernym) will now meeting in London on the evening of April 12th to further discuss the initial drafting of guidelines for the *sensitiveAttributes* function. The ultimate aim is to come up with a succinct set of rules on what should be deemed "sensitive". This would primarily be for the schema creators.

The final tech implementation may have wide-reaching consequential benefits for every player in the communication chain. We believe that a model can be hashed out that not only ticks all SPII concerns but also allows people to get paid for use of their data.

The data analytics slant is the real game-changer. Imagine if all participants in a global subset of data can be paid when their data is used for statistics and analytics applications for societal, corporate and personal benefit. We'll continue moving forward with the proposal as it most certainly has legs.

Compatibility between JSON-LD and Indy Proof Request Exchange

Tuesday 5E
Convener: Dan Gisolfi
Notes-taker(s): Dan Gisolfi

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

The W3C Verifiable Credentials Specification ("VC-Spec") currently recommends the use of JSON-LD to define structured content for credentials. Unfortunately, several cryptographic techniques for selective disclosure using zero knowledge proofs require identity attributes to be described in a flat data model. Given the ratification path underway for the VC-Spec and the work going on in support of projects like Hyperledger Indy, we need a non-disruptive path forward while not reducing the desired benefits of solutions like Sovrin.

Given that we had the right people in the room face-to-face , namely Daniel Hardman (Evernym), Nathan George (Sovrin) and Manu Sporny (Digital Bazaar), we were able to recommend a way for the VC-Spec to suggest how to handle anonymous credentials and selective disclosure without expanding the mission of the VC-Spec which cannot include crypto topics. As a result, a pull request (PR) against the VC-Spec will be submitted.

Armor Up! The Gravity Wars: Real World vs VR and Human OS Identity Influences

Tuesday 5F
Convener: Jeff Orgel
Notes-taker(s): Jeff Orgel

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

Lens-Crafting: How Experience Has Crafted These Optics And This Perspective
With the observation of any new data-scape, things are noted, contemplated and packaged for use as wisdom going forward into deeper understanding of that space. One of the greatest gifts I can give or receive is when we can put handles on thoughts with words for each other. We can then understand each other better and talk about ideas where there hasn't yet been much language.
The space of IT forces and its impact on our Human Nature is what I call Real-IT®, our unique and individual relationship with "I.T." These Real-IT relationship choices can gently ripple onto, or devastate like a tidal wave, the beaches of our real world landscape. Your Real-IT will reflect into your Reality. Can we manage ourselves? Will we manage ourselves?

Game Space – Messing With Human Firmware Via IT Systems:

Design Altruism and Dark Patterns in the digital landscape may manifest as transparency, or lack thereof, regarding system design and intention. Better and lesser angels appear as our base animal nature acts out on a virtual landscape - of connected networks - of different sorts...

Online disinhibition effect, our feeling of being more than less in physically isolated privacy when online, challenges a pivotal Real-IT premise – to treat the digital landscape as though it is the Real World. It is the same thing that influences a ticked off 92 pound Grandma in her sensible import to flip a middle finger at the huge 80,000 lb. truck and driver. I don't see her shoving him standing side by side…but maybe! **Real-IT® Premises: Centers Of Gravity**

IT Delivers A Convenience Which Comes At A Cost (though not necessarily dollars and cents):

- STORY [b&w]: The art of determining IT cost is a key to making Real-IT choices which facilitate your intention.
- NOTE: A pain point, if any, is often cloaked in IT Convenience Benefit Ether (ITCBE). The higher the perceived benefit, the more the consideration/impact of cost is overlooked in the rush for the benefit.

Base Human Nature Is The Game Space Of Influence Of IT Forces:

- All systems run on top of the HumanOS (evolutionary firmware)
- IT Forces can be best managed when we know the Pressure/Pleasure/Pain Points of Human Nature that these forces play to. We can then regulate impact of forces.
- Look to base nature in the animal kingdom for guidance and vetting of sensibilities.
- Management of choices by the Human Brain is the Killer App

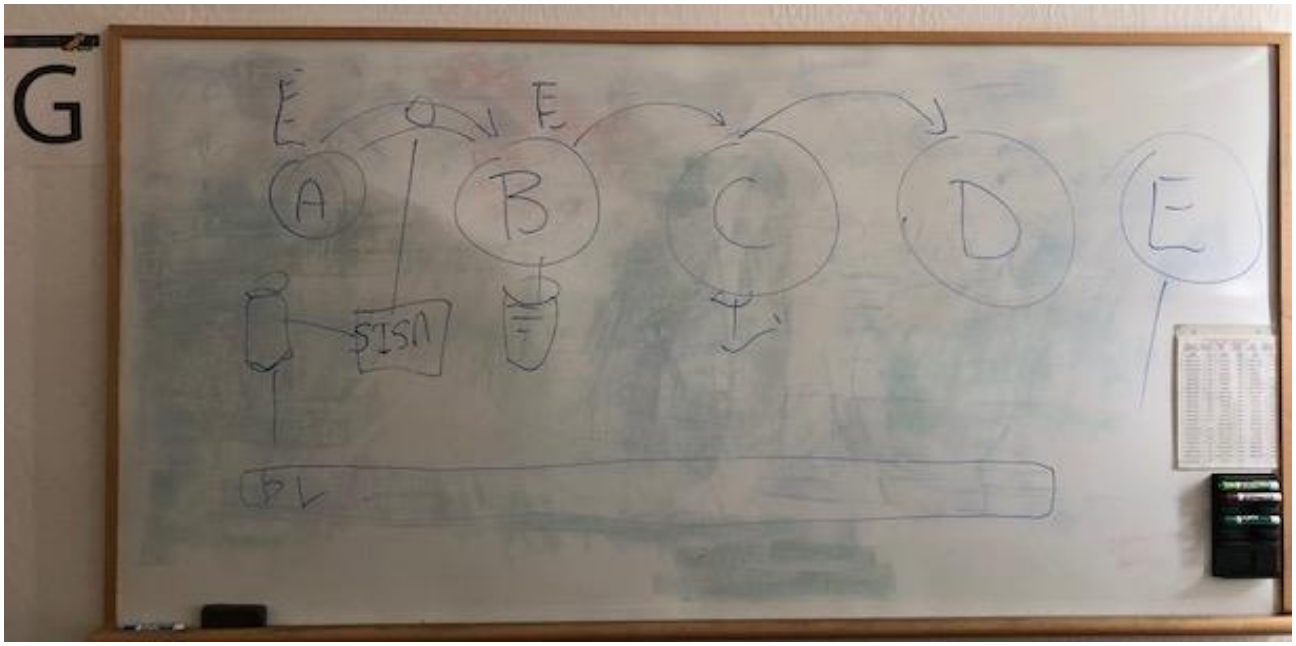
Gravity Wars

- VR (and somewhat less significantly, MR & AR) will make extraordinary connection to our base nature via neurology and will have a significant gravity pulling the HumanOS, as never before, away from Real World.
- IMHO, more people than we expect may be very inclined to delegate away much of their Real World presence to immerse in VR spaces.
- Focus on the state management skills combined with awareness of IT forces stay in balance (aka Digital Aikido)
- [STORY] Somewhat sociologically terrifying maybe, but we do not need to be intimidated.
- There is a space of optimal balance unique to each of us to be struck which will enhance and enable us.

Standard Information Sharing Agreements (SISAs)

Tuesday 5G
Convener: Jim Fenton
Notes-taker(s): Jim Fenton

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



OAuth + SPA (Single Page Apps) Can We Just Use Code Flow Everywhere

Tuesday 5H
Convener: David Waite
Notes-taker: David Waite

Tags for the session - technology discussed/ideas considered:
OAuth, SPA, Implicit, Code

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

My motivation for hosting this session was that I have started to recommend customers avoid the implicit flow and use code flow for Single Page Apps (SPAs). I wanted to get feedback from the community at large, and get head nods (or objects thrown).

I started out by covering the reasons suspected for implicit flow:
- Avoiding an extra API call
- CORS (for allowing cross-domain API calls) not widely available in 2012 when OAuth was standardized
- Avoiding code leakage in URL for redirects, which can cause codes to be captured in browser history, potentially in referrer headers, and in server logs
- Fragment identifiers in URLs are modifiable by javascript without refreshing the page, allowing the code to be stripped after processing without redirecting
- Lack of faith in browser javascript to protect tokens
- Simplicity for clients, no refresh token
- Became the de facto "public client" flow

John Bradley commented that the primary motivator was client simplicity for connecting to large providers - a client redirect results in a token being sent back directly.

The consequences of implicit have been:
- lack of refresh tokens can lead to needing a different behavior for refreshing a session than for establishing a session (hidden iframe vs browser redirect), requiring duplication of oauth code
- Difficulty in refreshing token can cause an Authorization Server to implement different access token policy lifetimes for implicit clients, creating an entirely new policy requiring security considerations
- Browser behavior carries fragments on redirects, a relatively unknown behavior which causes token leakage if not handled
- With OpenID Connect, signed JWTs must be cryptographically verified to be secure in the implicit flow. While verifying the tokens over code is more secure, there is a baseline level of security just from receiving the token over the TLS channel for the code flow.
- Single page application may be wrapped via a framework like PhoneGap/Cordova into a native application. We have recommendations (BCP22) for native apps which recommend using code flow. This means that a common codebase may require implementing both flows for meeting all their deployment needs.

The room was pretty much unanimously in favor of recommending against use of implicit, with some concerns about technology issues and spec changes. The big changes since OAuth2 was published in 2012 were:

- BCP 22, native apps, pointing out to implementors that code flow does not require a client secret, and actively pushing for support of code flow without secrets
- Widespread CORS (cross origin resource sharing) support in browsers, allowing the code endpoint to be hit without significant implementation changes by an AS
- Content-Security-Policy and other mechanisms for isolating running javascript and limiting sources of javascript, allowing much greater protections from running arbitrary scripts
- PKCE, which allows a server to verify that a token request was made by the same client instance as an authorization request, limiting the ability to use a leaked code
- For clients which want to use fragments, OpenID connect added a response_mode=fragment which allows code to be sent via a fragment rather than a query parameter

John Bradley remarked on the last point that one justification for the multiple response specification was to allow an id_token to be returned immediately on the front channel, before the code was retrieved. This allows a client to immediately attempt to extract some information from the id_token to reduce perceived latency in the authentication/authorization process.

The speaker offered to help John in efforts to push for a best current practice (BCP) document which informed single page applications to use code flow vs implicit flow.

Digital ID for Stateless Refugees

Tuesday 5I
Convener: Jeff Aresty, Larry Bridgesmith, Jonathan Holt, Kristin Yasuda
Notes-taker(s): Kristin Yasuda

Tags for the session - technology discussed/ideas considered:

#identification # legal identity #global south

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

Part I: Refugee Music Video Screening & introduction of PeaceTones/IBO

- IBO screened a music video "Is the Lady listening?" that PeaceTones project recorded in Cox's Bazar refugee camp in Bangladesh with Rohingya refugees. (https://peacetones.org/call-to-action/
- By providing identification to the musicians, the aim is to create jobs and foster economic inclusion (The Invisibles)

Part II: DEMO of IPID (Interplanetary identifiers)

- Implementation of DID method on top of IPFS (interplanetary File System)
    - Suitable for the usage in refugee camps, because the method works offline
        - Tied to the hardware and assumes the possession of a phone

        - P2P method and does not require server nor stewards
        - Issue that needs to be solved is key recovery
            - Usage of biometrics (vain + DNA) is one possibility
- Another DEMO of DID method from Pelle (uPort)
    - QR Code(key) generation that can be scanned using a mobile app
- Question: what is the business case you are trying to solve?
    - Portable identification for the people who are not connected to the Web and move constantly

Open question to the participants: "What possible obstacles remain?"

- Refugees lack formal credentials that can be put into the wallet that has just been demonstrated
    - Last thing refugees want to do is to give out their real name
    - SSI does not necessarily solve refugee's problems
- Need to make clear refugees at which point of the journey are we addressing: those who just crossed the border, or those already in the camp?
    - Identification and a method to match supply and demand in the camps are different things. People are not looking at the UN IDs not as identities, but as means to get food
- Do these solutions require State actors/top-down approach?
    - Low trust towards State institutions in parts of the developing world

Feedback from the participants:

1. Solutions need to be context specific
    - We should also consider providing identification for marginalized populations in the developed world such as homeless people, in addition to refugees and global south communities
2. Political questions remain but we can and have to start acting

Wednesday April 4

What is Sovrin? How to Become a Sovrin Steward. Self Sovereign Identity 102

Wednesday 1A
Convener: Phil Windley, Drummond Reed, Joe Andrieu, Ridley Hughes
Notes-taker(s): Drummond Reed

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

In this session, Drummond first repeated portions of the Self-Sovereign Identity (SSI) 101 session from Monday (see the notes from Monday 5B).

Then Phil Windley followed by explaining key concepts about how the Sovrin Foundation is implementing SSI in the Sovrin network. He covered the following terms (all of which are defined in the Sovrin Glossary):

- **Trustee**—one of the individuals who serve on the Sovrin Foundation Board of Trustees
- **Steward**—one of the trusted institutions who run nodes of the Sovrin public permissioned ledger (see the public list here)
- **Identity Owner**—the term used instead of "user" for all participants in the Sovrin network
- **Agent**—the software module that works in conjunction with a wallet to form connections and exchange digital credentials peer-to-peer on the Sovrin network. Agents are either edge agents, operating on an identity owner's own local devices, or cloud agents, hosted by a third-party provider called an **agency**.
- **Wallet**—the secure module (typically in some combination of hardware and software) where an identity owner stores the owner's private keys and other secrets
- **Trust framework**—a document, typically implemented as a shared community contract, specifying the business, legal, and technical (BLT) policies by which a community agrees to achieve trust online.

Phil explained how the Sovrin Trust Framework operates as the constitution for the Sovrin network, and how as of that day, 28 stewards had been approved by the Sovrin Foundation and 15 were live on the Sovrin ledger.

Phil closed by explaining that any organization interested in becoming a Sovrin steward can start out by contacting the Foundation via the contact page at https://sovrin.org/contact/.

Links:

1. IIW Introduction to Self-Sovereign Identity
2. The Sovrin Glossary
3. The Sovrin Trust Framework

DIDAuth + WebAuthn

Wednesday 1C
Convener: Dmitri Zagidulin
Notes-taker(s): Dmitri Zagidulin

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

Slides can be accessed here:
https://drive.google.com/drive/folders/1LyYp_SZpqboIPfUa1lo9zKtNv9SIv-5I?usp=sharing

Agent/Wallet? What is Agent? What is Wallet? Are They The Same?

Wednesday 1E
Convener: Antti 'Jogi' Poikola
Notes-taker(s): Bill Wendell and Antti 'Jogi' Poikola

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

17 wallet projects were listed on the wallets-session Day 1. One confusion point from the Day 1 session was how to define "identity wallet" and what is it's relation to "agent"? Here at IIW we're talking about them wallets and agents interchangeably, causing confusion. This session was set to target that question.

PART #1: WALLET

Wallet (where you store your private "stuff")

- key ring

- Will people have a central wallet or many wallets?

What "stuff" would you put in your wallet?

- the key's control your data, transactions and relationships

- some often used & small data (credentials / identity attributes) --> most data in other places (like PDS for example) in the wallet just the keys to manage the data stored elsewhere.

Metaphor to physical wallet

- Credit card is a key to manage money that is not in the wallet

- Some small and often used credentials like the driver's lisence is in the wallet

PART #2: AGENT

[wiki article]

Agent (your communication end point to the world):

- end point that is responsible for communicating with other agents

- consent agent running on my personal domain and managing my informations sharing permissions

- software agent within which you manage relationships (DIDs) and sharing of identity attributes (data) --> See the three dimensions of identity session from Day 1.

Software agent vs. human agents

- non technical people think agents like real estate agents, layers and other exoperts that represent the individual in some relationships

- "I'm my own agent, but I can imagine having an (expert) agent to act on my behalf"

- can a software agent represent the individual legally in the same sense that human expert egents are representing legally their client? --> maybe up to some point and in the future even more --> "personal AI".

- trusted agent: it is assumed that agent will always act in your best interest

Informacion fiduciary

- Default for Information fiduciaries = always act in my best interest

- See Atlantic Magazine article on Information Fiduciaries http://bit.ly/GrandTrust

Agents representing non-human entities:

- Does the Smart Home have an agent independent of it's owner?

- Keller Williams, we are no longer a real estate agency, we're a data company --> part of the multi-trillion dollar race to control the smart home of the future

- Can you delegate the operation of your smart home to an agent?

- Future: Every AI is going to have "beneficial ownership"

Connection of agent and the hardware where it runs?

- The agent is the software (using cryptography behind it) which is on the device

- Can you have a cloud-based agent? --> Yes: It can run also on clud

- Agent = the device you are using? --> No: on the same device there can be multiple agents

- How tightly is the device and an agent tied togeather? Is it possible to move a agent from one device to an other or will it be functionally just bootstrapping a new agent?

PART #3: BOTH

Is the wallet inside, combined or separate with the agent software?

- From end user perspective, it is hard to separate, agent and wallet togeather provide the functionality to manage identity and data transactions. --> what would become the "marketing" term for wide audience (like "browser" bacame the house hold term of accessing internet)?

- Are the PIMS like Digi.me agents or Wallets or both?

- Whenever you are building a wallet, you are building an agent & a wallet

Interoperability

- If all wallet start-ups are try to build their own ecosystem, only work with some ledger, only accept their digital currency --> they will all fail.

- At what layer do the standards exist?

- is there wallet interoperability --> DID standard?

- agent standard coming out: DIF Identity Hubs / Sovrin agent?

Zero Knowledge Proof 101

Wednesday 1G
Convener: Kazue Sako
Notes-taker(s): Chris Blanton

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

Notes also online at: https://github.com/afroDC/Personal/wiki/Kazui-Sako-Zero-Knowledge-Proof-101-Notes-from-IIW-26

Simple one way function:

x -> f(x)

Easy to go one way to f but mathematically hard to go from f(x) to x.

The most common example is a hash function.

Known(public): g, p:prime

g is a constant p has to be prime

f(x) = g ^ x mod p

Easy to know x and compute g ^ x mod p but difficult to do in reverse.
==========
Use case of a hash function:

register password(x)

It is not smart to store password(x) in plaintext, so we register password as f(x)

From there it is easy to compute that x = f(x).
==========
Zero knowledge proof (ZKP)

Alice wants to prove Bob that she knows x without giving any information about x. Bob already knows f(x).

So again:

Known(public): g, p:prime g is a constant p has to be prime

random number 'r'.

Commit:

Alice sends Bob u = g^r mod p

Bob receives u

Challenge:

Bob returns a challenge(e). Either 0 or 1

e = 0 || 1

Response:

If Alice receives 0, Alice returns v = r

Else if Alice receives 1 Alice returns v = r + x

e = 0 -> v = r

e = 1 -> v = r + x
Check that Alice knows x:

if Bob sent e = 0 before:

if u = g^v mod p:

pass

else fail
if Bob sent e = 1 before:

and if u*f(x) = g^v mod p

pass

else fail

==========
Bad actor can cheat with:

u = g ^ r mod p / f(x)

To get around this, multiple rounds of this(t), where 'r' is different for every t.

g = number

p = prime

t = number of rounds/iterations

for t:

  r = random number

  Send Bob 'u = g^r mod p'
  Bob receives u
  Bob returns 0 or 1 as 'e'

  If Alice receives e==0:
    v = r
    return v to Bob
    g^v mod p = u

  If Alice receives e==1:
    v = r + x
    return v
    g^v mod p = u*f(x)
==========
(Correct) Alice is always accepted (pass)

Chris(bad actor) with high probability, will be rejected.

By performing this protocol, information on x is not revealed.
==========
If Alice performs correctly she will send.

v = r when e = 0

v = r + x when e = 1

Otherwise, the bad actor (Chris) will most likely send "garbage" as they won't know r.
==========
More secure method of ZKP:

if e < 2^160

Alice:

v = r + x * e

Bob:

g^v mod p = u*f(x)^e
==========
If you want this to be non interactive:

e = H(u) where H is hash

in this case:

g^v mod p = u*f(x)^H(u)

Both Alice and Bob run H(u) individually and do not pass it.
==========
Paper recommendation given by Alan Karp:

Comparing information without leaking it
==========

Native SSO for Mobile Apps

Wednesday 1H
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 is a link to the presentation I went over in my session.
https://www.slideshare.net/gffletch/native-sso-for-mobile-apps

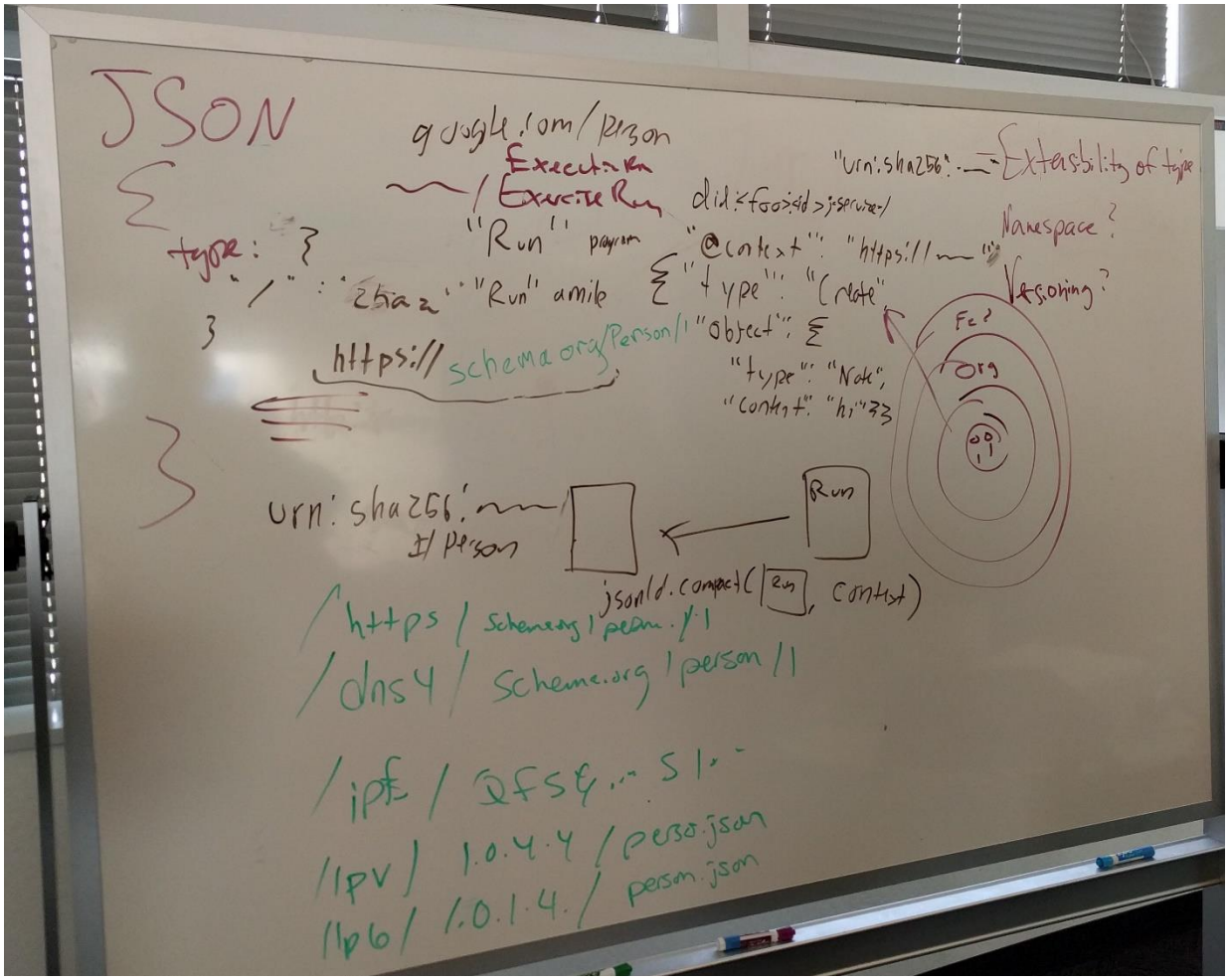
Additional notes:
1. Consider using refresh token instead of id_token (or sending both)
2. Change the name of device_id to device secret

Agent Communication #2: Message Types and Name Spaces

Wednesday 1I
Convener: Sam Cullen
Notes-taker(s): Sam Cullen

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

We talked about extensible message types, and the good and bad of json-ld and other existing formats.



DKMS Prototype Demo

Wednesday 2A
Convener: Drummond Reed
Notes-taker(s): Drummond Reed

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

In this session, Drummond Reed and Devin Fisher of Evernym presented the same demonstration of the prototype code for DKMS (Decentralized Key Management System) that they gave the previous week for Anil John, Program Manager for Identity and Data Privacy at the U.S. Department of Homeland Security Science & Technology Directorate. This represents the culmination of a one-year contract with DHS to research the requirements and develop a design and architecture for a key management system for broad market acceptance of DIDs (Decentralized Identifiers).

The slides for the demo at available at:

https://docs.google.com/presentation/d/1nuPVtmG1NVoEdTK6WPlYAeIVog3QsaEh_FaY1edyH84/edit?usp=sharing

The DKMS Design and Architecture V3 document is publicly available on the Hyperledger Indy github repo at:

https://github.com/hyperledger/indy-sdk/blob/master/doc/dkms/DKMS%20Design%20and%20Architecture%20V3.md

The Q & A during the demonstration covered many questions that are answered in the design and architecture document above. There was strong interest in follow up work, particularly on usability of the offline key recovery and social key recovery options.

DID Ledger Lightening Talks

Wednesday 2D
Convener: Manu Sporny
Notes-taker(s): Manu Sporny & Anastasia Miron

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

Slides: Veres One:
https://drive.google.com/open?id=1TpAGXvSZH-JRMQLw7KyGmWO4TuBFl_CVk3msMKzXFs

Veres One[edit]
- A Globally Interoperable Blockchain for Identity
- IIW XXVI - April 3rd-5th 2018

Vision[edit]
A world where people and organizations create, own, and control their identifiers and their identity data
Fit for Purpose[edit]
- Veres One is a fit-for-purpose blockchain optimized for identity.
- It is public and permissionless

Veres One is FAST[edit]
- Fastest DID Ledger
- DID Creation
- Bitcoin - create: 0.6M / day - consensus delay: ~3,600 seconds
- Ethereum - create: 2.1M / day - consensus delay: ~375 seconds
- Veres One- create: 18M / day - consensus delay: ~30 seconds

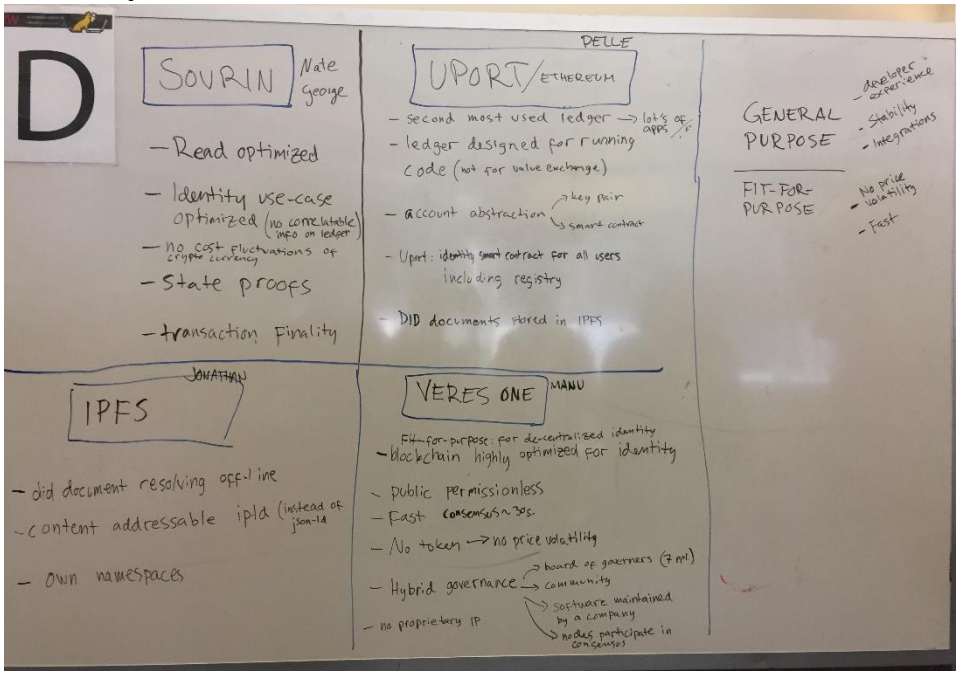
Did NOT do an ICO[edit]
- Veres One does not use a token and will not do an Initial Coin Offering (ICO).
- ICOs Create Volatility and Network Debt

Veres One is Cost Effective[edit]
- Bitcoin - ~$15-$73 per DID
- Ethereum - ~$4-$14 per DID
- Veres One - ~$1-$2 per DID
- Fee-based revenue models ensure long term operation of the network
- Commodity prices guaranteed due to strong downward pressure on operational costs

Roadmap[edit]
Beta (Oct 2017) Release Candidate (Feb 2018-today) Production (June 2018) Production Customers (Oct 2018)
Questions[edit]
- Any questions related to Veres One or the larger ecosystem?
- Manu Sporny | CEO | Digital Bazaar
- Co-Inventor of Verifiable Credential & Decentralized Identifier Technology
- Co-Inventor of JSON-LD
- Co-Founder of Veres One

- 10+ Years in Web Standards
- Customers in Finance, Government, Education, and Healthcare
- Email: msporny@digitalbazaar.com
- Twitter: @manusporny
- https://www.linkedin.com/in/manusporny/

Photo's by Anistasia Miron



Also the second day, all 4presenters from 4different DIDs sat down and discuss what works how and all the other details. It was amazing to see it!!

What do you HATE about OAuth?

Wednesday 2F
Convener: Jusstin R.
Notes-taker(s): Scott Fehrman

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

implicit grant
- originally optimization for SPA / javascript apps
- more of a cross domain session cookie
- tokens over insecure channel
- response injection

grant choice
- how to pick the correct grant type / flow

resource owner grant
- security concerns
- native apps that were not capable to open browser to access auth server

redelegation
- down scoping

separation of designation and authorization of resource
- can send wrong token to wrong
- confused deputy situation

fuzzy audience restriction
- does not define an audience restriction
- bearer tokens can go anywhere

no resource inhibitors

devices and native apps

nonce and state
- state was intended for use by a systems that supported states, a state handle
- code challenge
- bad names

signed response
- Facebook added this
- avoid OAuth 1.0 problem on complex crypto

only TLS
no universal grant audit
- common format across flows
- grant management API (AS)

optionality of scopes
scopes are strings

- difficult to parse, unstructured, space encoded

auth end point as GET
revocation doesn't chain

expires_in ...

- useless in the real world
- people use the refresh token

put too much on front channel
redirect URI matching
multiple Authorization Servers

- A discovery problem
- random AS attacks
- Bound discovery

no client notification

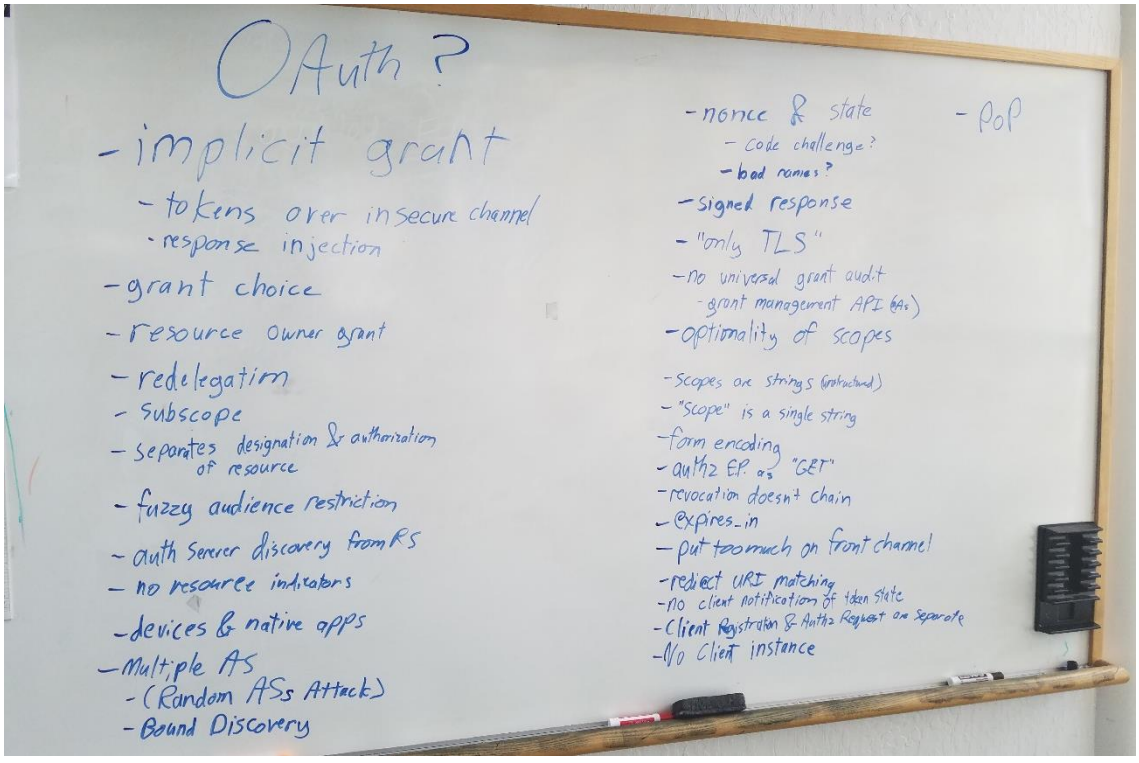
- token state changed

dynamic client registration and authorization requests are separate
client instance memory

- redirect token fails, refresh expires

Proof of possession

- not used



Publishing & Advertising After 25 May – GDPR Day

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

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

Wendell: IAB has put together a standard so that advertising can work. Another group of publishers represents the supply side of publishers. Jason Kint is one of their louder members, DCN, Digital Content Next, has been very negative about this whole proposal. It falls out on the lines of it will never fly.

Doc: Tell us what supply and demand are.

Wendell: We have this joke around the office. The activists were entirely right. The eyeballs are the product. This has been true ever since newspapers were made. As a publisher you're creating something you can sell to an advertiser. Ameliorate with subscriptions. You can have a demand side platform. But advertisers want coveted demographics.

Doc: Advertising, if you're P&G, you wanted to get everyone who reads the New Yorker, but it carried what was called an economic signal. Different discipline called direct marketing (junk mail) wanted to be personal. It wanted to be interactive in the sense the IAB wanted to be interactive. Digital world came along. DM wanted to target people personally. Banner ads died. I don't want a publisher. I want to target eyeballs. Now it's all direct marketing. The GDPR comes along. In spirit we want to protect the privacy of these people. It's still important to have in our minds that there is this distinction between tradiitional brand-time advertising and direct marketing, which is now called advertising. People like me are saying it was wrong on its face to follow people even if you could get good results. The other part of me says maybe there is still room for sponsorship. The reason we have fake news and why it's easy for Russian bot makers to make money is that this system rewards content. It doesn't reward journalism. It rewards the maximum production of content. Newark Star-Ledger was advertising not for reporters but for content producers. Mentioned in the New York Times. The rise of ad blocking completely parallels the rise in tracking. It's all correlation. You can't prove they are related but the correlation is so high. It's retargeting. What I'm hoping to see, is there anything you're doing that's useful to what we're doing on our side, Customer Commons, 1.7 billion people blocking ads. That is a massive signal in the marketplace about a dysfunction. LJ has the luxury of being a publication that can figure this out.

Wendell: I read Project VRM. They've had this idea to signal consent. The question with those ideas was how to implement them and how to go get everyone to use them. The government of Europe has ordered this thing to happen. The trade groups have assembled a solution, some reference implementation, we at Oath adopted that.

Q: GDPR is about the European view of privacy. Advertising is only one pain point.

Iain Henderson: It's the EU's response to Silicon Valley. Competing for the sustainable future. EU isn't going to win in a world where data is free.

Wendell: EU privacy commissioner at IAPP conference, the purpose of this law is to put these companies out of business. Quoted in quite a number of places. We are a large publisher. Guaranteed selling and audience buying was new and exotic. We were going to serve both sides. Obviously that didnt work out. Now our business focuses on our publishing shop. For the past year I've been working on making DM GDPR conformant. We have worked with other companies that exited Europe. Back to Doc's ideas, I and others saw this as an aligned concept with Doc's VRM ideas where the consumer could say what they want to have happen with their traffic. There was a proposal through the W3C to extend the DNT work to take this into account. They had a much longer runway but the W3C process is very consensus driven. Industry, browser vendors. Still an opportunity but it didnt happen. So they went with technology we control as publishers. Store consumer responses in a database, cookies, server side in the cloud. I see this is an incarnation of all the VRM ideas. Sense of purpose may not be sliced correctly or expansive enough in scope. Quantcast developed enough functionality without consumer consent fatigue. These consent solutions will have to name all these companies. Part of the art here is how do you solicit consent as a publisher before they consume media, while being compliant. Doc's magazine outsourced subscription management. Under GDPR, that has to be disclosed.

Arthur Coleman, Acxiom: You'll see a rush of people to reduce the number of pixels, and the number of people you have to flow consent through, so it's terrifying the industry.

Iain: What you see now is a very much cut down version of the regulation through lobbying. Privacy regulators meet twice a year. In Jerusalem October 2011 the idea came up to update the regulation. In that first discussion, the idea of the individual as their own data regulator was absolutely there. Worldwide audience, not just European regulators. The next meeting was in Paris March 2012. That concept was gone. My theory, that was lobbied out between October 2011 and March 2012.

Arthur: So what exactly is Oath's response?

Wendell: I can announce we will be doing two things. We will be reconsenting all users (Yahoo, AOL) into the Oath brand. That is independent of GDPR. Consumer consent goes with the brand. That will happen. It turns out for reasons of calendar, they will be close to GDPR. We will do the consent event for that and we're going to do something for the rest of the world like GDPR lite. Too hard to figure out where people live. Worldwide you will have access to your data. It will be all your data. Systems go and grab it out of everywhere, a nice summary dashboard. If it's all your mail, you know where to get that. If it's your cookie settings and screen width in Yahoo Finance, that's no fun but you will get that.

Arthur: GDPR asks to show where you are sharing your data.

Wendell: You will get a representation of where it's been shared to. [Following proof of ID]. There's a need for a DSAR portal, standalone, for small publishers. We run big ad tech. Imagine you run a little WordPress site. You want to log in. Now you have GDPR obligations. There ought to be a WordPress scale standalone open source implementation for GDPR compliance for small publishers in the same way Quantcast built this consent management scheme and contributed it to the IAB and the world.

Doc: If somebody goes to the Daily Beast or Buzzfeed on May 26, what are they going to see that's new?

Wendell: I would expect every publisher on the planet that serves European readers will have a roadblock that says do you consent. The purposes in the ads industry are fairly small. Analytics. Reuse of data for targeting. Reuse of data on another site. Precise geolocation. They will ask for that.

Arthur: When a European is here in the United States, we have to identify them and they are under GDPR.

Wendell: The company publishing may also be registered as a European entity. If you intend never to have anything to do with Europe again, you can blow this off. But that's teensy. Professors who have data about conferences, papers, they are now subject to these requirements. Need to support Access, Erasure, Objection, Restriction, Rectification.

Q: Destroy logs? Now you ask for consent. If pooled together and not personally indentifiable, that's okay.

Wendell: You can ask people to reconsent. Or deidentify the data you're no longer allowed to keep. There is no grandfathering. They can come in with auditors. If they find user data you didn't report, you're illegal.

Iain: We're expecting to get rid of 75% of the customer records.

Arthur: Individuals have to opt out for each purpose, for each vendor. Consumer will never get to any of it. It's really got to be simple. How do you know your audit trail is good?

Wendell: We built a chain of custody system. It's not a blockchain because we have our own audits and trust ourselves. I used information labeling techniques. Even city-level or IP-level targeting.

Q: CDNs?

Wendell: Network addressing is considered imprecise, even with IPv6.

Doc: What Google came out with this morning. Is it possible on G Day when all these sites had no front door, people will say I hate all this?

Arthur: There is research on that. The lack of opt-in is 70%. Depends on how you do it. Many small publishers will turn away from tracking and make brands bring the consent with the data.

Wendell: NY Times may get your name and address. Some other place you might not let have anything.

Iain: Big minefield. You must provide an equivalent service without consent.

Wendell: Other ways publishers will get the ability to have user data. Pay walls will grow up. Maybe micropayments. Non-money kinds of things. If you're doing ad tech, you need consent and chain of custody. If you're doing a newspaper, why not just have a paywall. The regulators are going to make a decision about whether your paywall is real or not. As Joyce presented yesterday, none of this has been actually focused grouped. It should have been focused grouped for years, walked through many different levels. For various reasons, it wasn't. And now here we are. It is 55 days. What are we doing. The number of phone calls of business people who don't have answers yet is stunning.

Q: Some words don't pass the 8th grade reading level, like rectification.

Arthur: The industry focuses on ourselves. Now we have to pay attention. I go to hundreds of sites a day. Little publishers will take all tracking all tracking off your site and go to contextual targeting and let the brands bring in the data. The Internet may become unusable.

Q: Consent form blockers?

Dave Husedy, Hyperledger: What are you doing for data integrity? Would you open source your chain of custody?

Wendell: Those are more ideas.

Quest for the Mnemon Seed: The Three R's of Key Management: Reproduction, Rotation, Recovery

Wednesday 3A
Convener: Samuel M. Smith
Notes-taker(s): Samuel M. Smith

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

QuestForTheMnemonSeed_IIW_20180404.pdf

https://github.com/SmithSamuelM/Papers/blob/master/presentations/QuestForTheMnemonSeed_IIW_20180404.pdf

This session discusses a new class of data called *decentralized autonomic data* (DAD). The term *decentralized* means that the governance of the data may not reside with a single party. A related concept is that the trust in the data provenance is diffuse in nature. Central to the approach is leveraging the emerging [*DID*](https://w3c-ccg.github.io/did-spec/) (decentralized identifier) standard. The term *autonomic* means self-managing or self-regulating. In the context of data, we crystalize the meaning of self-managing to include cryptographic techniques for maintaining data provenance that make the data self-identifying, self-certifying, and self-securing. Implied thereby is the use of cryptographic keys and signatures to provide a root of trust for data integrity and to maintain that trust over transformation of that data, e.g. provenance. Thus key management must be a first order property of DADs. This includes key reproduction, rotation, and recovery. The pre-rotation and hybrid recovery methods presented therein are somewhat novel.

The motivating use of DAD is to provide provenance for streaming data that is generated and processed in a distributed
manner with decentralized governance. Streaming data are typically measurements that are collected and aggregated to form higher level constructs. Applications include analytics and instrumentation of distributed web or internet of things (IoT) applications. Of particular interest is the use of DADs in self-sovereign reputation systems. A DAD seeks to maintain a provenance chain for data undergoing various processing stages that follows diffuse trust security principles including signed at rest and in motion.

Streaming data applications may impose significant performance demands on the processing of the associated data. Consequently one major goal is to use efficient mechanisms for providing the autonomic properties. This means finding minimally sufficient means for managing keys and cryptographic integrity.

Importantly this session describes detailed descriptions of the minimally sufficient means for key reproduction, rotation, and recovery for DID leveraged DADS.
More detail can be found in the RWOT Spring 2018 Paper in file DecentralizedAutonomicData.md at https://github.com/WebOfTrustInfo/rebooting-the-web-of-trust-spring2018/tree/master/final-documents

This is the link for my paper on Friday

ReputationDisintermediation_IIW_20180405.pdf

https://github.com/SmithSamuelM/Papers/blob/master/presentations/ReputationDisintermediation_IIW_20180405.pdf

Bringing the best of IIW to India

Wednesday 3C
Convener: Munir Mohammed, Maria Palombini
Notes-taker(s): Munir Mohammed

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

Suggested Topics:
- Affordable Technologies
- Accessibility
- Cultural/Ethnic Requirements
- Device Challenge (1 per family) and how the identity works
- eKYC/Aadhar

Set up Suggestions:
- To have lightening taks (5 mins) to bring momentum
- use Posterboards

Outcomes:
- relationships
- Discussions
- Interoperability/Collaboration
- Building Communities

FastFed & OIDC Federation: Enough Similarities to Share/Merge?

Wednesday 3D
Convener: Darin McAdams and Roland Hedburg
Notes-taker(s): Darin McAdams

Tags for the session - technology discussed/ideas considered:
SSO, Federation, OIDF

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

FastFed and OIDC Federation are two standards under the Open ID Foundation. This session examined the similarities/differences between the goals and how they should align. This was done by enumerating the market segments and goals for each spec.

FastFed went first. The initiative originated from the commercial/enterprise space. In this world, a company may use an IdP such as Google/Azure/Shibboleth/ADFS... The company may also use SaaS apps such as Salesforce, DropBox, etc... Today, setting up SSO between an IdP and a Saas app can take 1-2 weeks by an enterprise administrator. Goal of FastFed is for it to take 1-2 minutes.

To achieve this target, FastFed aims for the following measures of success:

- Configuring SSO is self-service by the enterprise administrator. No need to talk to anyone at the IdP or SP.
- No identity knowledge required. An administrator shouldn't need to understand SAML or OIDC; this is largely abstracted away.
- Mouse clicks only. Administrator don't need to read documentation, copy and paste values into forms, or upload/download files. A simple wizard experience.
- Solve both SSO and User Provisioning

Assumptions:

- The administrator(s) have existing accounts at the IdP and SP for their company.
- IdP provides the governance controls about what administrator(s) can do. For example, a member of the organization can be given permission to configure SSO to all apps, or to a specific type of app like "Salesforce". This is defined and controlled within the IdP. Out of scope of FastFed.

NOT Goals:

- Trust relationships between the IdP and SP. There is no relationship between these parties, no compliance schemes. An enterprise decides what they want to use.
- No SSO Metadata validation, except for the following:
    - Knowing "This is a Salesforce app" so the IdP can enforce access controls for administrators around whether they are permitted to configure SSO to Salesforce (or whatever app).
    - Redirect URIs are valid for the app vendor. E.g. Salesforce only uses Salesforce URLs for redirects. Basic security stuff.

Problems to be solved in order to achieve these goals with OIDC:

- Dynamic Client Registration: how to make it self-service by an administrator? How does the SaaS app attain the registration endpoint and initial access token?
- User Schema: Need a shared schema to avoid asking the administrator to specify attribute mappings. OIDC schema is insufficient. SCIM has EnterpriseUser, but no finalized specs for binding SCIM->OIDC
- Trusted way for Salesforce to prove "I'm Salesforce" during the SSO configurations flows.
- User Provisioning: How. (SCIM?) When. (JIT, Pre, Other?)

Next, OIDC Federation took the floor to explain the goals. In essence, everything that FastFed specified as "NOT a goal" is what OIDC Federation took as an explicit goal. No overlap. It's seeking to bring the federation concepts from SAML into OIDC protocols (e.g. InCommon) Proposal is to sign the OIDC metadata statements to prove compliance and membership in various federations. OIDC Federation is focused on sectors like higher education.

The remainder of the discussion was about the different market segments, how they behave, and whether some customers may desire both FastFed and OIDC Federation (short answer: yes, and the two standards should play well together).

Q) How does someone join a federation?
There is an audit, either on-prem or self-certified. Goal is to prove this audit happened.

Q) What is a use case for RP to depend on OP in federation.
Student taking classes at another university.

Q) How to discover the OP for a user?
OIDC Discovery doesn't really work. They might all have gmail addresses. May force people to specify a university name, or select from drop-down. Universities just own identities, can rely on other service providers like google for authentication.

Q) User Schemas?
Still a hard problem. It's a mess.

Q) Is anyone looking at defining a SCIM schema for the educational sector?

Still need to define a standard set of claims in educational sector.
One thing in progress within Internet2. Search for: "APIs and Schema — The Relationship between TIER and SCIM".

Saving Democracy - What Could Happen

Wednesday 3F
Convener: John Kelly
Notes-taker(s): John Kelly

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

We voted individually on whether each of 16 future events were highly likely, unlikely, or uncertain.

We noted that voting on future events works even if we strongly disagree about what should happen.

Event voting is an example of voting to discern - deciding what is important and meaningful, before deciding what we will do about it.

This is just one example of group democracy akido which can help foster collaboration among people who initially believe cannot or should not collaborate.

The future cases we voted on can be accessed here:
https://docs.google.com/document/d/1fA0P_GGyvge5Ax8orZpfoeOxEaNL7bPLdHh9vO2hRZA/edit?usp=sharing

Digital Guardianship

Wednesday 3J
Convener: Peter Simpson, Bryan Pon, Drummond Reed
Notes-taker(s): Drummond Reed

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

This session was given by three trustees of the Sovrin Foundation:

- Peter Simpson, Founder and Executive Director of iRespond
- Bryan Pon, Principle Researcher at Caribou Digital and Chair of the Sovrin Identity for All Council
- Drummond Reed, Chief Trust Officer at Evernym and Chair of the Sovrin Trust Framework Working Group

The session started by recapitulating the basic concepts of self-sovereign identity (SSI) from the SSI 101 and 102 sessions on Tuesday and Wednesday morning, especially the roles of Issuers, Holders (Identity Owners), and Verifiers of digital credentials.

Then Drummond explained the dilemma that some classes of Identity Owners, such as infants, the elderly, refugees, and those without Internet devices or access, require the services of a **guardian** in order to wield a self-sovereign identity. See the Sovrin Glossary and Sovrin Trust Framework for specific definitions and examples. See slides 53-62 of the first link below for visual diagrams of the guardian role.

Peter then explained that very often when a guardian is needed, so too is a method of identification of the Identity Owner that does not depend on a local device. This is the role of a **biometric service provider** (BSP). See the Sovrin Glossary and Sovrin Trust Framework for specific definitions and examples. See slide 61 of the first link below for a visual diagram of the BSP role.

We had a good discussion about how a BSP works and still provides adequate control and privacy protection to identity owners by virtue of being separate from a guardian.

Bryan then led a discussion around the many questions and challenges of digital guardianship and how it is a crucial concept the work of his Identity for All Council at the Sovrin Foundation.

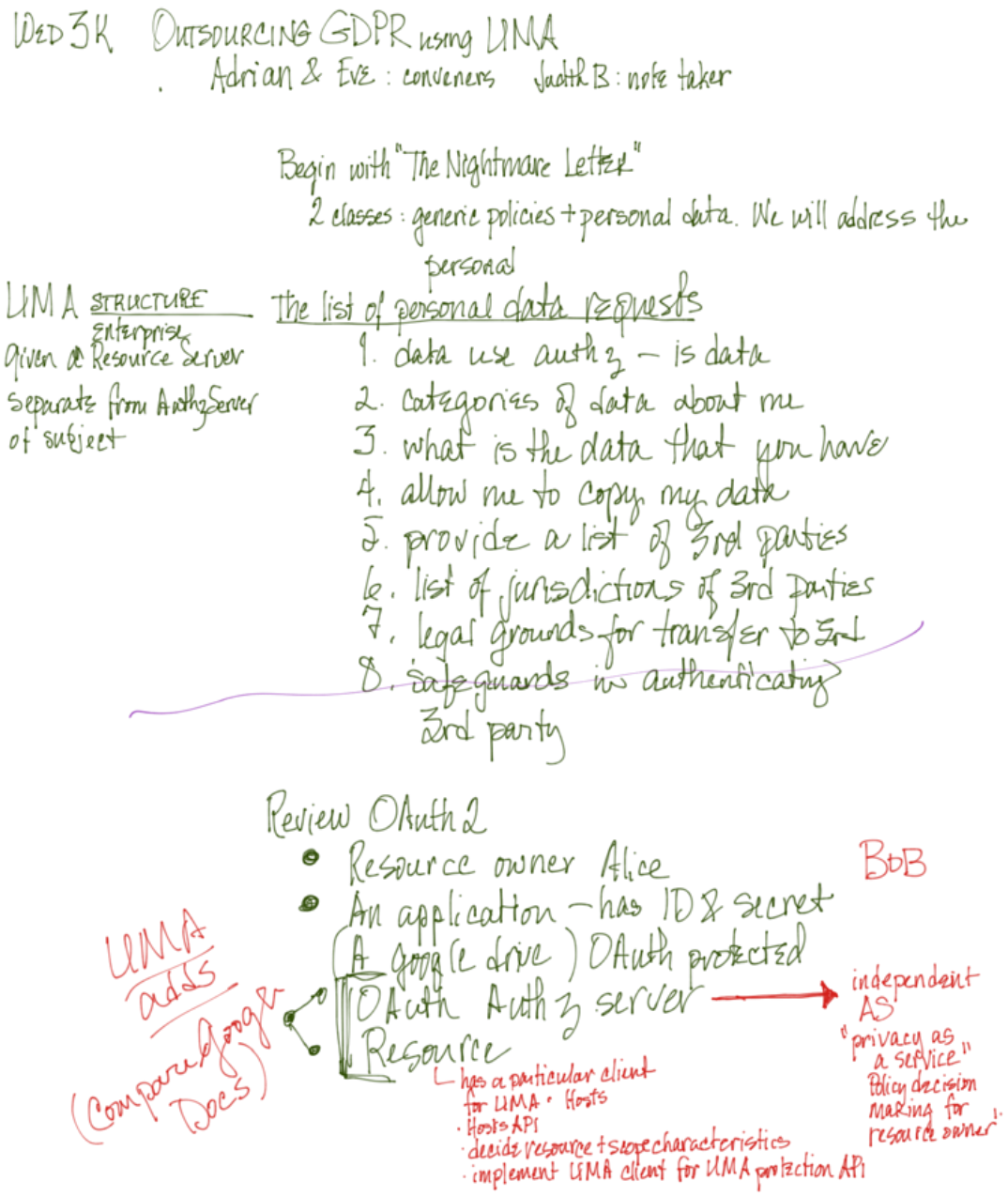
Links:

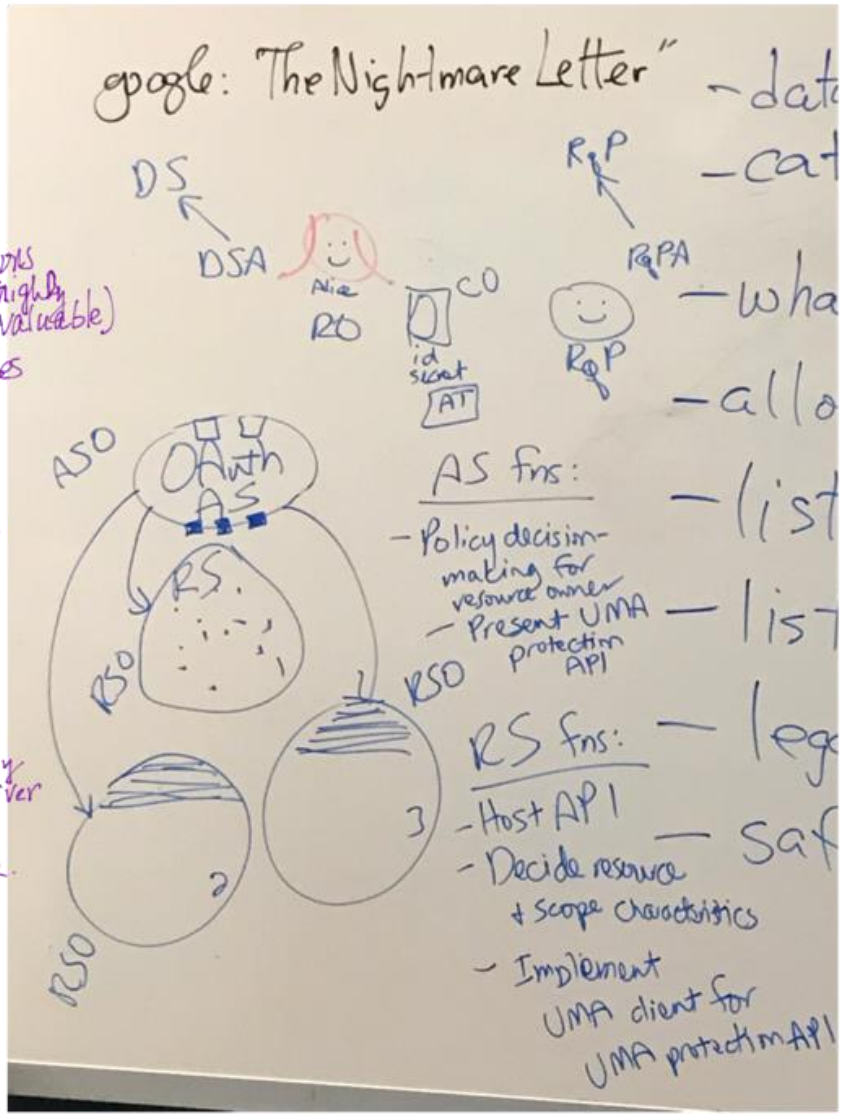
1. IIW Introduction to Self-Sovereign Identity
2. The Sovrin Glossary
3. The Sovrin Trust Framework

Outsourcing GDPR Using UMA

Wednesday 3K
Convener: Adrian, Eve
Notes-taker(s): Judith Bush

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





Identity
vs
Issuer (External assertions that are highly valuable)
vs
Self asserted preferences
"isle or window"

The difference between an IDP & AS "personal" is vast.

Does a resource server tightly couple to a single Authz server or allow Alice to choose her "privacy as a service" provider.

If you are going to AI your preferences vs. explicit settings or "inherited" settings ...

Compare to a RS accessing an AS that you own, the AS can machine learn FROM THE SUBJECT. (The AS has a fiduciary relationship to the subject)

IAB EU Transparency & Consent Framework

Wednesday 3L
Convener: Wendell Baker
Notes-taker(s): Wendell Baker

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

Transparency & Consent Framework, Interactive Advertising Bureau (IAB)
- Frequently-Asked Questions (FAQ); 2018-03-08.
- Cookie and Vendor List Format, Version v1.0a
- CMP.js API, Version v1.0, hosted at Github

Purposes
- **Accessing a device** allow storing or accessing information on a user's device.
- **Advertising personalisation** allow processing of a user's data to provide and inform personalised advertising (including delivery, measurement, and reporting) based on a user's preferences or interests known or inferred from data collected across multiple sites, apps, or devices; and/or accessing or storing information on devices for that purpose
- **Analytics** allow processing of a user's data to deliver content or advertisements and measure the delivery of such content or advertisements, extract insights and generate reports to understand service usage; and/or accessing or storing information on devices for that purpose.
- **Content personalisation** allow processing of a user's data to provide and inform personalised content (including delivery, measurement, and reporting) based on a user's preferences or interests known or inferred from data collected across multiple sites, apps, or devices; and/or accessing or storing information on devices for that purpose.

Features
- **Matching data to offline sources** combining data from offline sources that were initially collected in other contexts.
- **Linking devices** allow processing of a user's data to connect such user across multiple devices. **Precise geographic location data** allow processing of a user's precisegeographic location data in support of a purpose for which that certain third party has consent.

Purpose versus Feature
- **Purpose** is a data use that drives a specific business model and produces specific outcomes for consumers and businesses. Purposes must be itemised at the point of collection, either individually or combined.
- **Feature** is a method of data use or data sourcing that overlaps across multiple purposes. Features must be disclosed at the point of collection, but can be itemised separately to cover multiple purposes.

Promotional

- InteractiveAdvertisingBureau/GDPR-Transparency-and-Consent-Framework, at GitHub
- The Advertising Industry's GDPR Transparency & Consent Framework, IAB Europe; also advertisingconsent.eu

Transcription of the session by Mei Lin Fung

Organizer, People Centered Internet, co-founded with Vint Cerf

External advisor to the Stanford Center for Population Health Science

Member of the Global Future Council on Digital Economy and Society, World Economic Forum

Member of the Steering Committee, World Economic Forum, Internet for All

Vice Chair, Internet Inclusion, IEEE Internet Initiative

(e) mlf@alum.mit.edu ; mlfung@gmail.com

(t) meilinfung

IAB report discussion – Wendell Baker

There is another permissions level –

Consumers who have their consent cookie will participate, defacto is 'no consent.

On a chain of custody basis – to signify that consumer had given consent to …..

List permissions defined to date on Pg 18

Consumer can state this in their browser as defined by a publisher

Thru real time bidding – server to server – can signal what consumer has consented to along the way

Because all members of IAB have signed agreement – this is a voluntary group creating a conforming standard

This allows IAB members to speak to each other

Consumer must consent to be tracked otherwise GDPR will not allow it

Doc – Adtech system defacto becomes an identity provider about consumers who have given consent – by solving the cookie mapping problem

Wendell – IAB says we are only doing consent.

Cookie tracking problem – fall out, people hate it, if consumers have an ID.,.. could be helpful

Sam – will content be held hostage – consumers will not consent otherwise

Iain – have to have equivalent service for those who do not consent

Wendell – who is going to sign up for this? At OATH we will launch a dialog to fill in this stuff – 3rd party publishers have to conform to GDPR in Europe – have to ask invasive questions (once provided you log in thereafter)

Cookies will time out – may be very short

Sam – law requires that equivalent service must be provided for those "unwilling to consent"

Wendell – debates with engineers who think only a few will not consent. There will be a wall

Iain – 1 minute part midnight after GDPR – we should expect things to half

Wendell – we expect to be QA'd before going live. Usually on Internet – its as its rolled out – we will this time, build tests ahead of time – its no longer cheap on the web – we will have to insist on provenance tracking

Doc – on commercial web (which is not the whole web – not Wikipedia, not universities) – we will see a new front door on every website

When people see all these front doors – all different – der Spiegel, Wikipedia, google – and all have a different consent gauntlet…

Will people hate

The sites
The advertising business
European regulator

Or will there be a universal log in ?

Iain – this is about competitive play for Europe – people expect innovation to spring up in Europe – on the side of the individual

Wendell – log in providers springing up – Universal SSO using SAML will happen – ifts a paywall, what do you pay, what do you give people who don't pay – can have tiers of service

Consortia for Universal log in – VIANT

Doc – this table will be half this conference in IIW October

Brides magazine – very confined customer basis

Wendell – lots of niche blocks – ADSENSE will come back – problem in industry is how to show auditing for circulation which we say we have – alternatives to current estimates – working out what is the right balance

Login requirements and Sarbanes Oxley requirements are more onerous

Adblock – was 10-15% then became inflammatory when people emerged using beacons to see if ad was above the fold or not, or whether it appeared or not

In the old days, you could bill for adblock – now viewability tracking is possible for campaigns

Now adblock is untenable to all the industry

See business insider article about the consortia – Axel Springer, VIANT, French newspaper

Imagine you need to log in to newspaper with auditable logs

Andrew – I already do – I have a subscription

Wendell- now the law will require it

Sam – people will have a huge burden – some consent is worth it and some is not going to be worth it

Paywalls, etc – have to move barriers far enough "gauntlet required content" or "gauntlet not required content" that division is going to be really obvious

Wendell – a lot of content is written by robots – eg spammers create content.. financial earnings

Propublica deep dive – real journalism costs a ton of money and risk for a person…

So less material to read – people will recognize the robots – ads will not be able to monetize the robot content in the old way – that could change the proportion of robot content – (MLF: up or down?)

Sam – people will feel it in terms of gauntlet and in terms of distinguishing between content that is robot generated vs human generated

…….: What about cut and paste?

Wendell – not supposed to be doing it – that may show up for a while

Targeted audience buying was always odious to publishers…. Supply and demand are usually inverses in econ 101. Buy side is a lot smarter – they are not inverses in practice – changed through more information

Publisher mindset is not sophisticated – supply side is not keeping up with buy side sophistication

Doc – when ad tech came along and brand advertising entered the Internet – there is not a function at the publisher to do that… they will go to a 3rd party and say give us a front door to cover this for the GDPR

Andrew –yahoo portal may come back – if publishers are told by Google to manage the layer, one way to solve it is to publisher portal

Wendell – OATH family may offer publisher tools –

Doc – May 25th – will every app require it ?

All adware apps have this problem –

Wendell - data must be stuffed into adware SDK's that will work with this

IAB is only display ads – not mobile apps

Consent string thru our apps – we will use the consent signaling string –some adware vendors will say " we will do our own thing"

Its an IAB decision whether to deal with them

When someone says I'm not ready for IAB…. That's one thig

When someone says I'm not going to use this – then we say Thank you, when you are ready to do business in Europe, come back

If you have a login system – you get this once. Without log ins – you will be asked everytime

Doc – it will be wild

Wendell – analytics will be split in consent and non consent

Doc – the answer is a simple and standard across individual side that says "here's how I work" across all the stuff (google, etc)

Wendell – would have loved W3C and vendors took it on. Bake in all ideas into next gen browser

Separate cookie jar that holds this cookie

Doc – I followed DNT (do not track) which showed up at Berkman center – someone spoke up – John Mayer – like Do not Call – this became the "tracking preference"

Wendell – that's Adblock baked in the browser – if the affordance is in the browser baked in at the sale of the device showing the browser – signaled up to the server to know consumer's preferences

Our nightmare is 1 button – never see ads again – never happened

Tracking preferences for blocking ads – this is a permissions based thing – positive consent
Dave – only works if there is a common ontology

Wendell – IAB has members to develop this
There is a different group on the browser, phone and devices – not been involved.

We are 1 browser release away from universal ID and a cookie management process – they could make the problem go away

Apple instituted ITP – intelligent tracking protection – survey your cookies – if they detect a tracking cookie

If you are in a first party context – user preference prevails

Dave Huston– firefox had this – I worked on this at Mozilla - not on, by default

Sam - if it is really bad – gauntlet is bad – need to respond

Doc – what can customer commons do?

Wendell – standardize terms. Stand up a consent manager with your own terms

Dave – because you have an accounting piece – consider overlap with decentralized ledgers – they are trying to teach browsers to do authentication using ledgers – signal something to a browser that you are going to consent (or not) to terms

Merge the two ideas together – always have consent payload, sometimes have authentication payload

Wendell – could signal something benign, send it around – consent – if leaked is that a big deal?

Circulate to developers, first responders – if behavior is like a Cert

Dave – will look like when a Bank sends something to a phone – needs to be something on your phone – interactive consent

Sam – use TLS flex one (Evernym)

Andrew – Kantara – data format to report purpose and consent of user – transmit to others – like the cookie but full data format – consent receipt to fill gaps – need transport in, interfaces specified

What would it take to make a transport format (right now it's a data format)

Its just a spec – this is what a receipt looks like
Dave – could it be an RFC

Andrew – consent receipt envisions the activation of GDPR – this is a method to …..
Not cc

Iain - No uptake because not marketed well.

Mei lin – what can we do? IIW

Wendell – many generations of IIW address different needs – material economic, commercial knowledge of GDPR is not here. No one is talking – after GDPR everyone will be talking – IIW can address with incompleteness of industry solutions.

Sovrin – Exploring Building an Alliance: Want's & Needs (especially if you are not Everynym)

Wednesday 3M
Convener: Kaliya @identitywoman
Notes-taker(s): Kaliya @identitywoman

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

This session was called to explore the development of the Sovrin Alliance.

People said that the network needed to figure out how to communicate clearly how it is uniquely better they other options in the market place.

WE identified several persona's.

Program Managers who make choices about what to commit to.

Cybersecurity - need to see the deep technology.

Developers who are the ones who need libraries to do the integration.

Executives - who are also making decisions.

Regulators - who need to understand the tech.

Explanation is needed to communicate to these types of people.

Relying parties need to know more about what the benefits are including economics and risk lowing. There also needs to be work on creating a market for claims.

Issuers need to be developed - so for example can death certificates begin to be issued in this way.

Then of course there is the Claimant - the Individual.

Demonstrations are needed so that people can use is.

Industry areas that were identified as being present and where work should be done.
- property
- banking industry
- voters
- alternative social web
- Universitiy
- Health Care
- ID Verifiection
- Pharma

- Manufacturing and Supply chain
  - High value provenance
  - Food
  - Pharma

Value Network Mapping didn't happen but people can learn more about it here.

https://identitywoman.net/value-network-mapping-an-ecosystem-tool/

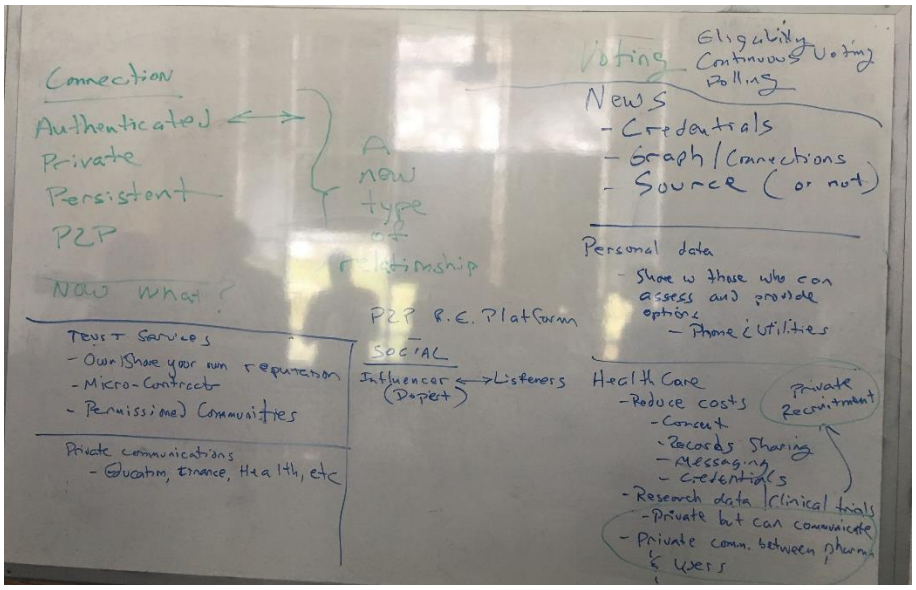
And we will do it again some time soon.

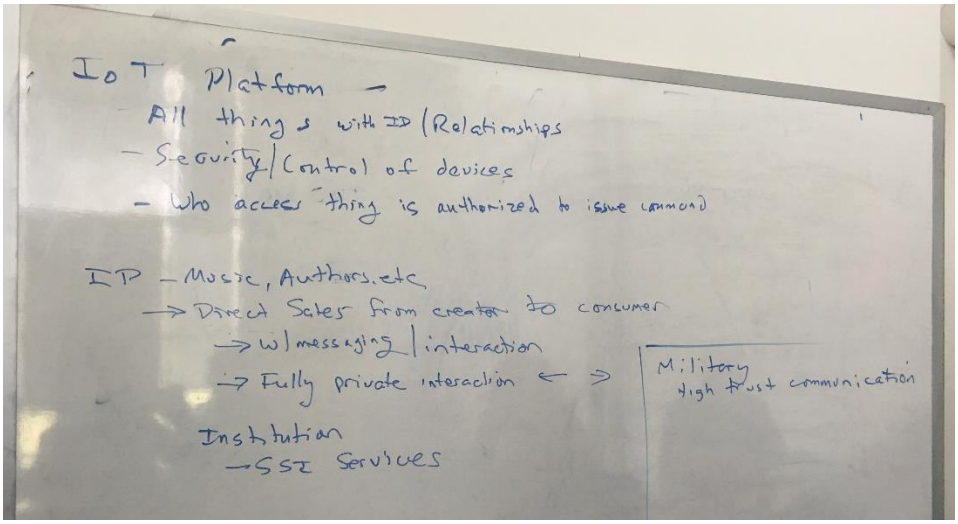
The Business of Self-Sovereign Identity

Wednesday 4A
Convener: Timothy Ruff & Steve Havas
Notes-taker(s): Riley Hughes

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

We talked about what the business of self-sovereign identity looks like. We drew a handful of dots on the board, each one connecting to the other. Tim said something along the lines of, "When we talk about self-sovereign identity, we often think too much about the dots. When we talk about business, we need to think of the lines." We continued to talk about how having a DID relationship with another party creates a secure, encrypted, direct relationship between the parties. The question was asked, "what types of businesses become possible when you have this type of relationship?" The photos attached are the discussion that followed.





Kantara Consent Receipts – Communicating User Consent Between Data Controllers

Wednesday 4B
Convener: Andrew Hughes
Notes-taker(s): Andrew Hughes, AndrewHughes3000@gmail.com

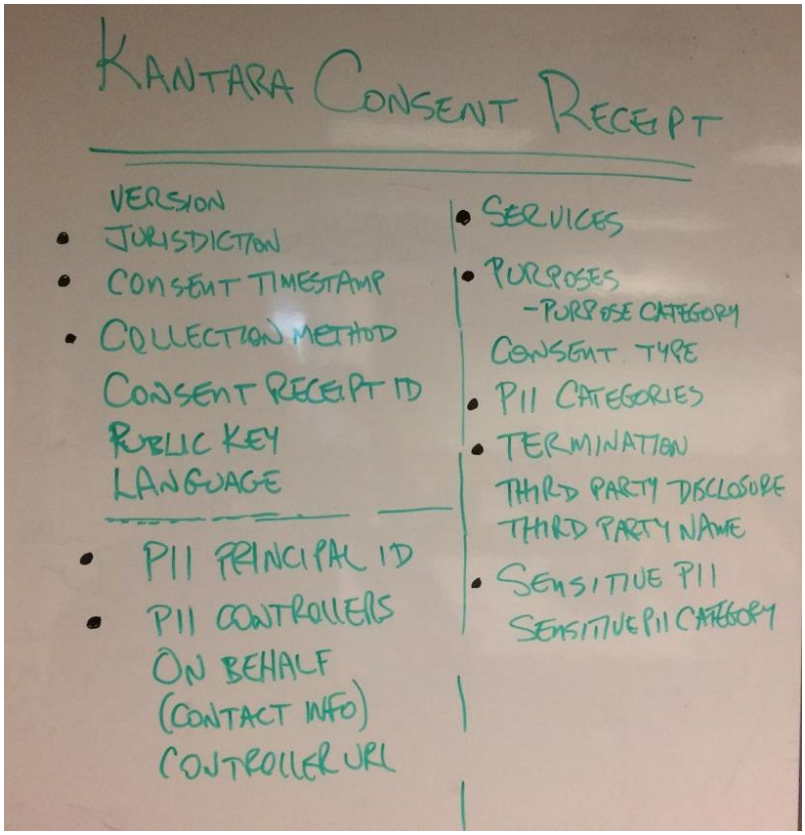
Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

Andrew Hughes, AndrewHughes3000@gmail.com

Kantara Initiative Consent Receipt Specification – uses for interoperable communication.

The Kantara Initiative Consent Receipt (CR) Specification is a standard record format used to record information about a person's consent to collect and process their personal data. By itself, the CR is not very interesting. However, widespread use of this common data format will enable interesting possibilities.

This picture shows the fields defined in the CR. The dots highlight interesting fields that would usually be recorded by any data controller that collects user consent.



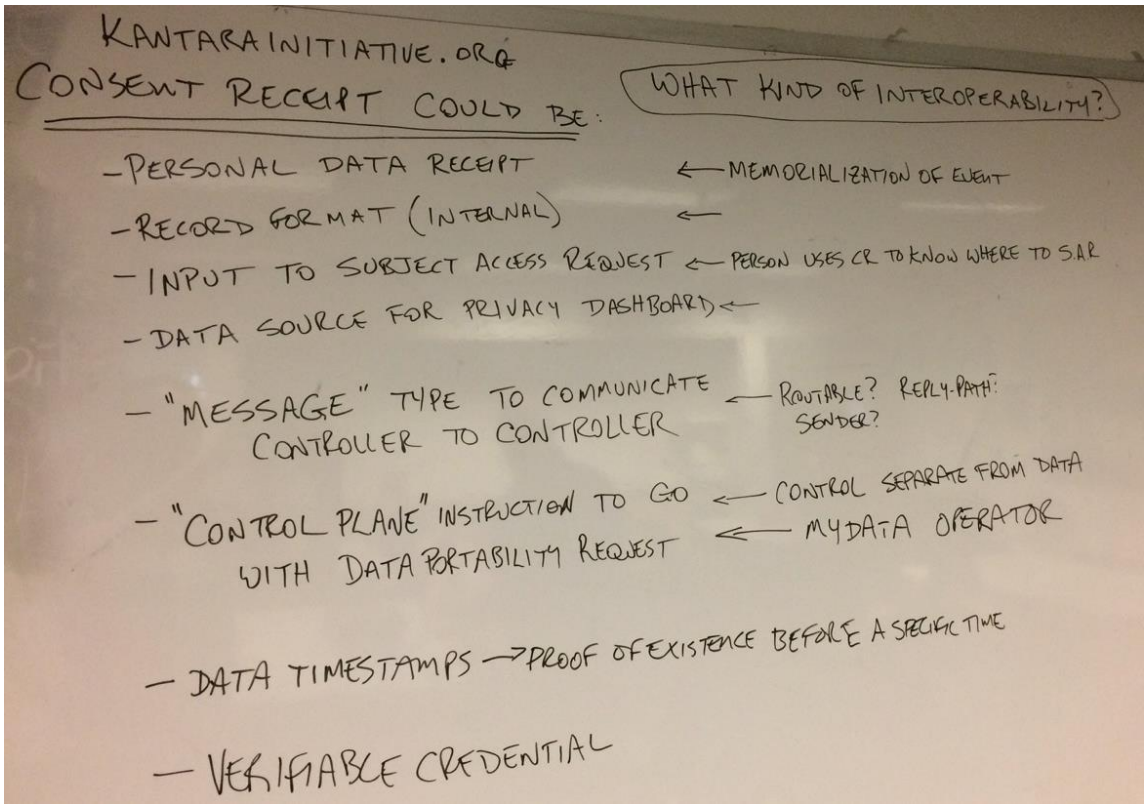
The main question discussed was what ways might consent receipts be used to enable interoperable communication of consent information or transmission of personal data.

We talked about 'privacy dashboards' that might show a person all the places where they consented to data collection. The dashboard might have buttons to 'revoke' consent, submit a Subject Access Request or other interesting activities.

In the case where one controller needs to communicate the consent they collected from a user to another controller, the CR might be constructed as a type of 'message' that is transmitted using a messaging system. Questions were: should these CR messages be routable? Should they have things like reply paths or senders in wrappers or headers?

We also discussed the concept where the CRs acted as 'control plane' that might be transmitted separately from the actual data when porting data from one controller to another.

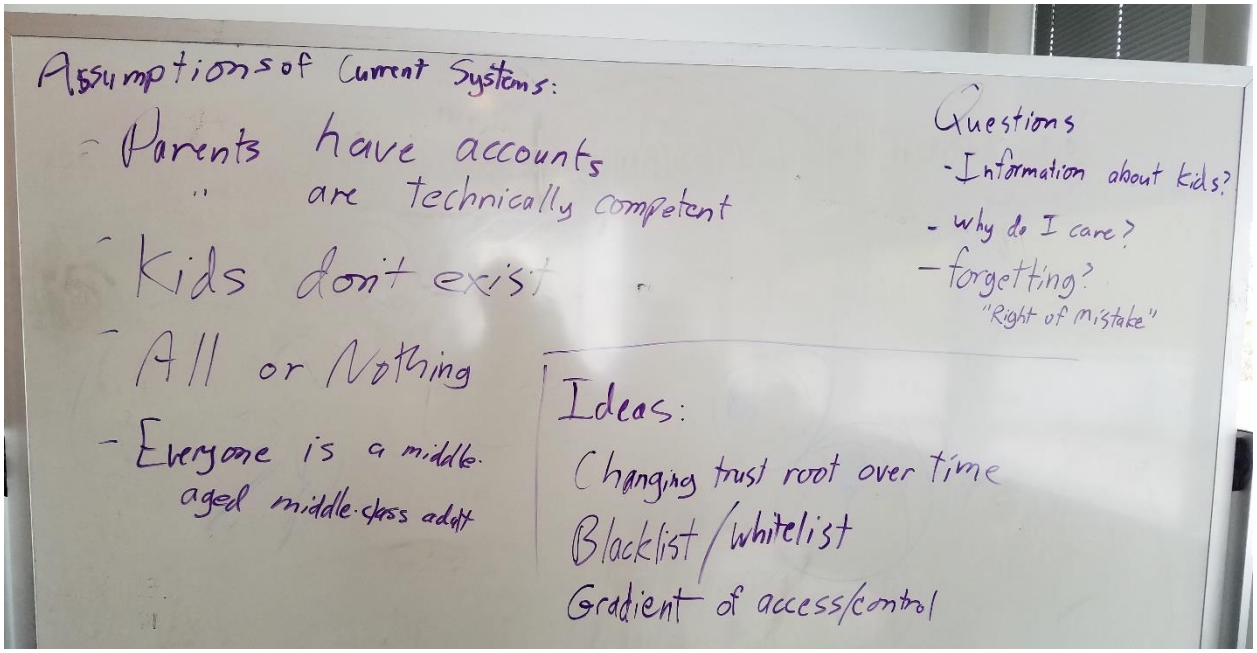
The call to action is to watch the Consent work groups at kantarainitiative.org as we work on interoperability using the CR spec and build stuff.



The "ID" Of Kids

Wednesday 4C
Convener: Justin R
Notes-taker(s): Justin R

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



Expanding Language = The Identity of Words ~ Amebic / Shape Shifting

Wednesday 4D
Convener: Jeff Orgel
Notes-taker(s): Jeff Orgel

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

As people interact with technology and systems on the digital landscape we use language of various sorts. Symbols, gestures and most of all, words all play a part. Just as technology and systems change, so too, do many the related elements of communication. Icons, touchpoints, the interface itself shift and evolve over time.

Whereas much of the above occurs due to system and engineering design changes, words change in a space "off band" of these design shifts. Culture operates on its own. A word can take on a completely new meaning, sometimes overnight. "Sick" doesn't always mean ill. "Pink" is not always a color. "Free" is a term related to a value exchange which most people are often not clear about. While we usually perceive free as meaning at no cost, related to no dollars and cents, digitally it often means the values exchange is more valuable, persistent "payment" in a currency that may never stop following you around…ever.

Unless you take the time to read the terms and conditions, how will you know the currency being exchanged? When my Father searched for replacement parts for a tool, how would he have known that "wet" and "grinder" are sexually freighted terms in the digital game space of search? How would people know that their tween/teenager is walking around with a very sexualized term printed boldly on their clothing…because "pink" is not always a color…

In order to best help the Human OS operate in the scope and bounds of the individual's intention, this Real-IT ® awareness skillset keeps people between the lines on their digital journeys. As a tool in that skillset, the best tool I am aware of at this time is www.urbandictionary.com . The challenge of knowing what means what when is often formidable.

As we ourselves are defined and identified as this or that in the digital landscape based on our actions and choices, understanding the amebic and shapeshifting nature of language, is a baseline for sturdiness and maintenance of intention.

Discussing + Examining CULTURAL BIAS In Specifications and Other Technical Documents

Wednesday 4E
Convener: Mike Maturo
Notes-taker(s): Liam Quin.

Session tags:
acknowledge bias, diverse organization creation, develop anti-bias efforts at IIW and beyond

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

Hosted by Mike Maturo of the City of Osmio
Attended by Kaliya, Jogi, Time, Kazue, Amy, Liam, John, Munir, and Elizabeth

Some reasons for attending:
- Japanese culture is very different
- saw a book, Automated Inequality
- MIT lab work in the area of bias
- people whose parents have no identity docs because of border changes
- gender bias
- design and architectural choices in tech that impact how we related to each other
- the context of technology development
- Lots of cultural, gender bias issues in India; interesting that in India there might be one device (phone) per family, not per identity
- diversity in W3C working groups and in specs

Bias is not only cultural, racial, or gender but disabled accessibility too
Linguistic bias: how does one from non-English-speaking culture do a search?
Example given: meditation app that was popular in US/UK but incredibly difficult to translate

Explicit biases are easier to address than implicit biases, but drive implicit biases (note off-chain values and their impact on on-chain infrastructure, so to speak)

Real-world inequalities/lack of diversities are manifesting in our technology

Bias is not always bad, e.g. staple guns made for men with big hands, but bias needs to be identified.

Book: “Blind Spots” on gender bias
Address bias by putting multiple people with different biases together (but some people don’t even know they’re biased)

You have to have self-awareness, so you can hear someone telling you that you’re biased
Old boys networks exist in the left, too: "I'm only going to work with people who are culturally sensitive"

“Human First Tech” is a website dealing with issues of bias

Remember, though, that fighting bias can lead to increased resistance from those in power

We take for granted at IIW that giving everyone an identity is good, but what is someone wants to opt-out?
If SSI means exercising who you are, you should have the right not to be identified.

You need to make something happen, and make it right. We need to have diversity to make it happen. Sales activities should be enabling this.

Rightscon.org
Rights must be balanced with responsibility; who is responsible for feeding people?

There are cultural assumptions about what white men do to built trust.

We should talk about accountability, not trust (e.g. accountability vs. trust frameworks)

What's the average income of IIW people? Are we conscious of our class, of our privilege?

How can people recognize their privilege at IIW e.g. morning circle

At W3C, formal reviews for language, culture, and accessibility bias are conducted

6 mo children could distinguish chmpanzees as well as people; at 9 months could only distinguish humans. So we prune our abilities. So maybe white children not expost\ed to (say) African Americans don't learn, have early acquired bias.

UMichigan Geography of Thought

Lot of stuff here is about self-empowerment, anti-social-order

Ideas for IIW participation in anti-bias activities:
- anti-bias training for IIW leadership and community sessions
- PoC caucus (a la women's breakfast) with parallel "white ally"
- code of conduct
- white awareness
- Improve the pre-event video, feels like an exclusive video
- karaoke (again)
- prominent leadership spend/ multiple days in off-site training
- how can we help people here develop technology w/o biases in it?
- people building reflective of people who effects

An Analysis of S.S.I. Using Appreciative Inquiry

Wednesday 4F
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:

https://www.slideshare.net/heathervescent/selfsovereign-identity-an-analysis-using-appreciative-inquiry

Mobile APP - APP OAuth

Wednesday 4G
Convener: Dick Hardt
Notes-taker(s): Dick Hardt

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

Applications can register and own an https URL that can be used to invoke an application to start an OAuth flow. The client app can invoke an API on iOS that will invoke the app with the standard OAuth parameters. If the app is not installed, iOS will return a failure, and the existing in-app browser flow can be invoked. We did not have time to discuss Android, but the view was it should be easier to do.

The Future of Privacy While Accessing Published Content / SAML Interoperability Deployment Profile

Wednesday 4H
Convener: Judith Bush & Nick Roy
Notes-taker(s): Keith Wessel

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

While updating SAML2int, the working group chose to tackle some of the bigger issues that challenge federations today. To help the reader understand some of the group's decisions, here is a summary of a few of the issues and our rationale behind the requirements for these issues. Feedback on the requirements for these items, as well as on anything else in the document, is of course encouraged.

Identifiers and NameIDs
This section eliminates the use of any NameID format other than transient. In addition, the complex, confusing, and in some cases poorly adopted set of attribute identifiers used today has been replaced with two clear identifiers for communicating the subject. This model leverages the new OASIS identifiers profile: https://www.oasis-open.org/committees/download.php/62438/saml-subject-id-attr-v1.0-wd04.pdf. While the identifiers profile is

Logout recommendations
Federated logout is a long-standing debate in the community. The working group, after much debate, created requirements to establish clear guidance. IdPs need to accept a logout request from an SP and need to publish a logout endpoint. What they do with the logout request is somewhat flexible: there's not a one size fits all. The profile also touches on the danger of an SP performing an automatic federated logout as a result of user inactivity. SP support of single logout requests from IdPs is included, but we chose to leave this optional. We feel that our approach will meet the needs of deployers while leaving room for institutional policy.

Logos
Firm requirements around logos have been needed for a long time. Requirements today even differ from one federation to another -- a problem in the era of Edugain. The InCommon baseline expectations provide further necessity for logos. The profile makes some clear guidance for format and size along with suggestions for appearance. The working group tried to be specific while leaving room for artistic interpretation
still in process, it continues to move toward adoption. We believe this will make the adoption of identifiers much clearer and easier and the choice of identifiers by service providers more straightforward.

Cryptography
Several major vulnerabilities over the past few years have underscored the importance of modern cryptographic algorithms. Cryptography requirements in this document attempt to set a firm line for what's needed to securely sign and encrypt. At the same time, the working group tried to make the requirements relatively future proof.

Deep linking
This is an issue that can cause significant frustration to those using federated services that lose track of the intended destination during the login process, and the working group saw this as one that needs to be fixed. The requirements for this aren't complex but serve to remind deployers of something that often gets overlooked, especially when federated authentication is tacked on later.

Support for multiple IdPs
This issue works together with deep linking in most cases. Other profiles and earlier versions of SAML2int mention the importance of IdP discovery. This section stresses that any federated application needs to be prepared to work with multiple IdPs, a limitation of many applications today.

Logout recommendations
Federated logout is a long-standing debate in the community. The working group, after much debate, created requirements to establish clear guidance. IdPs need to accept a logout request from an SP and need to publish a logout endpoint. What they do with the logout request is somewhat flexible: there's not a one size fits all. The profile also touches on the danger of an SP performing an automatic federated logout as a result of user inactivity. SP support of single logout requests from IdPs is included, but we chose to leave this optional. We feel that our approach will meet the needs of deployers while leaving room for institutional policy.

Logos
Firm requirements around logos have been needed for a long time. Requirements today even differ from one federation to another -- a problem in the era of Edugain. The InCommon baseline expectations provide further necessity for logos. The profile makes some clear guidance for format and size along with suggestions for appearance. The working group tried to be specific while leaving room for artistic interpretation.

DID Resolvers and DID JWT

Wednesday 4I
Convener: Pelle Braendgaard
Notes-taker(s): Pelle Braendgaard

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

We talked about the 2 generic DID resolver libraries

- https://github.com/uport-project/did-resolver for JS
- https://github.com/decentralized-identity/universal-resolver for java/docker

Then discussed the did-jwt library which allows you to create standard JWT's and validate them using the did resolver. https://github.com/uport-project/did-jwt

The conversation then morphed into a debate between the current approach to listing public keys https://w3c-ccg.github.io/did-spec/#public-keys and that we could easily use JWK instead.

Quantum Resistant Active Code Signing-Including BlockChain-Final

Wednesday 4I
Convener: David Challener
Notes-taker(s): David Challener

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

The presented paper can be downloaded here: https://drive.google.com/open?id=1MMsUoN-MrPy0vyaVW6bgHrCKGiCzMMPm

Separable Identity and Intersectional Collaboration

Wednesday 4K
Convener: Courtney Brown
Notes-taker(s): Jon Pincus

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

Key points

The identity you choose to engage with informs my expectations of your actions.

The identity I choose to reveal informs the interaction with community that I seek.

For the communities we work with, it's closer to the model of reality. Today, people use four different browsers to accomplish this. It comes down to, do we trust communities and the people in them? "I think the answer is obviously yes."

Detailed notes:

Separable Identities - facets of identity, alter egos, personas. A multi-person may identify as black. We're not just one thing, systems push you into categories.

TWTTR: Twitter is a high-capacity commons, what we have is singletons (people) showing up as part of a thundering herd - #MeToo, #IStandWithEmma.

Who's showing up, how do the represent, how do we use that to further the dialog?

CNTTR -(lCounter): each person who shows up shows their representation with verifiable claims as part of the communities they're representing (in whole and in part) - different parts of the thundering herd. We have the opportunity to get rough metrics across communities and demographic populations. Another way to guide policy. If these are verifiable claims, have verifiable counts - gets around problems about undercounting as method of oppression.

[Who verifies the claims? The authoritative group … but who's that? One of the problems Occupy had was there were no leaders, Still, verifiable claims of representation are valuable even if they don't solve all the problems.]

Next step: if there's a specific call to action, somebody representing multiple constituencies opens up possibility of the intersectional calls to action.

Maps to governance forms like First Nations, where the tribe designates who's part of it, and who's representing them.

Audience: this opens up self-assertion as well. "Identifying with BLM", can be self-identify. At Web of Trust last month, guy from IBM was talking about micro-credentials, just for showing up at an event.

Audience: a person's identity is composite. Communities, similarly.

Authority to speak for the community needs to come from the community - compare MLK with Ben Carson.

Intentionally steering clear of the R word - not talking about reputation!

Distributing the capacity for rough consensus of outside observers.

Identities are fluid and change over time. Some identities are dangerous to present. How to deal with that? Are there problems of tokenization? Can someone pass? Camouflage is useful. Perhaps a claim that you're "just a person". Which envelope do you send your response in.

The identity you choose to engage with informs my expectations of your actions.

The identity I choose to reveal informs the interaction with community that I seek.

Audience: have we talked about separable identities and safety in the real world? Not explicitly. Many times as a female it's unsafe to reveal that I'm a female in the internet world … then again there are places I can only be involved in as a female. Or political views.

Changing language to "verifiable credentials".

The basis of identity in this society is you emerging from your mothers' birth canal. With community, it's harder - community has to approve.

NameTag has some similar ideas (although yet the credentials).

ProFinder is a network like LinkedIn that does web crawling

There's a certain amount of squishiness - it's a human matter, rough consensus. Can't avoid the squishiness.

It's all about trust: what you choose to reveal about your identity is all about much you trust them. "Trusted oracles" and larger questions about delegations of community knowledge.

What are the risks of moving to this model? Need to do A/B comparison via TWTTR.

Camouflage is an acceptable identity.

Suggestion for next steps: building use case models.

For the communities we work with, it's closer to the model of reality. Today, people use four different browsers to accomplish this. It comes down to, do we trust communities and the people in them? "I think the answer is obviously yes."

Do-It-Yourself password free! – Cryptographic Authentication for Web Apps

Wednesday 4M
Convener: Francisco Corella, Karen Lewinson
Notes-taker(s): Francisco Corella

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

The session was a continuation of a demo.

During the session and demo we demonstrated how easy it is to implement cryptographic authentication for web apps using the Pomcor JavaScript Cryptographic Library (PJCL). The library can be used client-side and, if the web app is a Node.js app, server-side, which is convenient for full-stack development.

We played with a sample app, distributed flyers summarizing the registration and login flows, and went over portions of the code. The flyers and the code of the sample app can be found online at https://pomcor.com/pjcl/ .

Secure Elements DICE and TPM

Wednesday 1I
Convener: Alan Viars
Notes-taker(s): Alan Viard

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps: Trebuchet 11

TPM 2.0 Notes

Level Setting: What is a TPM?
A Security Co-Processor
- Public Private Key Operations
  - Key Creation
  - Key signing
  - Key exchange
- Non-Volatile Storage
  - Access protected
- Symmetric encryption
  - HMAC operations
  - Limited symmetric encryption

Purely Passive
    It does NOT monitor your system

Level Setting: What is a TPM?
Two Questions
Why was the Specification upgraded from 1.2?
    Over 1 Billion served

Why do I care?
    How can I make use of TPMs to solve my current problems?
Why the Change from 1.2?
Security
    TPM 1.2 was built around SHA-1
        The algorithm was embedded in all structures
        There wasn't room enough to simply change to SHA256

Complexity
    TPM 1.2 had grown "organically" after 1.1b
    It was unnecessarily complicated

Ease of use
    TPM 1.2 was hard to use
    Complexity of authorization

New Functionality
    Algorithm flexibility
    Unified Authorization
    Fast Key loading

Why Use a TPM 2.0?
Problems that can be solved/ameliorated with TPMs
    Poor entropy leading to weak keys
    Supply chain risks / Counterfeit hardware
    Keeping bad guys off of your internal network
    Keeping malware infected hardware off of your internal network
    Massive password database releases
    Multi-factor authentication
    Email Security
    FIPS certified / Common criteria certified encryption engines
    Securing your root certificates
    Merging physical and logical controls

For more information:
https://www.apress.com/us/book/9781430265832
(Free download)

For more information
Dice: https://trustedcomputinggroup.org/winbond-introduces-trustmetm-secure-flash-memory-implementing-trusted-computing-group-tcg-device-identifier-composition-engine-dice-architectu

Communications Words Storytelling For Humans

Wednesday 5D
Convener: John Philpin
Notes-taker(s): John Philpin

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

Link to the PDF notes:

https://www.dropbox.com/sh/rtqa5y3ua9viq1b/AAAynOsaTbk00fk4EJ1j6dlVa?dl=0

GDPR AEORR (Access, Erasure, Objection, Restriction, Rectification)

Wednesday 5E
Convener: Doc Searls, Dazza Greenwood
Notes-taker(s): Scott Mace

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

Elizabeth R.: GDPR and EPR directives were meant to govern privacy offline and online. Still some derivations by member state. But GDPR was to create uniformity. First draft of GDPR was 2011. Think about how significantly things have changed since then. GDPR in some ways is kind of obsolete. Technology that is so dated. But it is what it is. The E-Privacy Regulation is still in draft. Probably will become law in about 2 years. Super interesting. Even though offline and online difference is eroding, EPR governs machine to machine communications. EPR could in a couple of years have more impact. GDPR still requires some sort of human nexus. EPR for those of us who work with blockchain. GPDR focuses on personal data. EPR focuses on metadata. The drafts get leaked and circulated to some key stakeholders. By the time it goes public it's been doctored and altered. All that is the landscape. Caution to think about the GDPR in that context. We identified data subject, data controller, data processor, 3 key parties. There is such disruptive tech already that challenges the fundamental model set up in GDPR, not only challenges but is inherently inconsistent. Data subject is problem number one. The classification of these roles is inherently flawed. Thinking about self-sovereign identity, how do we govern? I am the identity owner, the data controller, I craft my terms and conditions. That would be a truly self-sovereign identity. But if you think about how hard that would be to implement commercially, every business would have to intermediate all these terms and conditions for every individual. Concessions to be made to have a functional society. There is a tension there. SSI Big Tech initiative launched today. How do we architect that.

Doc: Context. On May 25, if Wendell's right, all of a sudden if you're in Europe, there's a new front door to every Web site to require a new pile of consents for individuals. The self-sovereign minded, the individual will do something autonomous. For Oath and other companies in the traditional ad tech business, how do we keep it going. I have a feeling that in the same way that Y2K was like a small thing a big deal was made of, GDPR may be a big thing that little is made of.

Elizabeth: The establishment test is broad. The activities test is also extremely broad. The biggest difference is the reach is significantly broader. We're overemphasizing consent. It's really not true. It's super watered-down. Another prong, the legitimate basis test. Some things will require expressed consent. Does this thing have any teeth? Most violations are 2% of annual gross revenue, per violation. Some are 4%. In reality, there's no way the regulators in the EU are going to disrupt the global economy with their enforcement. It will be the obvious people, Facebook and Google, and smaller bad actors. We're overemphasizing some things and underemphasizing others.

Paul Knowles: In Europe if you are negligent about GDPR they'll come down on you. If you're thinking about data protection, they will embrace that.

Elizabeth: Totally true.

Dazza: Access: Tech capabilities: Get/post, email, FTP.

Elizabeth: Design "patterns" (components): Workflow – request, identify and allow for authentication and authorization (i.e. OAuth2), delivery

Dazza: SSI?

Elizabeth: We're moving away from triparty model. If you have SSI, you don't need this, ultimately.

Dazza: Perhaps. In the SSI world being envisioned, we only control our identity and personal data and there will be things outside the boundary condition, like government agencies, who also have our personal data. Legal regimes give us access rights to it. And also an endpoint they can deliver it to.

Wendell: Why does logging into a Wordpress site not totally solve this problem? Small publisher comment site. Use existing account.

Q: Account system.

Yogi: That's just a simple case. CRM systems beyond simple WordPress sites. Like a clear button. A registry service.

Elizabeth: This is where the EPR comes into play. Some of these rights will be mediated through the machine to machine communications.

Bryan Pon: What is the overlap between GDPR and EPR?

Elizabeth: They're meant to be complementary.

Doc: A practical question. My blog is a Harvard blog. If I hear Wendell right, it is incumbent on Harvard to put up that door saying you need to consent...because of GDPR. Do they need to do that, and what is it going to say on there? Most people reading it have never logged in and made a comment. Are they going to have to register to read it?

Elizabeth: No. Everything here is designed to be proportional to its use. Reasonable means.

Doc: They're running between 4-6 trackers, Google Analytics, Quantcast etc.

Elizabeth: That's EPR. Way beyond cookies. That will be regulated. A good example of how the two would work together. The GDPR would be the dominant regulation. The EPR would be there in the background.

Doc: What are these entities (Harvard, LJ) going to do? If you run a log file you're going to have to put up a warning page?

Wendell: Generally. It is data about a person with their identity in these log files. Part of the analysis is, what are you logging, how long are you keeping it, what's the purpose. Many other business processes you want to do often entail building more stuff. Given you can boil down what you need for a simple entertainment site, what would you have to build. The example we used was WordPress. Set of logins, tracking users and comments over time. You would have to provide these facilities to all the data subjects because we have their data.

Dazza: Postulate LJ and GDPR regulation. Stretch goal, say person can actually deploy a term on which consent is contingent: "Only show me ads that comply with Do Not Track."

Wendell: All the login preferences, size preferences, package up in a tarball zip file.

Doc: That's a different request. Is that a SAR?

Wendell: A subject access request.

Doc: The scenario I laid out, a reader says show me ads not based on tracking.

Wendell: Say you don't have a paywall. You have to go by consent. A dialog, check box. Serving ads without tracking. Not allowing free form terms, exotic permissions.

Doc: You're saying give me a cookie that says consent.

Wendell: They'll record that choice.

Doc: A regime you worked out?

Wendell: Indeed. IAB, 6 bit-ish, Oath 9 bit-ish. You can revoke core consent, you may not have my data at all. These are obligations you have for holding data.

Yogi: My worry here is we are overemphasizing consent. If you have legitimate interest you are not obligated to these terms.

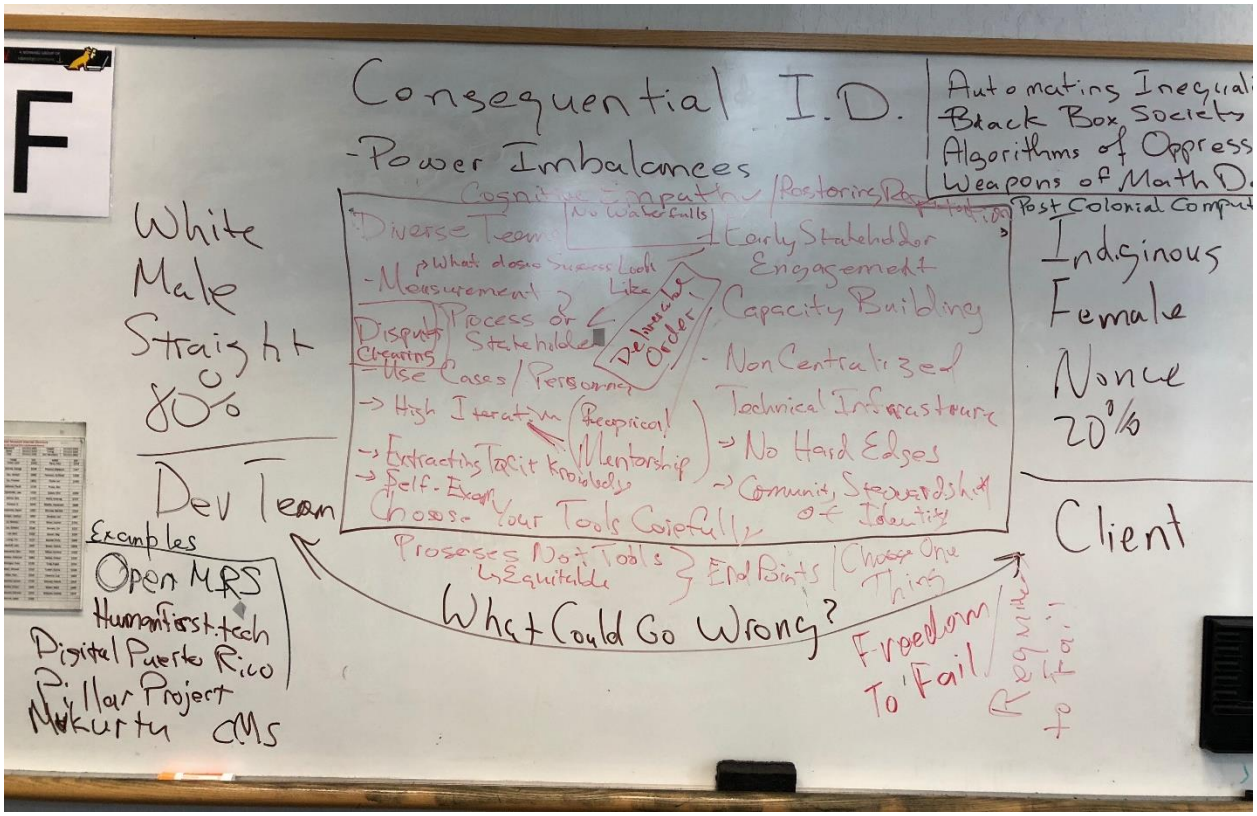
Doc: We're looking at GDPR as a forcing function.

Elizabeth: You shouldn't rely on consent. It's extremely hard to implement and to prove.

Consequential I.D. – How Not To Reinforce Power Imbalances in the Systems You Implement

Wednesday 5F
Convener: John Wunderlich
Notes-taker(s): John Wunderlich

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



Phone # Global Identifier

Wednesday 5G
Convener: Dick Hardt
Notes-taker(s): Dick Hardt

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

While there are lots of problems with using a phone number, it is the best option of the options (email, phone) that are globally known and available today

ORCID: What Should It Be Considering?

Wednesday 5H
Convener: Laura Paglione
Notes-taker(s): Laura Paglione

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

201804 IIW session presentation. ORCID. Presentation.
https://doi.org/10.23640/07243.6089834.v1

Veres One (DID Ledger) Deep Dive

Wednesday 5I
Convener: Manu Sporny
Notes-taker(s): Many Sporny

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

Slides:
https://drive.google.com/open?id=1bUZbtgdxKxTR1it10G9ZozYGD486qxZTBPuiOZjzoT4

Veres One[edit]
- A Globally Interoperable Blockchain for Identity
- IIW XXVI - April 3rd-5th 2018

Vision[edit]
A world where people and organizations create, own, and control their identifiers and their identity data

Fit for Purpose[edit]
- Veres One is a fit-for-purpose blockchain optimized for identity.
- It is public and permissionless

Veres One is FAST[edit]
- Fastest DID Ledger
- DID Creation
- Bitcoin - create: 0.6M / day - consensus delay: ~3,600 seconds
- Ethereum - create: 2.1M / day - consensus delay: ~375 seconds
- Veres One- create: 18M / day - consensus delay: ~30 seconds

Did NOT do an ICO[edit]

- Veres One does not use a token and will not do an Initial Coin Offering (ICO).
- ICOs Create Volatility and Network Debt

Veres One is Cost Effective[edit]

- Bitcoin - ~$15-$73 per DID
- Ethereum - ~$4-$14 per DID
- Veres One - ~$1-$2 per DID
- Fee-based revenue models ensure long term operation of the network
- Commodity prices guaranteed due to strong downward pressure on operational costs

Ecosystem[edit]

- Veres One Project
  - Houses Board of Governors
- Maintainer
  - Ensures technical operation of the Network and implements new features.
- Community
  - Advises Board of Governors, which ensures proper execution of the mission.
- Accelerators
  - Can quickly create identifiers on the Veres One Blockchain.
- Nodes
  - Provide compute and storage resources that keep the Network secure.

Veres One Project[edit]

- Board of Governors
- Votes on consensus positions of community, has limited Emergency privileges, and can be replaced by community.
- Debates changes to network and pricing until a proposal is formed with no principled objections.
- Funds distribution is determined by the Community and Governors and set based on Network needs.

Funds Distribution[edit]

- Pie Chart (see slide deck)

Roadmap[edit]

Beta (Oct 2017) Release Candidate (Feb 2018-today) Production (June 2018) Production Customers (Oct 2018)

Questions[edit]

- Any questions related to Veres One or the larger ecosystem?
- Manu Sporny | CEO | Digital Bazaar
- Co-Inventor of Verifiable Credential & Decentralized Identifier Technology
- Co-Inventor of JSON-LD
- Co-Founder of Veres One
- 10+ Years in Web Standards

- Customers in Finance, Government, Education, and Healthcare
- Email: msporny@digitalbazaar.com
- Twitter: @manusporny
- https://www.linkedin.com/in/manusporny/

Open ID v. FIDO v. SSI

Wednesday 5J
Convener: Mike Schwartz
Notes-taker(s): Mike Schwartz

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

Mike Schwartz from Gluu posits that there is surprisingly little overlap between SSI, FIDO and OAuth. Futhermore, he suggested that SSI is some kind of "next evolutionary step" is detrimental to the adoption of SSI.

We reviewed the OpenID, FIDO, and Self-Sovereign identity diagrams in this folder: https://gluu.co/know-git

SSI promises some potentially great innovations:
1. Not controlled by a domain (user can't be held hostage)
2. Not reliant on TLS as the encryption mechanism

Use cases showing where SSI and OAuth can work together would be helpful. Gluu has some interesting use cases for SSI where verifiable claims can be sent as a pushed UMA claim token for the purpose of API access management. SSI is really interesting because it might provide a attractive publication mechanism for information not traditionally sent via identity assertions like an id_token or SAML assertion.

Another use case mentioned by Jack from Veridium was Blockstack's use of dropbox (which uses oauth to protect access to its resources) to publish data under the user's control, referenced on the bitcoin blockchain.

Mike is working on a blog called "SSI versus SSO" which will be published on https://gluu.org/blogs sometime after IIW, that summarizes many of the points.

Follow-up Blog Post : "SSO v. SSI" https://www.gluu.org/blog/sso-v-ssi/

TLS Flex Expanded Library Support For Alternate Certificate Sources

Wednesday 5L
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:

We worked on the paper draft, and talked with a few folks about our work and got some feedback on the title.

An earlier draft can be found at the RWOT repo:
https://github.com/WebOfTrustInfo/rebooting-the-web-of-trust-spring2018/blob/master/draft-documents/TLS-Flex.md

How Do You Make Money in the Sovrin Ecosystem?

Wednesday 5M
Convener: Richard Esplin
Notes-taker(s): Richard Esplin

Tags for the session - technology discussed/ideas considered:
Sovrin, Business Model

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

Business models:
* Provide a wallet specific to a certain demographic
* Provide a wallet to organizations that scales to large numbers of connections
* Auction network connecting potential buyers and sellers
* Exchange of claims--provide claims for a fee
* Provide services to bring people on to the network: give IDs to schools
* Provide a SaaS service for hosting wallets of claims (like Coinbase in the Bitcoin ecosystem)
* Domain specific identity solutions (Schools, daycares)
* Sell SDKs that provide additional capabilities to solutions in the ecosystem
* Issue a coin for the additional capabilities provided in the ecosystem
* Provide consulting for organizations that are adopting solutions in the ecosystem

Concerns:
* Sovrin Coin Offering:
-- "Cheapens what we are doing"
-- "Coin offerings are a scam"
-- "Why don't just pay for transactions with USD?"
* But it is also a challenge that there is no layer 2 token for Sovrin. It will be hard to attract developers until there is a direct way to monetize the ecosystem.
* How are Stewards rewarded for their contributions to Sovrin?

Thursday April 5

Zero-Knowledge Prof's 101 ENCORE – Only High School Math

Thursday 1F
Convener: Kazue Sako
Notes-taker(s): Christian Lundkvist

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

Suppose we have publicly known integers g, p, where p is large(~ 2^256), g < p. (p is often a prime)

Define f(x) = g^x mod p

We use the fact that given f(x) it is computationally infeasible to compute x ("Discrete logarithm problem")

For modular arithmetic (i.e. the "mod p" above),
see https://en.wikipedia.org/wiki/Modular_arithmetic

(All operations are modulo p here)

Alice gives y = f(x) to Bob, he holds on to y. Alice has the secret number x and wants to prove to Bob that she knows x such that y = f(x) without revealing x.

Alice can prove to Bob that she knows x through the following protocol: Alice creates random number r

Alice gives u = g^r mod p to Bob Bob sends a random number e \in {0, 1} to Alice

If e=0 Alice defines v = u

If e=1 Alice defines v = g^(r+x) mod p

Alice sends v to Bob

Bob verifies by checking:

if e=0 check that v = u

if e=1 check that v = u * y (=u * f(x) = g^r * g^x = g^(r+x))

If Alice knows x she can always give the right response v. If Alice doesn't know x she has probability 1/2 of giving the correct value (if Bob sends e=0).

Now if we do this 10 times the probability of Alice sends the right thing without knowing x is 1/2^10 (around 1 in a million). Why is the choice e=0 relevant (it's unrelated to x)?

Suppose Bob always gives e=1 and Alice knows this. She can then cheat by providing

u = g^r / y mod p

to Bob, and when Bob sends e=1 Alice can respond by sending v = g^r mod p. Bob will compute u * y = g^r/y * y = g^r mod p = v so Bob's check will always succeed even though Alice didn't know x. This is why Bob needs to also send e=0.

Generalize a bit:

Alice generates r, defines u = g^r mod p, send u to Bob

Bob sends e, Alice sends back v = g^(r + e*x) mod p Bob verifies by checking that v = u * y^e (same as above in the case e \in {0,1})

Now, instead of e \in {0, 1}, let e be a random number in the interval [0, p-1] and do the same thing:

Alice generates r, defines u = g^r mod p, send u to Bob

Bob sends e, Alice sends back v = g^(r + e*x) mod p Bob verifies by checking that v = u * y^e

Now you only have to do one step in the interactive proof, and the probability of Alice generating a successful number v without knowing x is around 1/2^256

This is still an interactive proof, can we make the proof non-interactive?

Instead of Bob randomly choosing e, we can automatically generate a "random" response value e by hashing u:

e = Hash(u)

Now Alice can create a non-interactive zk-proof v:

Randomly generate r Define u = g^r mod p define e = Hash(u) v = g^(r + e * x) mod p Bob verifies the proof by checking that: v = u * y^e

If we only do this an attacker can replay Alices proof u, so Alice could add something like a nonce value to e, i.e. use e = Hash(u || nonce)) where || means concatenation of byte strings. This way you can protect against replay attacks.

We now see that at this point we've actually designed a general signature scheme, by using an arbitrary message instead of the nonce above. This signature scheme would be defined as follows: Alice has a private key x, and generates a public key y = f(x) = g^y mod p.

To sign a message M with the private key x Alice does Randomly generate r Define u = g^r mod p define e = Hash(u || M) v = g^(r + e * x) mod p

The signature is defined as the pair (u, v).

To verify the signature on M using Alice's public key y Bob computes e = Hash(u || M) and checks that v = u * y^e. This is very close to the Schnorr signature scheme: https://en.wikipedia.org/wiki/Schnorr_signature

Also instead of using modular arithmetic directly we often use more specific group arithmetic (such as elliptic curve arithmetic in elliptic curve cryptography).

User-Controlled GDPR Consent Cookies

Thursday 1G
Convener: Andrew Hughes + Doc
Notes-taker(s): Andrew Hughes + Doc

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

Andrew H. @Idamandrew

When the ad spaces go out to auction, the ad buyers are bidding, and publishing networks are active, they will be able to read users consents recorded in the IAB cookie and do fulfillments according to the instructions. These cookies will be passed down the chain as far as they need to go. 24 bits per site to encode the company.

Iain: They don't want to expose the 300 entities on the list.

Andrew: Talks about what might go in the dialog boxes. The ad buyers will create a new domain with subdomains. We should hack it as hard as possible. Opening gambit. What if we have some sort of privacy/cookie/consent manager – privacy dashboard – a script or browser plug-in which lets me write these cookies. We'll know the encoding. We can flip the bits.

Q: It's your browser.

Q: Depending on what they dictate, if it's HTTP only, it won't be accessible to Javascript – except as an add-on.

Q: It's just like Grease Monkey.

Q: Ad blockers will be able to identify which domains serve this.

Q: If you have this cookie already, the gauntlet won't happen. The cookie has an identifier that will correlate across sites. Jenny identifier would make everyone show up as the same person. Phone companies stopped issuing this phone number. Any grocery store, key in 867-5309. Known as the Jenny discount. We have the opportunity to get the Jenny discount.

Doc: We could go to the EFF, Privacy Badger, they would be glad to. We need tracking protection to jump out behind the perception as ad blocking. It one ups the awful system Ad Block Plus has, a complex system Google pays us to pass through their stuff alone.

Joe Andrieu: We're creating an auto-consent, which is undoing GDPR.

Doc: Does this mess with the GDPR in some way, the letter or the spirit? Does this have a simple order that still permits through other forms of advertising? Wendell said one of those six things says this person wants DNT as it was originally intended. But I don't know.

Joe: What will publishers do when you say no?

Andrew: Wendell does not speak for the IAB. No one knows what's going to happen. Every European Web site had a popup for cookies.

Doc: If we do this right, the incentive alignment that works for the publishers, who jobbed out income production to ad tech ecosystem, Google said to publishers you're on your own. The incentive for publishers is you can still have advertising provided no tracking.

Andrew: If you do not consent, you have to have an equivalent experience. So it won't be like a black screen in most cases.

Adrian Gropper: Another dimension, to the extent GDPR forces them to be more transparent to what happens down the chain, we want to collect this information and make it useful in some way. We should as the spec comes out try to leverage the transparency component to either make it easier to score Web site practices or to identify particularly egregious things going on the chain. Things none of the ad blockers are doing. Privacy Badger is inscrutable. I'm tempted not to change the sliders.

Doc: If we do this in a clear enough way, I can go to Berkman and ask for research to follow up on this.

Andrew: Presumably you can read these cookies and start doing analysis on them.

Q: If the browser can't send a cookie down, the spec says if not one from browser, they make up "no cookie" signal

Doc: The original purpose of the cookie taken off? A negative thing for a lot of users. We need to throw some conditionality in there.

Sam: The tool just saying no all the time may not be in the best interest of the user.

Doc: Does the first party only condition apply here and solve the remember my state problem.

Q: You could say I will allow you to store a cookie but no tracking, analytics. First party ads only.

Conditionality in the privacy manager, give them the cookie that allows storing cookies only for first parties and no to all third parties coming to the page.

Doc: Puts publisher interest in alignment with ours. Takes the third party ad tech system off the table.

Q: Every time I go to a new publisher, am I going to see this splash screen.

Andrew: That's why the starting premise is modification rather than blocking.

Q: Say it gets done through Privacy Badger. If it's big enough, this system will go away.

Doc: It's not that big, but it could be big if we play it right. Infinite amount of fear on the part of publishers.

Q: If we can convince U Block.

Q: Has Ghostery gone to the dark side?

Doc: Gone to the light side.

Andrew: This is a moving target. I'm sure they're working on something past day one that will work properly.

Q: How to use verifiable credential to transmit my terms to each Web site.

Sam: You're preemptively giving them version 2.

Nathan George: I don't have to interact with the Web site to say my permission has ended. When I revoke, I want all third party stuff to stop tracking me.

Q: Give them a better solution that is user centric. Not only do you get veriability--

Jlinc Q: A lot of people between the person paying for the ad and a customer. You're disintermediating the ad industry. It's a good result.

Andrew: Given what they understand, the industry knows users will not want to participate...the question is how do we get a plausible list of carrots to them?

Doc: To publishers the carrot is you still get to advertising, and sponsorships. You can't get sponsorship with ad tech, which is just chasing eyeballs. So sponsorship comes back and a working ad model. And branding can happen again. A trillion dollars has been spent on ad tech without creating a single brand.

Q: It automates compliance and has tamper-proof storage of consent receipt. Reduces risk on ad tech side. We have these verifiable credentials from the user. It's mitigation of risk on their part.

Doc: Risk mitigation for publishers and advertisers for GDPR compliance. Addresses spirit if not the letter of GDPR. For the IAB, you still get to be interactive and programmatic. You just don't get to track. You move into intentcasting, customer-qualified leads.

Sam: Annoying to them, if I go buy a widget from Amazon, I will get advertised for the next two weeks. I could say I'm interested in headphones, they can act on that with permission.

Doc: The actual problem there is the dishonesty on the part of Amazon is intentional. Headphone maker has given coop money to Amazon, lies about who a qualified lead is. Incentive for Bose is to pull some of the dishonesty out of the system.

Adrian: What's Brave going to do?

Doc: He's adaptable. He needs to be in this conversation.

Q: Need to segment, what some parts of the industry perceive as a carrot others perceive as a threat.

Q; If any one organization steps forward, they'll get crushed. Tell Mozilla to stop ruining the Internet. It was horrible. Leadership walked away from DNT.

Doc: The other browser makers could have stepped up and they didn't. The IAB right now is staggering back from the power of the GDPR. And E Privacy is coming along after that. Even though GDPR is watered down, the spirit is exactly what we're going after here.

Q: How set is the format of that cookie?

Andrew: It's a spec right now.

Q: Could it go to a macaroon? They could change it in the future.

Andrew: If they view this as a threat, they will use countermeasures. We need to help them find version 2.

Q: If you move in this direction, we can automate GDPR for you.

Doc: Risk is always on the table, especially here. They're thinking which awful tradeoff? Put intentcasting back on the table. That's good for advertisers and to a lesser degree publishers.

W3C Q: Once you start getting verifiable claims and blockchain on the table, advertisers are worried about ad fraud. Replacing with something blockchain based has exciting possibilities. Reducing possibility of the site being hacked. Also you can fulfill ads faster. You don't have to do an HTTP request. You have a local cache of it. You can save a number of milliseconds for every ad.

Q: Ad block speeds up your experience on the Web.

Doc: It's not that programmatic goes away. Tracking does. Throw intentcasting in there, can be communicated faster.

Q: How do you build an onboarding process that isn't a PITA. Need a UX/design team.

Q: Let's call Mozilla. They have a whole team studying this for many years. Reams of information on UX on consent and interaction. Interact with the browser vendors.

Doc: Who's on board for making this happen and how do we do it? W3C, Mozilla. I can host a list at Project VRM. Linux. Take the energy in this room to hack this thing.

Q: Kantara has been thinking about this. We can do mailing lists, working groups. Hyperledger.

Joe: If we want the browser vendors involved, W3C. A long process, challenge. I chair the credentials community group.

Q: I can offer setting up infrastructure this afternoon. We need the air cover a standards body can provide.

Q: IEEE Privacy Engineering Steering Group.

Doc: Making by the 25th a plug in or add on involving any of these. EFF Privacy Manager?

Dave Crocker: You dont want that many groups. Start with a targeted set to get the initial implementation spec'd and done in 3 weeks.

Sam: First phase is do the cookie hijacking, technically simpler to do. Verifiable claims is longer term.

Adrian: Two aspects to GDPR. Consent/consent receipts/verifiable claims is only half. All the transparency issues built into GDPR compliance have to do with how your privacy information was actually used. Nothing to do with consent. I tend to think Kantara is the place most likely to fit this model. But I don't want to just pay attention to the consent aspects. Unless we can understand who is responsible for reporting, we're not dealing with the GDPR.

Q: We should talk about people.

Q: You need a hit squad to do this in this timeframe. The labeling is so important. Cookie anticipation might be a more affirmative label. Talk to the other folks.

Joe: They're using only 6 bits out of 40 (??). Tell them have a bit for the consent terms you've been talking about. Respend to IAB with specific user-asserted terms of consent.

Doc: Who here is fluent in how to do that?

Sam: A huge business advantage to someone who is already in the business doing it.

Doc: Joe's idea suggests we have a list of who is on board and who/what we need.

Joe: Just respond to the IAB, these are the six terms you should put in that cookie. I can work with you on that. We've got a week to do it.

Q: Quoted from IAB document, page 7. Cookies aren't a long-term solution.

IAB Transparency and Consent Framework.

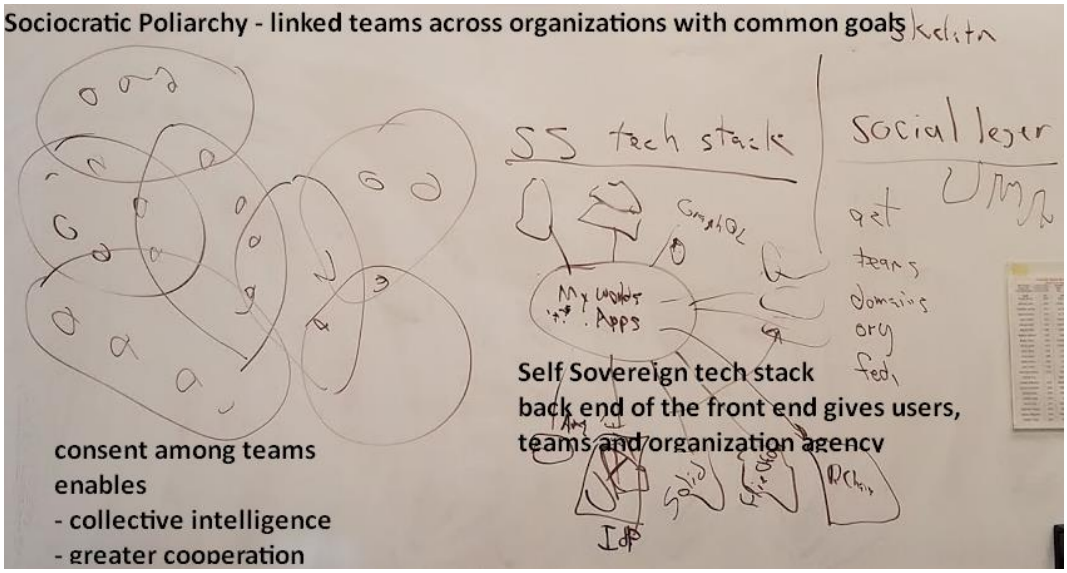
Doc: And a mobile app.

Cooperating Among Communities Owning Interoperable Identities

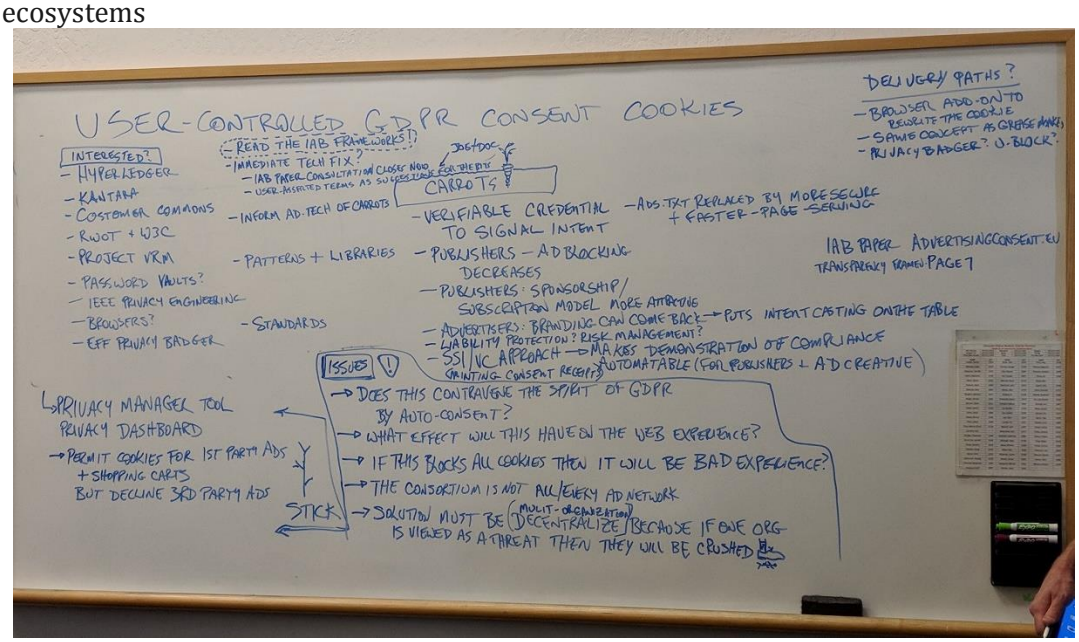
Thursday 1H
Convener: Jim Whitescarver
Notes-taker(s): Jim Whitescarver

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

Our communities want to respect the privacy of members and have a single sign on for all the tools they use. Each member and/or the organization can be onboarded to using tools for self soverency available today.



Potential of a non-profit BYOid cooperative among communities creating trustworthy identities in teams and organizations from the bottom up such that they could be trusted by federations and national identity ecosystems



InSide Out SID's (Standard Immutable Delegation) & Trustless Distributed Computing

Thursday 2A
Convener: Christopher Kula
Notes-taker(s): Christopher Kula

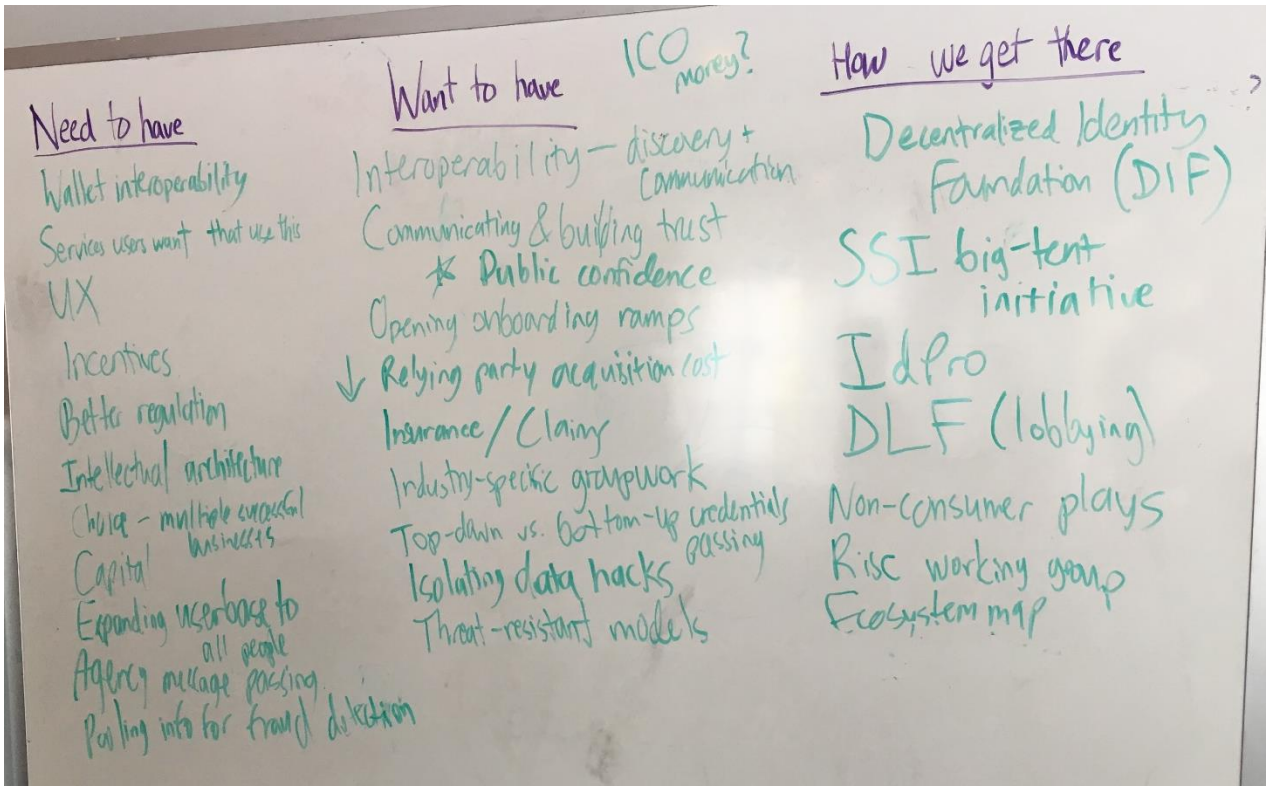
Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

A few ideas were meant to proposed regarding inverting object relationships in consensus systems. Incomplete presentation.

Future of SSI, Tech Scalability and Onboarding Issuers and Identity Owners

Thursday 2C
Convener: Nader Helmy
Notes-taker(s): Nader Helmy

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



REAL Federation – OTTO: API's, Vocabulary, RoadMap

Thursday 2D
Convener: Mike Schwatz
Notes-taker(s): Judith Bush

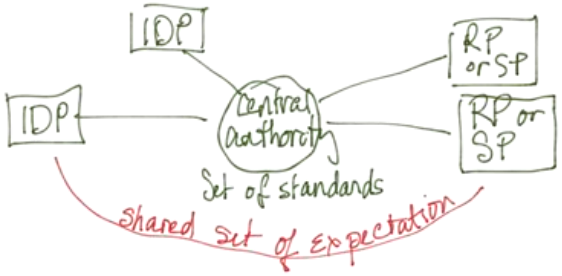
Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

Slides: https://gluu.co/otto-2018

Wed 2D OTTO Mike Schwartz convener Judith Bush notes SLIDES https://gluu.co/otto-2018
OPEN TRUST TAXONOMY for FEDERATION OPERATORS

What is a Federation 101

What is InCommon? Consider this as an example of a typical federation. [See www.incommon.org]
The Federation members all agree to certain terms in the federation agreement. Provides technical and semantic and legal efficiencies. "Tools & Rules to establish trust"



Another example: RADIUS for shared wifi

CONTRAST with "federation" to mean a bilateral SP to IDP configuration.

For federation there is a natural scale of agreement. Easy to come to shared agreements in a vertical.

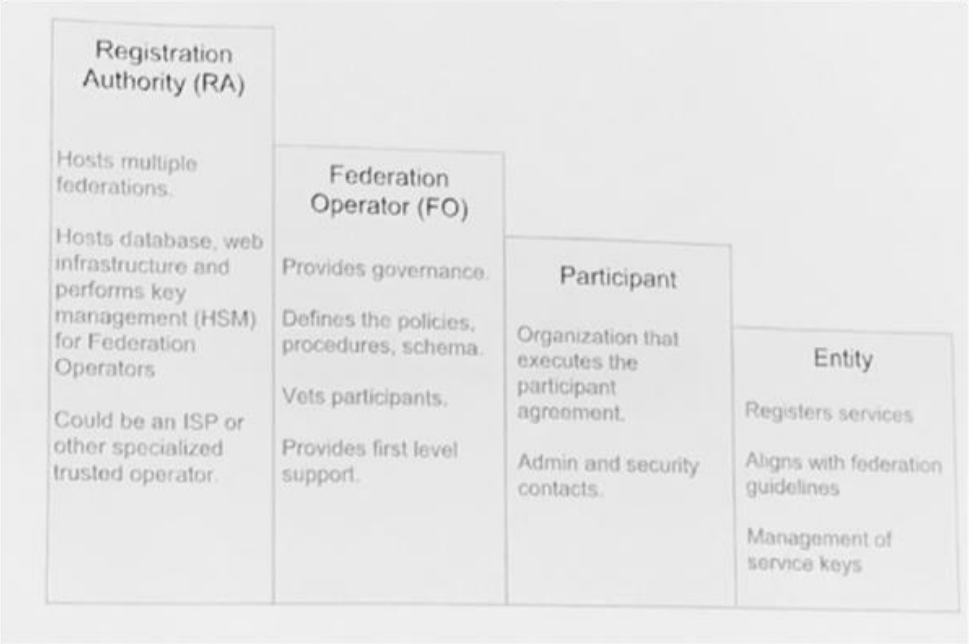
What does OTTO solve

1. Leverage the federation trust model for OAuth protocols
2. Reduce duplication of data during inter-federation
3. Make federation metadata more searchable
4. describe a generic model
5. APIs to standardize entity-to-federation communication
6. Support OpenID & SAML first but leave extensible
7. Simple extensible & open & interoperable

Search by a variety of dimensions not just look up

including the other technical configuration standards defined.

Not just add & modify my meta data.



CRUD APIs for: Configuration
Federation
Participant
Entity
Metadata
Schema

Standards for interop

API standard
https://gluu.co/otto-api
gluu.co/otto-api
Core Vocab
https://gluu.co/otto-vocab

OpenID Vocab
https://gluu.co/otto-openid

SAML Vocab
https://gluu.co/otto-saml

Github Code
https://github.com/GluuFederation/otto-node

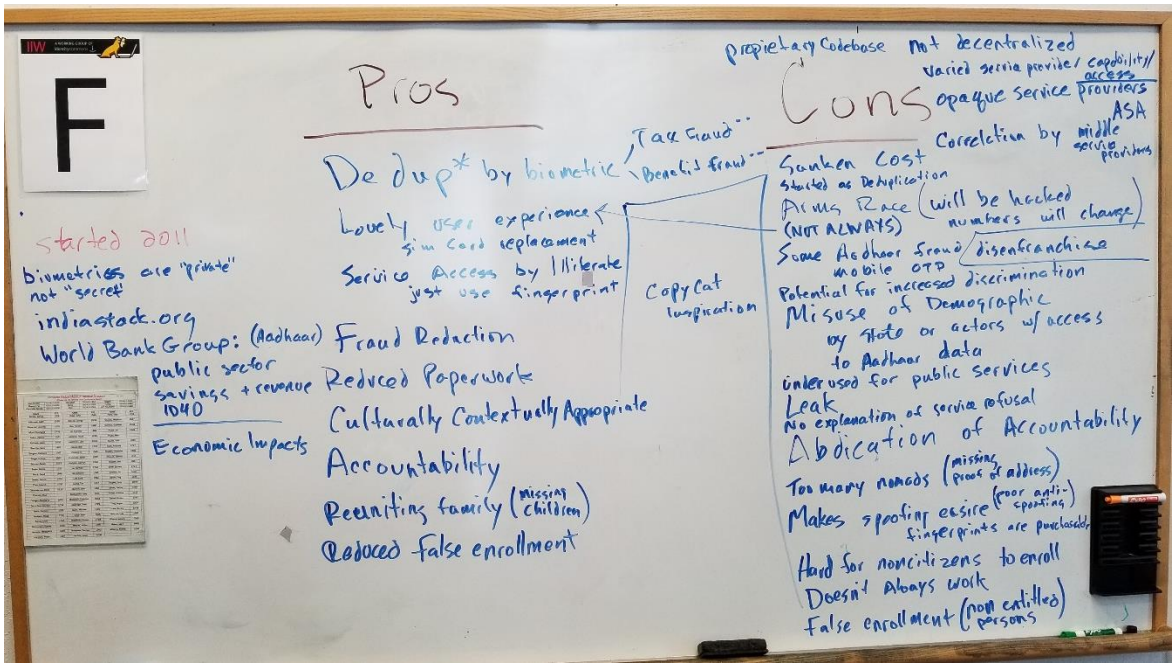
Swagger-UI
http://otto-test.gluu.org/swagger

Slides @
https://gluu.co/otto-2018

Addhaar Pros + Cons

Thursday 2F
Convener: Joe Andrieu
Notes-taker(s): Joe Andrieu

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



Contributing to W3C Standard

Thursday 2G
Convener: Manu Sporny
Notes-taker(s): Dave Sandford

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

Manu started his description of how to contribute to W3C standards by pulling up the github page for the W3C Credentials Community Group: w3c-ccg.github.io

He indicated that it takes on average 6-8 years to get a standard done, so the process is not for the faint of heart. The ideation phase might typically take place prior to initiating activities in W3C in forums like IIW or Rebooting the Web of Trust.

During the "Incubation Phase" parties interested in developing standards will create a W3C Community Group that only requires 3 people and provides web page, email lists, IRC. Members of a community group do not need to be W3C members. Active community groups might have weekly calls, minutes, etc.

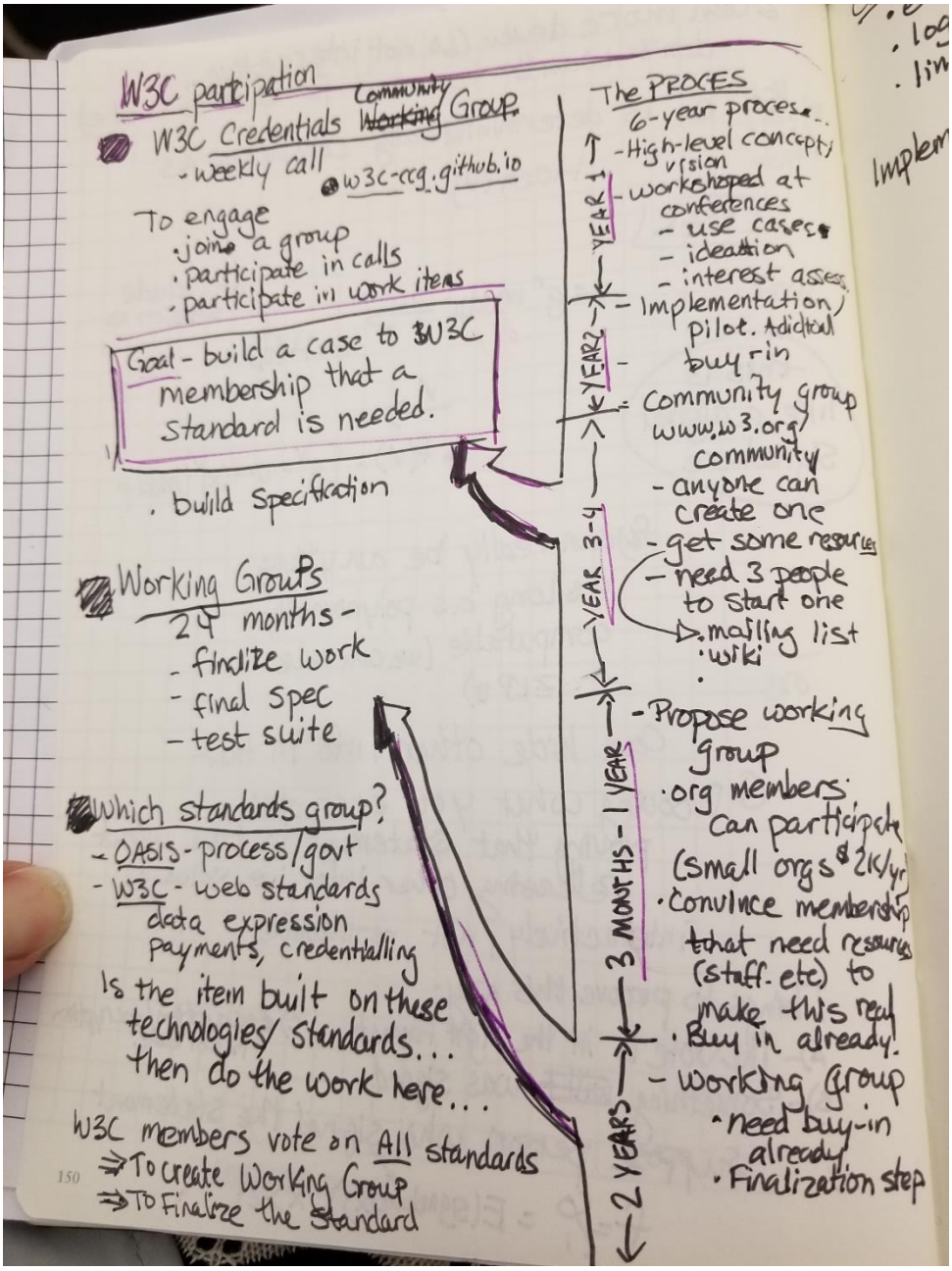
The next phase past the incubation stage, is the creation of a W3C Working Group – to initiate this you should probably already have draft specs and reference implementations – requires participants to be W3C members or 'invited experts'. Only W3C members get a vote – although typically decisions are made by consensus. Votes can be to create a WG, create a standard.

W3C members are organizations. For small organizations, this could be as little as $2K/year. Working group companies must agree not to asset patent or royalty claims on the standards they work on. Once a WG is formed the expectation is that the WG will finish standards, implementation and preliminary deployment in 24 months.

Specifications are always in open github repos and anyone can log an issue. A proposal to change a spec is a pull request.

The next phase past a Working Draft (available for the formation of the WG) is a Candidate Recommendation. For a CR there should be implementation and usually you have to issue a test suite. Typically all substantial (i.e. ones that will affect implementation) issues must be closed.

The next draft is a Proposed Recommendation and this will go to all W3C members for approval. It has a one month waiting period. Finally, a Recommendation is approved by W3C. Beyond W3C Recommendation – often the Recommendation will be submitted to ISO which gives it greater legal standing in some countries.


W3C participation
W3C Credentials Community Group
- weekly call
w3c-ccg.github.io
To engage
· join a group
· participate in calls
· participate in work items
Goal - build a case to W3C membership that a standard is needed.
· build Specification
Working Groups
24 months -
- finalize work
- final spec
- test suite
Which standards group?
- OASIS - process/govt
- W3C - web standards
data expression
payments, credentialling
Is the item built on these technologies/ standards...
then do the work here...
W3C members vote on All standards
⇒ To create Working Group
⇒ To Finalize the Standard
The PROCES
6-year proces...
- High-level concept/ vision
- workshoped at conferences
- use cases
- ideation
- interest asses.
- Implementation/ pilot. Additional buy-in
- Community group
www.w3.org/community
- anyone can create one
- get some resources
- need 3 people to start one
· mailing list
· wiki
- Propose working group
· org members can participate (small orgs $2k/yr
· Convince membership that need resources (staff. etc) to make this real
· Buy in already!
- Working Group
· need buy-in already
· Finalization step
YEAR 1
YEAR 2
YEAR 3-4
3 MONTHS - 1 YEAR
2 YEARS

Comparing Info Without Revealing It

Thursday 2H
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:

Presentation can be accessed here:
https://www.dropbox.com/s/qz7jed7vzaheh4n/Compare.pdf?dl=0

Agent Centric vs Data Centric Reality

Thursday 2I
Convener: Jean Russell
Notes-taker(s): Tom Brown

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

It's about agency, not about data

"How we control the valves is what matters" - Doc

We didn't need a phone until Apple invented it.

We don't have the mother of necessity.

Holo (your perspective) is:
1. DHT – neighbors gossiping
2. bridge to the web

"crypto accounting" is double-entry book keeping
holo fuel (pages for web hosting)

private markets: brave, holo

holochain has no native currency but there is an app called holo with holo tokens
I can give permission to access my data
holobox if you can't/don't want to operate ubuntu for yourself
not trying to perpetuate anonymity. Transparent by default

not a permissioned system. Need to have the hash of the chain you wish to accesss. Shared secrets.

User driven may have been a better phrase than user-centric

we're compromised because of dependency on central services like google

All good libertarians are dependent on the world around them

Google Maps (on mobile) transformed maps into agent-centric as it put us at the center of the map.

Traffic data includes everyone's data

We outsource expertise.

Massachusetts has a right to repair law (You can get Tesla data)

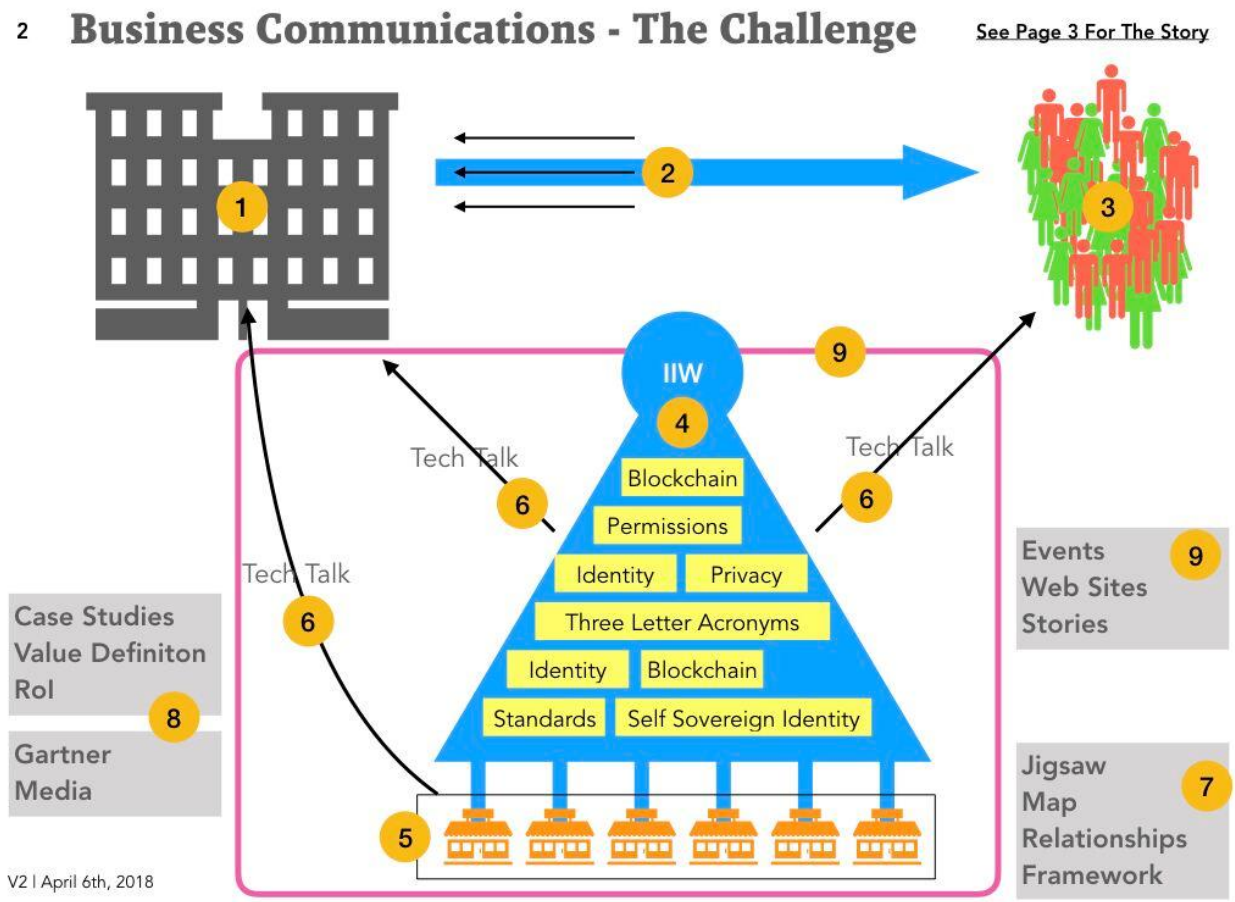
Alexa, Siri are cute at first.

The good parasite doesn't kill the host too soon

Digital Puerto Rico (Tu 4C – We 2L – Th 2J)

Tuesday 4C, Wednesday 2L & Thursday 2J
Convener: John Philpin, Mei Lin Fung
Notes-taker(s): John Philpin

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

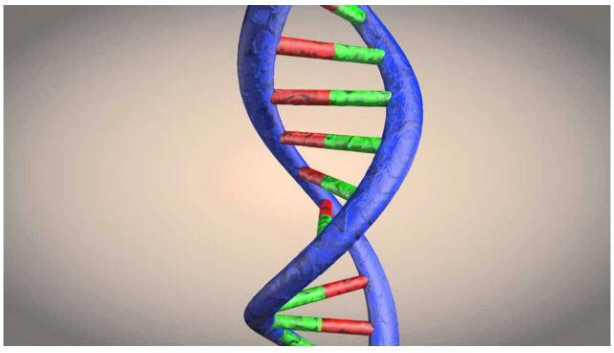


3 Explanation To Diagram

- Businesses (1) are already talking (2) to customers (3)
  - sometimes they even listen (3) to customers
- IIW (4) has and continues to create an amazing community to technical experts (individually and as part of companies (5) to come together and share ideas, thinking and solutions
- The conversations (6) with the businesses are going well - but they are likely to be with people in the business that understand the language being spoken. That is not typically sales people, marketing people, CXOs - but those are the people that really own the budgets and are the decision makers to deliver enterprise wide change.
- Those people need to be spoken to in terms that they understand.
  - (7) How does all of this fit together
  - (8) what is the business argument for doing this
  - (9) where can they go to learn more, converse with their peers
- Like wise - 'main street' - the very community of people (3) we espouse to represent really have no idea what is going on - and arguably have no interest - witness the majority section and treat meant of passwords, facebook, privacy et al.
- The opportunity is to create a business oriented focus group that can help provide 'translation services'. materials, frameworks etc that can be used by the community and for the community - and individual companies as well - of course think of this as a layer (9) that surrounds the core IIW that is business friendly.

V2 | April 6th, 2018

4 Idea - John Wunderlich - Use The Double Helix?



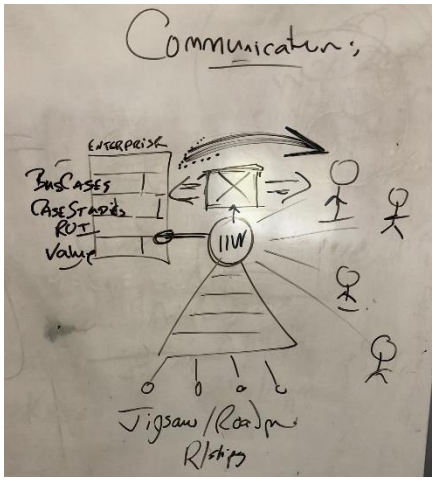
To Be Developed

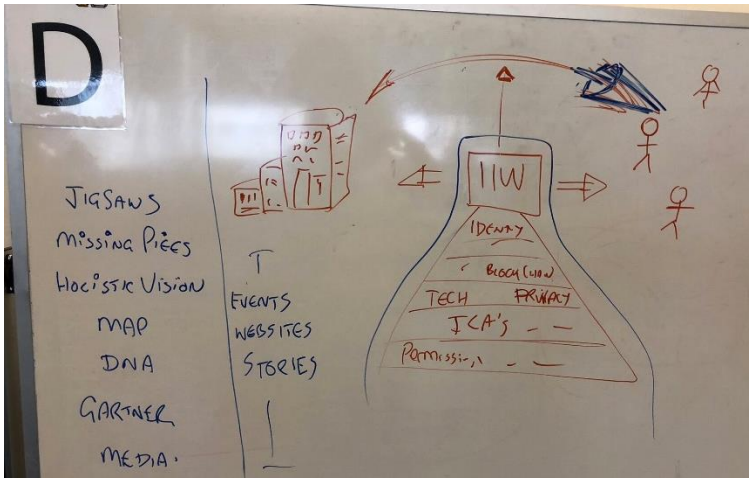
V2 | April 6th, 2018

5 Next Steps

- Convene an interested subset of people who want to take this on with me - maybe introduce others in their company who would sign on
- Begin to develop a business oriented community
  - **within?**
  - **in parallel?**
  - **outside of?** the IIW tech community
- The community will kick off through phone calls and online engagement
  - Slack is one way to do this - but also Kaliya and I talked t the end of the conference - and I have an idea ...
- Ultimately create a dialogue that is aimed at business that can compete with other business conferences like MarTec (to pick one !)
- Initial target is that at the next conference we would have two or three business specific sessions that start to consolidate the consensus amongst the IIW. We would also be looking to invite people to the conference - from businesses that would ot normally come.

V2 | April 6th, 2018

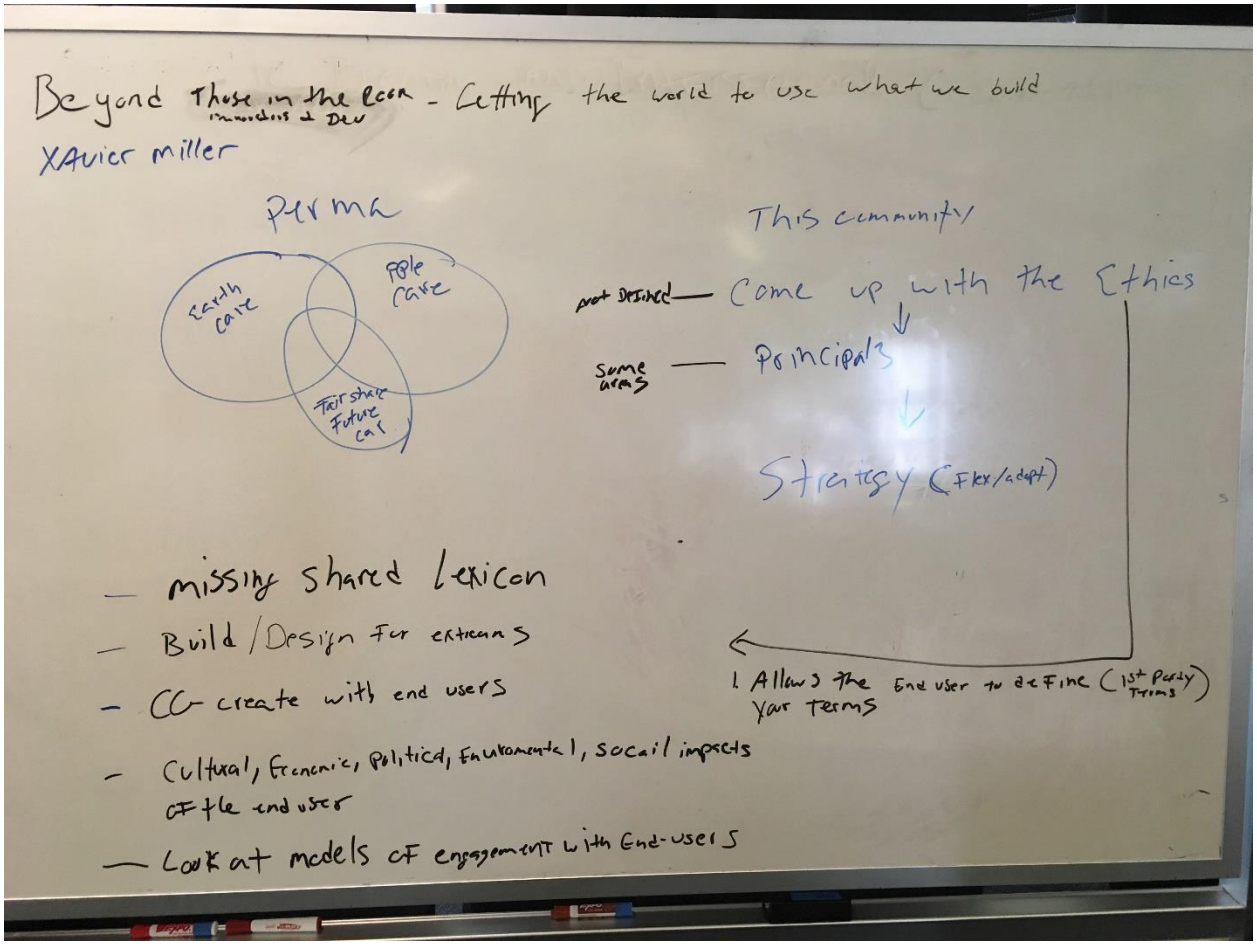




Beyond Early Adopters – Getting the World to Inform What We Build!

Thursday 2K
Convener: Xavior Miller
Notes-taker(s): Xavior Miller

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



MyData Movement – Looking At Identity From the Perspective of Human Centric Personal Data Management

Thursday 3A
Convener: Antti 'Jogi' Poikola
Notes-taker(s): Antti 'Jogi' Poikola

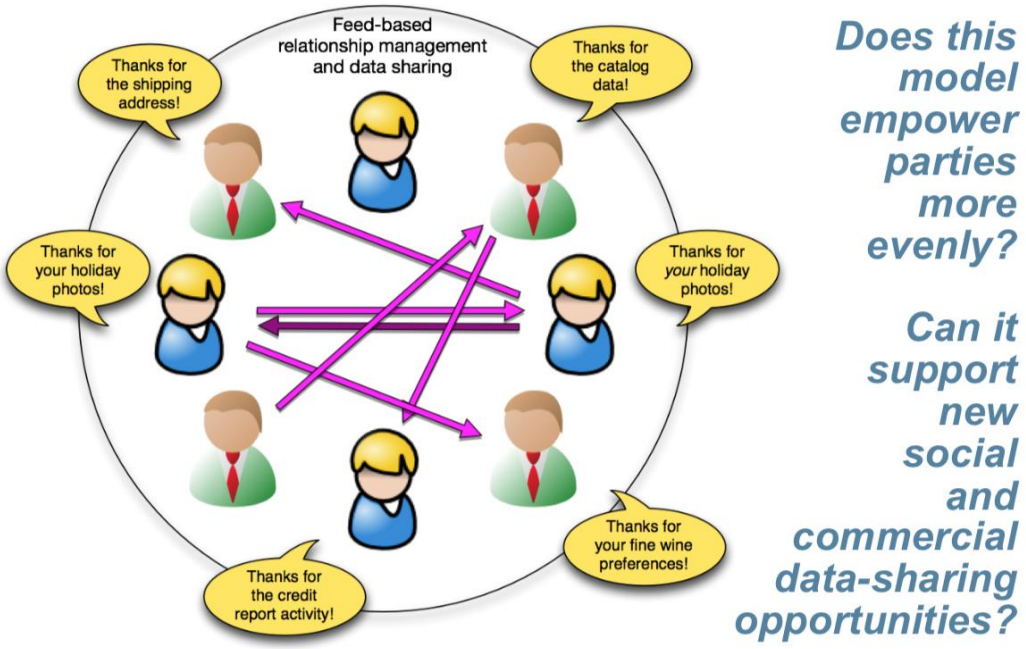
Tags: #mydata #interoperability #human-centric #mydata2018 conference #community-building

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

Notes are here: http://bit.ly/IIW-mydata Key points from the discussion:

- We would need "IIW business" to develop the new business models in the personal data domain with the same innovativeness and spirit what we have on the technical side.
- People should be equals in the interactions with organisations, it is not needed to turn the whole thing around so that people would be mandating everything and organisations under them… key is in balance, symmetry and equality. (see Eve's slide below)
- The word consumer is terrible, but also "user centric" and "customer centric" are putting the organisation in the driver's seat (our customer, the user of our service).
- Let's not speak about "data ownership", but rather about data rights (ref. Sandy Pentland from MIT). Ownership is exclusive but usually different parties have some legitimate rights over the same data.

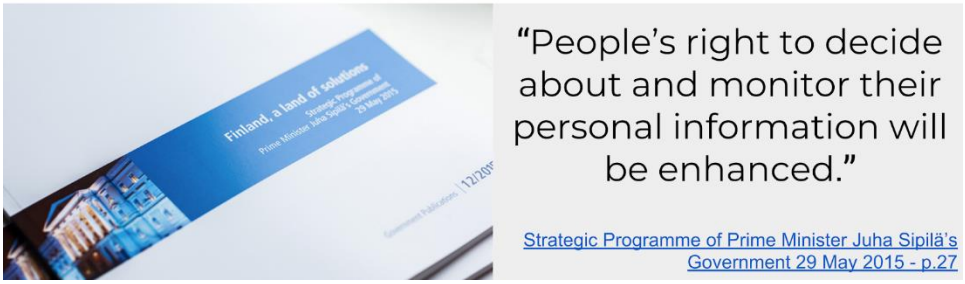
Eve Maler's slide exactly 10 years ago, presenting the idea of people being equals with organisations.



Below links and images that Jogi showed during the session:
Slides: http://bit.ly/IIW-mydata-slides
White paper: http://okffi.github.io/mydata
"MyData – A Nordic Model for human-centered personal data management and processing." Text and all original images (Creative Commons licensed) can be found from Github.

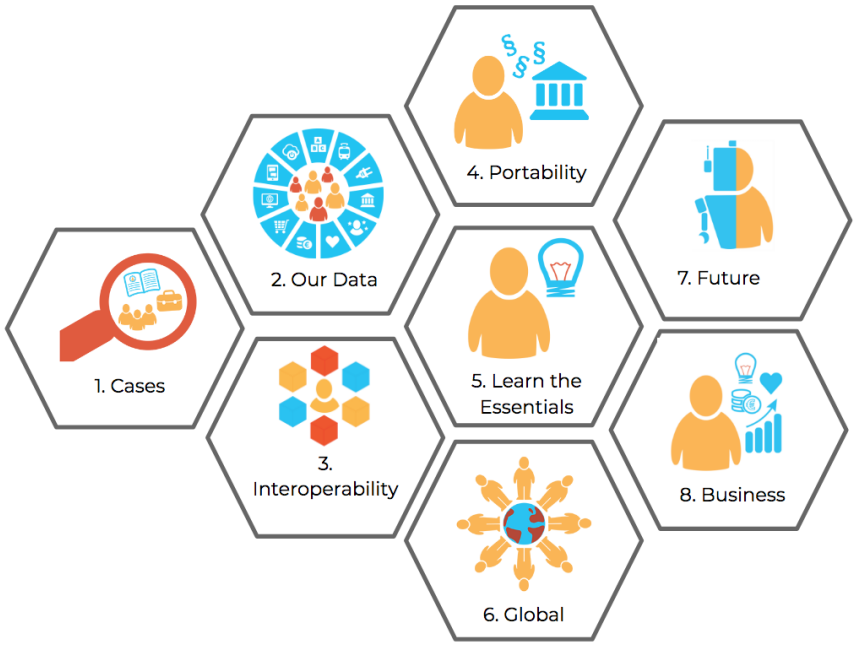
Locally the white paper influenced so that "MyData" idea is mentioned in the Finnish government agenda (highest level political paper). The english version of the paper lead the Finnish MyData people to learn to know about numerous initiatives, companies and organisations around the world who share the same vision. → birth of the global community.

MyData in the Government Agenda

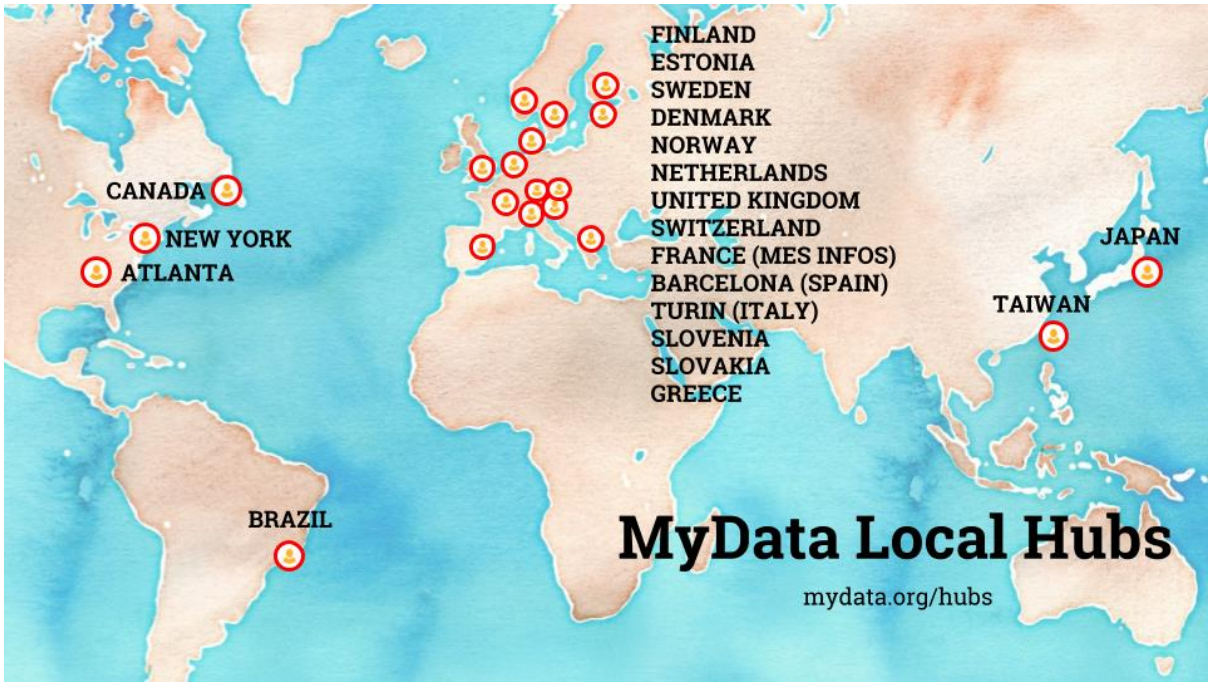


Conference (yearly end of August Helsinki): https://mydata2018.org/call-for-proposals
Organised now for third time in Helsinki Finland (videos and content from 2017). Approx. 800 participants, 3 days, programme proposals trough "open call", also open space on the second day. Call for proposals officially open until Apr 5th, but there is secret two week extension (until Apr 19th) provided for the IIW folks ;)

Topic tracks in the 2018 conference:



Community (local hubs and smaller meetings): http://mydata.org/slack
19 local hubs around the world, most of them are still very new (only couple of months old), organising informal meetups and contain just few people, but some are already more robust with local company involvement and joint projects bubbling up. If you want to set up a local hub: https://mydata.org/hubs



Declaration: https://mydata.org/declaration
Written by the community on 2017 (to be revised later), can be signed online, three key shifts:
1. From formal to actionable right (gdpr is not enough, we need tools to make it easy),
2. From data protection to data empowerment (people can decide what to do with their data), 3. From closed to open ecosystem (interoperability → competition)

eIDAS & SSI

Thursday 4I
Convener: Luca Boldrin
Notes-taker(s): Luca

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

There are no notes, but I prepared a few slides which I enclose:
https://drive.google.com/open?id=1JqXDSvlTnceO_anA1ZY8E2Av40OeBAM3

Self Sovereign – Reputation – Radical – Disintermediation + 2 Sided Networks

Thursday 3D
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:

The presentation can be accessed here:
https://drive.google.com/file/d/0B_luqCyRPBXjMnp2YnVqS1dlMTZNRzRkVXBZRlJCLTRGWjVF/view?usp=sharing

How Agents and Decentralized Interfaces Help the De-Siloization of IoT

Thursday 3F
Convener: Sam Curren, Evernym
Notes-taker(s): Scott Mace

Tags for the session - technology discussed/ideas considered:

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

Sam: Silos for light switches and Alexa is the problem that I have. IoT is assigned to silos. There's not a good alternate way to deploy a bunch of IoT devices managed by users that makes this happen. If the dance is complicated, they'll take it back to Costco.

Q: It's a sad rainy day slide.

Sam: This is the problem that sucks. DIDs resolve to service pointers. Which points to some thing that I control. I've been talking about extensible APIs. Vlad calls it decentralized interfaces. One thing these silos have is an API. The device knows how to talk to the API. That's one of the reasons for silos actually existing. Has to connect to a predictable API. Let's say I have a big thing capable of running APIs. I could install an API that happens to be a light API. If I have a thing, maybe cloud, maybe in my house, and can install an API interface according to some standard, now we're removing one of the barriers to connecting this API to something I have control of. The API has some behavior. Kim Lane had a blog post and said where's the WordPress of APIs. So many have similar functionality.

George Fletcher: Are you thinking standardization of these APIs across verticals?

It's going to be messy. I'm unlikely to have one API for a variety of light switch devices. The people that created them did not agree for some reason. Maybe a competitor who didn't want to share.

Q: Or one manufacturer thought only white light, the second had colors.

Sam: A bunch of the shared logic is going to be the same. The same WP-like plug-in could support two interfaces with the same basic logic. In doing so, we attack the problem with a couple of options. We want to make our stuff work. So various devices can plug in. Now it's messy. Sometimes there's movement from an older API to newer APIs. That's mostly OK.

Q: Amazon wants to know the stuff you're doing.

Sam: The larger question is the value proposition for device manufacturers. Let's pin that for a second. The voice stuff is still going to go to the server of the richest man in the world. But instead of going to another silo to issue that command, Alexa messages my general API which then responds instead. I can avoid Alexa having to be tied in the cloud directly to all these things. I can have logic on how to turn on and off various lights.

Q: I spent some time on a contract doing smart lighting. There is no margin for devices at all. The only thing you can do is attempt to monetize data on the devices. Practically everybody says I'm not paying for the devices. How can you be profitable?

Sam: Alibaba will get there. For example, can buy non-UL certified WiFi switch. They're cheap, $8-10, less than 1/3 of U.S.-packaged tech. Not as easy as setting up Alexa, but that will come along. A lot of money in selling silos, no money in selling hardware. A super good question. The trends i'm seeing, we've got GDPR going on. I can see government regulation in Europe mandating certain behaviors for IoT devices. Can be more extensive laws. The value they have in running a silo is making use of the data. You still need services to make use of data. I.E. power monitor. Produces power use signature over time. Services apply machine learning and identify individual devices. Still value in the silo. We can with consent provide a data feed, an opportunity to perform same service but not run afoul of the regulation. We get to pay for more valuable services. $7 device from Alibaba.

Q: Carl Ewett has talked about the idea of personal islets.

Sam: I can pay more for a silo, might get one for free, sell your data.

Q: We got really hot last year in the summer. Bought AC. Takes a lot of power. PG&E would like to charge us $12K to upgrade. Bought open-source tech for energy monitoring, 14 sensors, in main breaker box. As soon as energy consumption goes over a certain threshold, turns off certain devices, like the pumps for my pool. I cannot buy a commercial system that does this for me. Can't depend on the cloud, because as soon as my ISP goes down, circuits would go out. Raspberry Pi runs my pool pumps. WiFi is unreliable. I would like to have exactly this. Raspberry Pi registers with central controller, does some key exchanges. Based on these measurements of power consumption, what are the decisions.

Sam: You've got logic in here. One of the things we don't have yet because we're arguing about credentials exchange, the intelligence can happen in two ways. Companies like Evernym will support agents like this, power management. We can install behavior that actually does that. Now you can do power management or whatever feature. But Evernym isn't the only model. Open source projects can evolve it like WordPress. If you happen to be running one of those, you will have a way that write an extension that fits nicely into this framework, publish it for review. Code can be put on a GitHub repository. That's rougher than I'd like for my mom's sake. I can trivially update my own fork of it. Not advocating an exact follow of that. End up with a WordPress-like agent that allows us to pick. That may be forked or improved by someone else.

Q: Why the device manufacturers would buy into the model.

Sam: We talked about regulation, that might happen.

Q: If I don't have a silo at all I don't have to build it. But if there's no margin in the thing I'm building, I don't care about security or other stuff that should be in that thing.

Sam: The people have realized the money is in running the silos. You can buy ZigBee compatible wireless devices that already exist. WinkHub, SmartThings hub, HomeSeer hub. I can buy a $35 light switch from a company that does not produce a hub, I can install it and it works. The pattern is already starting to happen. Consent to monitor or evaluate data will flow into other things that make that happen.

Alan: Carl has talked about the company still owns the data, they have incentive, gives you better control.

Wendell: If you don't actually hold the data, that's a way out of GDPR. If you leave it on the consumer's device.

Alan: Can be encrypted with device owner's key. The company doesn't have liability.

Sam: With that as a layer, makes it a little easier to do. Personal data has changed because we have some cool technology answers.

Wendell: Have you uttered the words Pico or Digital Twin?

Sam: These are features that can provide these types of things. Phil knows that picos can function agents in this sense. If we can get the manufacturers to trust users installing this, we will see siloless tech being offered.

Q: What is the user buying that has an agent on it?

Sam: Raspberry Pi, or in the cloud. One opportunity is to have an address for your agent. Can be made available on your home network. Could be a home automation hub or WiFi router.

Alan: I just bought your smart house, now what?

Sam: Yeah, the transfer of smart home devices. And have assurance it's not all going to the other guy.

Phil: The connected car product called Fuse had this feature you could transfer the feature associated with your pico to another owner. Delete some personal data like your trips but not other data.

Sam: Air BnB data. One thing we haven't talked deeply about is we have this agents, but they can represent units of collection – a house independent of the owner, or an HOA. Various levels of things you can stick those for various effect.

Wendell: Houses are 100 years old. How are you going to develop standards, specs and protocols without getting bogged down in doing backward compatibility.

Sam: The interesting piece is the definition of the interfaces. I don't yet have perfect answers for. You define a chunk of interaction in a way you can actually support. So if you define a little chunk of API, it's not going to be a lot of it, and that allows you to then insert other parallel pieces of API next to it in ways that don't conflict. Competing APIs? May support three. Then there's a discovery process. Do I happen to speak anything you speak? Then pick the preferred.

Q: A lot of IoT information management happens to be time series data.

Wendell: This framing assumes common networking, TCP/IP, REST, microservices. But back net and analog signaling is cheaper and just doesn't break. How will this scale across a wide range of technologies? We might not be using CAT 5 in 25 years but we might still be using analog phone wires.

Sam: If I have a temperature sensor running off a tiny wireless module that isn't IP anything, the signal gets upgraded along the way.

Wendell: There's local nets with particular interesting properties. At some point you upgrade those into a protocol you do understand for a central agent. Is that the point?

Sam: Yes.

Wendell: So you need a gateway.

Sam: Yes.

Q: Which protocol?

Sam: Six months ago, RESTful, RESTish. Moving toward messaging.

Q: Uber has complicated schemes by which they are passing messages from the device into Kafka.

Sam: Things like MQTT, I see being wrapped, passed into the ecosystem. This is fairly forward thinking. The interesting part to me is figuring out how the interfaces will actually run. You can define messages in terms of Swagger arguments.

Wendell: Flexible because it's text-based. Making function calls. You don't tend to get dynamic updates. Swagger systems don't tend to call you back.

Q: What are the actuators in this?

Sam: I'm assuming it can call Web hooks. The more interesting case is signaling. The gateways will perform this functionality. I'm waiting for the IoT device hack where they can reconfigure which lights are connected to which light switches. Useful things Alexa could do. Ask questions of your agent. Tell me what your temperature is without having to resort to a weather service.

Q: Greengrass can talk to Alexa.

Sam: If you're a nerd. Not generalizable enough for my liking. It's $15 less for a siloless light switch. I'm sure they can go low, they just realized they can get $35 for the siloed. Prices from Amazon.

Alan: That argues against your point they are selling the hardware to get your data.

Q: IoT meetup around here, getting people to spill the beans how IoT companies are monetizing. There are different levels of maturity. Trying to insert themselves into your life on an ongoing basis, just like Twitter or FB, with an app on your mobile phone. That's the ultimate model.

Alan: Why isn't the device that isn't collecting data less expensive.

Phil: Amazon is famous for loss leaders for other reasons.

Sam: But the light switch is a good example. ZigBee has become the well-defined interface. They undercut the other guys. All home automation folks, they hate selling light switches. They can't charge a lot. Want to automate audio and video. I suspect that's why it's happened with light switches. I put a flow meter on cold water intake to my hot water heater. I can approximate the reheat rate, I can ask Alexa how long can I shower. Frustrated I can't make more use of this. Right now innovation is being stymied because it's hard to establish these patterns. This will help lower the cost of innovation.

Q: Pretty much impossible for a silo of any kind to solve all the use cases for the house. The house industry solves this problem with the Home Depot. The IoT, if ever real in the house, will look more like the Home Depot than like the iPhone.

Sam: A lot of home automation stuff is easy to script.

Q: There's a base infrastructure that needs to occur: Discovery, security, a place to store time series data over the long term.

Sam: I'm working on how to manage the security of the communication between the device and the agent.

George Fletcher: You need introduction. I want to provision it with credentials and tell it where it can interact with the agent as a whole.

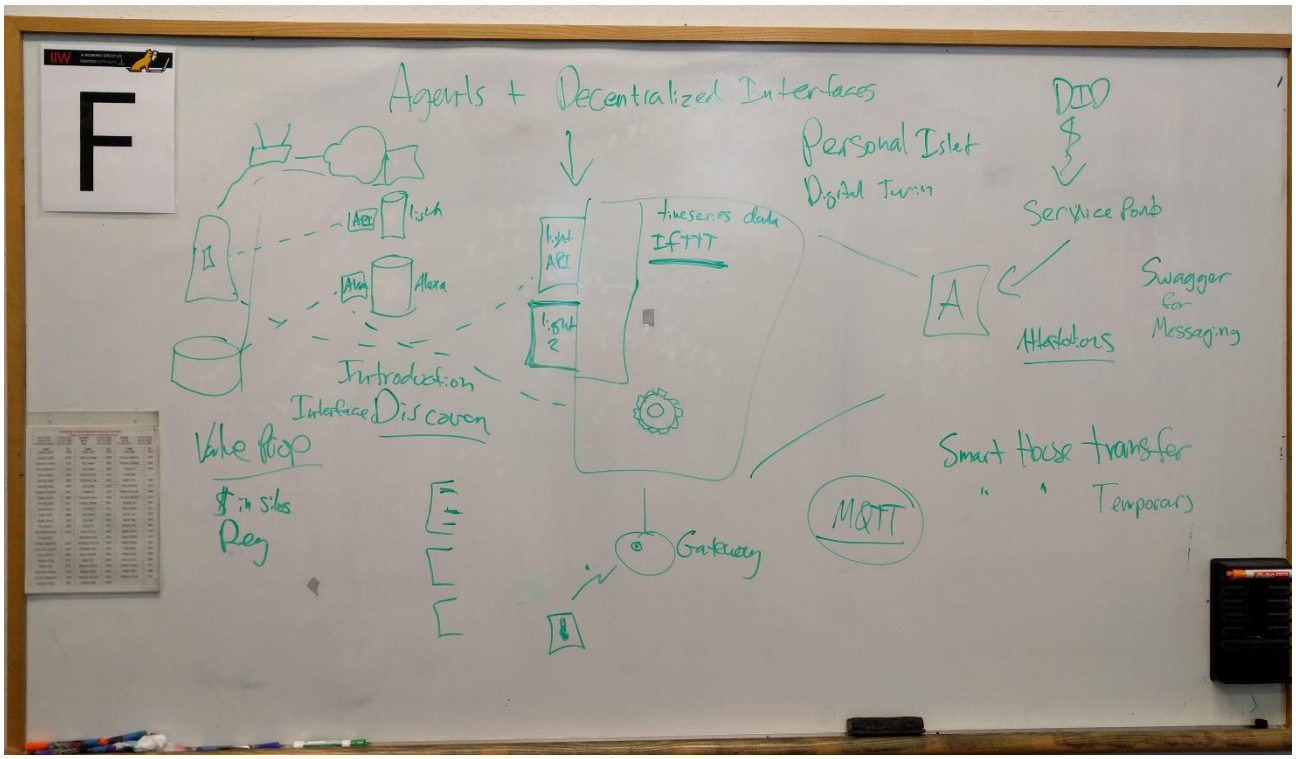
Sam: Interface discovery as part of the introduction. Yo agent, how can I talk to you.

Wendell: One thing you will need is a system to go analyze all those rules over the years, figure out if your house can do something unsafe. You can get pathological, unstable, risk point behaviors.

Sam: This is the experience of every nerd's wife. My wife wants the lamp to fade up when alarm goes off.

Phil: We walk into bedroom and want lights to come on, unless someone's in the bed. Then it's the dog.

Sam: What happens when it fails? If it fails badly, it's not a feature as well. I want a cookie jar that doesn't open itself until I weigh myself that day.



Designing Ourselves Into The Future & Humanizing DID's + VC's

Thursday 3G
Convener: Denise Aurora & Manu Sporny
Notes-taker(s): Denise Aurora & Manu Sporny

Tags for the Session -

technology, futures, science fiction, designing ourselves, humanity, human embodiment, human technology, technology of self, know thyself, stories, use cases, build worlds

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

Manu Sporny Notes
We gathered a number of people to talk about helping people break problematic patterns that they have and create a better future. The goal is to make sure that we're helping people reach their full potential with the technologies that we are creating. We gathered people that are story tellers with non-technical backgrounds to provide input to the W3C

Credentials Community Group and W3C Verifiable Claims Working Group.

The result of the discussion was a "Stories" section to the W3C CCG where people can tell their own stories about the future they want to create. This provides an outlet for those that are non-technical, but want to help and share stories (non-fiction, retellings, sci-fi, fiction, etc.):
https://w3c-ccg.github.io/stories/

Denise Aurora Notes
Discussed/Ideas Considered:
- humans in/as technology
- knowledge of self / know thyself
- designing technology for humanity technology as a positive force
- futurism
- dystopianism and utopianism
- light, dark has a role too
- real human stories/heroic adventures
- need of human stories to build technology for humanity
- use cases/stories to be acknowledged
- place for this discussion to be had

Discussion Notes (see below)

Key Understandings
- technology is being built by corporate interests
- technology can be built by human interests
- need for use cases and stories to build technologies for humanity

Outstanding Questions
- how do we make stories that have human relevance to help advance technology in ways that supports humanity's thriving, life, needs, joys

- how do we bring about the creation of technology that has human interests in mind
- how do we build worlds we want
- how do we support this financially

observations
- Paying attention to real human needs is not happening a lot
- technology that pushes the edge of creation is funded by large corporate interests -- have the money
- Refugee Use Case has been most discussed in W3C
- Engineers think in binary
- Futures discussions

action items/next steps
- make real world human use cases and stories
- include
    - science fiction stories
    - real world experiences
    - from experiencers
    - from artists
- develop real technologies with stories in mind
- make useful use cases in W3C
- make use case / story telling Group
- workshop in W3C

Denise Aurora's Idea Notes Discussed

We're creating and building worlds in the digital realm. Science fiction is coming to life faster than we alone may imagine…

Let's look into what we're creating, consider how we'll design the new world that's burgeoning through our human minds and innate desire for progressing the future into new dream realities.

Our current embodiment, our current and past experiences, our current ways of interacting with the world around us give us clues into the designing of systems that may augment human realities in

- the human body itself is technology
- how much do we know about/control it
- autonomic nervous system
- billions of neurons internetworked
- foreign invaders - bacteria, parasites & more
- futuristic potential stories (fictional or not)
    - i.e. alien machines that puppet us

Perception of Self, Multimedia Perceiving
How well can we know ourselves? And does our knowledge of self affect the technology we make?

Our Minds, Design, Information Networks
- Ancient technologies that survive today are for human brain & body balance & wellness

- Sri Yantra - Maha Yantra considered an original “Original Device” technology in some Indian traditions
- Visual Meditation (Yantra) for whole brain balance
- Humans, our mind networks & architectures are similar to current technology
- We have Input/Output
- We Send/Receive Signals
- Conduits of Reception & Perception
- Talking, Listening, Hearing, Seeing, Feeling, Making
- Sensory Apparatuses
- Technology of Self
- Algorithms spawn, catalyze within
- Mimicry
- Control and Authority of Self
- Knowing Thyself
- Core Self -- Identity
- What is at the core of our organic selves/machine?
- What pilots us?
- How do we decide?
- Prefrontal Cortex - Executive Self
- Influences & Persuasion
- Automated Systems, serve & not
- information, people, bots, ads, persuasion)
- “Going haywire”
- Human Transformation & Healing
- Smart Machines - Humanity

_____

Discussion Notes After
(After Denise Aurora Presented Some Ideas)

_____

Media/Art on Human Experience
Movies and Science Fiction Worlds that decipher futures with technology, dreams, emotions, battles, transformation, creation

- Movie : Inception
- The need for art and artists to create worlds that we may imagine in the future
- The role of art in the making of technology

Concepts of Human Experience
Feeding of Black and White Wolves within, which one do we feed? The darkness within.
Dark is not bad.
Start with knowing the self
self-worth, depression, inner pineapple, giving out life and warmth.

Real Futurist Stories

- Discuss the good and the bad as oppositions.
- Dystopian Futures versus Utopian Futures
- Bad is not that bad, it shows us, gives us insight.
- Programmed Dramas

- Complex, Realistic, Consequences, Stories, Emotional, Resiliencies
- In Story of Character had good and bad.
- Expand Our Emotional Capacity
- Use Case effects must be nuanced with all, good, bad, and everything in between.
- *Every Revolution has the good and bad.*
- Engineers think in binary
- How to make it make sense for engineers yet still include the nuances of human experience, honor human experience in technology creation.

Use Cases, Current Industry, Systems Design
- W3C
- Verifiable Claims
- Money Transfer, Accounts
- How do we bring human ideas & experiences to the light of our creation in technology, identity
- This is a Systems Design Discussion
- Socialize the W3C, execs, out in the world for customer to be primed, receive

SciFi, Stories, Use Cases, Ideas and Technology Ahead of Sociocultural Time

Futurism and Startups
Several people Stopped working in start-ups and became a futurist (Denise and another woman -- (Name?))

Elements in Use Cases
- Element is Data Analytics part
- self-protected is not easy
- When build a schema
- Those of sensitive info
- can be public
- people are using schema table
- people are not addressing sensitive points
- GDPR

Autonomy
- Inputs improve intercites
- All is Autonomy, MyStuff, MyData

Good Book : *Dragonflies Questions*
- less is more
- community
- we need literal science fiction stories
- relatable paths
- scifi stories
- In process of writing a new story

Standards
- no one is challenging stories
- need artists
- no people writing relatable story

Cocreation
- end users needs to step in
- people who want to create

W3C.org Existing Use Cases
- verifiable claims
- refugee crisis

Use Cases being talked about most
- Refugee crisis

User Cases Doc
- large corporate interests
- working group idea
- use-to-use
- engineers

Capabilities of weaving together stories for general public

Paul wrote a story for sensitive data

Data in Technology
- Corporate Compliance
- GDPR - General Data Protection Regulation in Europe
- Sensitive Data
- Any data that can be correlated is sensitive data

What is a Successful Use Case
- bring in diversity, futurism
- most follow money, other modes
- build something actionable
- take out key components
- fundamental metaphors
- futurist ideas

Stories
- Technique to get stories
- collaborative storytelling
- tell stories

Contributing
- time to story turn around
- get stories
- make website / page with stories
- stories that believe in improvements to humanity
- i.e. Refugee Story needs to be told by refugee
- control states, not a social story
- isolate, social model

Defining
- Use Identifiers rather than Identity
- What are the edges
- Sometimes need to be anonymous
- Trust Boundaries

- Multiple identities cases
- Pseudonyms
- Profit model vs not
- Terminology & Idea
- Identity Wallet & Can Do Box
- Verifiable Credentials vs. Identity

W3C
- identity workshop

Results! https://w3c-ccg.github.io/stories/

Hyperledger – Who/What/Where/Why Open Source

Thursday 3H
Convener: Dave Haseby
Notes-taker(s): Dave Haseby

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

Hyperledger is a group of open source projects dedicated to enterprise blockchain software and is organized under the Linux Foundation. Hyperledger has 10 projects and a number of mailing lists, chat rooms, working groups, meetups, and hackfests they organize to support and engage the community. Hyperledger just started a "labs" program for new projects that are related to blockchain and are of interest to the Hyperledger community.

Key Websites:
https://hyperledger.org
https://wiki.hyperledger.org
https://chat.hyperledger.org
https://lists.hyperledger.org
https://jira.hyperledger.org
https://gerrit.hyperledger.org
https://github.com/hyperledger
https://github.com/hyperledger-labs

Q: Why does Hyperledger have four different blockchain platform projects?

A: They are all slightly different with different goals. The Hyperledger community doesn't want to put all of their eggs in one basket. Hyperledger Indy was designed from the ground up to support distributed identity management and has lots of features tailored to verifiable claims/credentials. Hyperledger Fabric and Sawtooth are written in different languages and both targeted at large scale managed environments. Their primary difference is in where the primary API interfaces are between the pieces as well as how consensus and transaction validation is implemented.

Breaking Digital Gridlock – Banking and Identity

Thursday 3J
Convener: John Best
Notes-taker(s): John Best

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

Published Feb 9, 2018 – John's new book on Banking and Identity is now available.

From Amazon Oveview.
Strategic technology strategy for smaller financial institutions

Breaking Digital Gridlock empowers credit unions and community banks to make the shift to digital—even without a seven-figure consulting budget. From leadership, to technology, to security, and more, this book provides effective, real-world strategies for taking the leap without tearing your organization apart. With an emphasis on maintaining the culture, services, and features you have carefully crafted for your customers over the years, these strategies allow you to make your organization more resistant to digital disruption by adopting key technologies at key points in their evolution. Expert advice grounded in practicality shows how FinTech partnerships and strategic technology acquisition can foster new growth with minimal disruption, and how project management can be restructured to most effectively implement any digital solution and how to implement and leverage analytics. Specific implementation advice coupled with expert approaches offer the ability to modernize in an efficient, organized, financially-sound manner.

The companion website features a digital readiness assessment that helps clarify the breadth and scope of the change, and serves as a progress check every step of the way. Access to digital assets helps smooth the path to implementation, and a reader forum facilitates the exchange of ideas, experiences, and advice.

- Identify revolutionary versus evolutionary technology opportunities
- Empower employee innovation, and stop managing all risk out of good ideas
- Understand blockchain, machine learning, cloud computing, and other technologies
- Forge strategic partnerships that will drive growth and success amidst technological upheaval

It is widely accepted that digital is the future of banking, but *knowing* is not the same as *doing*. If your organization has been riding the fence for too long amidst uncertainty and budget constraints, *Breaking Digital Gridlock* provides the solutions, strategies, and knowledge you need to begin moving forward.

Who Am I? (Story Time with Marcus)

Thursday 4F
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:

This is a story from an Austrian children's book first published in 1972 that has sold a million copies and has been translated to many languages.

A cute little animal doesn't know its own name, and it doesn't know what kind of animal it is.

So it asks all the other animals in the neighborhood, but none of them can tell what kind of animal it is. So it becomes sad and desperate, and it begins to doubt itself. Perhaps it is nobody? Perhaps it doesn't exist at all?

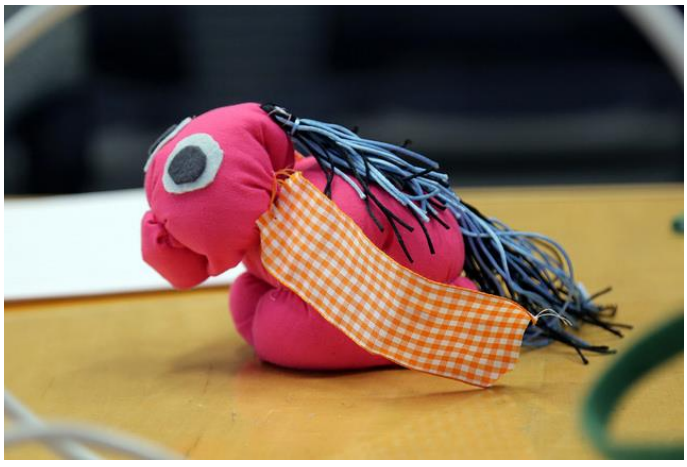
But then it suddenly realizes: I am me! And the Little-I-am-me is happy, and all the other animals agree: You are you!

The End.

For small children, the lesson is that they are an independent person, and that they can decide who they are independently of other.

For the Self-Sovereign Identity community, the statement "I am me" is the essence of what DIDs and DID Auth are all about - generating identity and proving it independently of service providers.

https://www.amazon.com/Das-kleine-Ich-bin-ich/dp/3702658572



A Self Sovereign Technology of Stack HIE of ONE

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

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

Interesting use case: Fax consent – safe harbor for MD
Adrian: Tech stack: DID, UMA/agent, mobile, me
The difference between these layers.

DID doc: public layer.

If I want to publish an endpoint for my agent or my mobile device or UMA auth server, all those things go into public layer. The other three layers are private. It maps into Sovrin quite well. Makes into the work being done in the Decentralized Identity Foundation. They call UMA auth server a hub or an identity container. HIE of One we call it a trustee.

Q: Do they differ in any meaningful way?

It is very much under discussion. Clearly mobile is a wallet. It has the biometric in it.

Q: Sometimes the wallets are virtual. It's where your keys are.

Adrian: This is the Sovrin blurring. I define the hub as always having an online endpoint.

Q: The hub/trustee is always on. A hospital will need to talk to the cloud agent 24/7.

Adrian: Sovrin spreads the wallet between the mobile and the hub.

Q: Let's get a paper out on this. I'll dig it up.

Adrian: Have we covered the standards by what we mean by the self-sovereign technology stack.

Q: PII is where?

Adrian: These three layers (not the public layer). I think this is pretty clean. If you look at the broader healthcare marketplace, a lot of people try to put private data on blockchains, on distributed ledgers. Medrec out of MIT (being revived) is a little like Sovrin. A distributed consensus, but it's a permissioned environment.

Q: What's their motivation for putting PII on blockchain?

Adrian: The value of your garden hose goes up by a factor of three. Less cynical way of saying it.

Q: Sequence? If you want to show you've got all the credentials for all the people before you walk into the operating room. Or that certain procedures were performed before other procedures were performed.

Adrian: People invent permissioned blockchains.

Wendell: The public blockchain, is there ever a notion that one of those providers could fail outright?

Adrian: Absolutely. Rebooting Web of Trust, nobody assumes any of this is going to last more than 10 years. My definition of self-sovereign is it has certain characteristics. Open source, substitutable, standards-based. There's no walled garden. Censorship resistant.

Q: Will the blockchain itself become unavailable? The idea is you have enough stewards that the blockchain is something that can never go away.

Wendell: I gave the example of a data center of records burned up. These things happen.

Q: I just got done discarding millions of records that were over 10 years old.

Adrian: Ownership definition in healthcare. If you can delete it, you own it. Lifelong ownership is a very key issue to how we design or apply this issue. I will tell you the HIE of One approach. We basically say that the UMA authorization server, all data stays at the place where it's created. Data stays at the point of origin. Then as a result you can have either anonymous relationships or pseudonomous relationships. Then you copy the data elsewhere if there is a trust issue.

Where HIE of One stands. Hoping to implement a couple of pilots. One is called a Homeless Health Record. Community Health Record HIE addon. People have come to us, both physician nonprofits, that HIE of One can solve. Trying to keep abreast of these standards. If any of these things [in the tech stack] are unique to us we fail.

We have 3 things we need. One of them we've sort of solved. We have a handle on the directory function. We have code. We don't have a handle on a utility token to deal with the network effect required to make this sustainable. Maybe a security token. We are not cryptographers and don't intend to be cryptographers.

Wendell: Why can't you buy all this stuff off the shelf?

Certainly adding crypto expertise to the team is unaffordable. I have a finance problem. I have to figure out how to fund it. $150B investment has gone into blockchain business models. I'm in good company but in healthcare I need to cross that bridge. But this isn't necessarily about my problem. I need to show joint venture to fill in the gaps. And technologically speaking, being able to do anything related to HIE of One, disintermediating data brokers, hospital based, others, particularly hospital, you have to manage all the roles hospitals are serving. Reputation is a tricky one.

Homeless Health Record is probably the simplest use case. If independent of any particular institution, nobody wants those patients, they're expensive and won't stay in your walled garden, you're losing money every time you treat them. No obvious owner. It's the camel's nose under the tent, the academic medical centers. They're willing to look at it in the case of the homeless population. Explicitly they asked for a way for the individual homeless person to have a health record in the cloud somewhere and for a caregiver that has a mobile device and credentials on a mobile device, could be a first responder, present those credentials to an independent health record, would see first a picture of the person. Has to be a QR code or mobile phone number that cedes this link. It is self sovereign to that homeless person. Everything is open and transparent. The community health record is where the medical society fits in. The HIEs are not sustainable. Many state HIEs are closing like in Texas. People are looking for alternative models for governance and sustainable. One avenue started in Kansas. They created an HIE

in the cloud, decided to market it through medical societies where the doctor is paying. This can get interesting. A lot of payers want to collaborate with providers and bypass the hospitals. There is the potential there to take health records away from the hospitals or traditional data brokers like Commonwell or CareQuality to monetize the data and fund the exchange. Anything that supports disintermediation of the mediators. We're working on 300 doctors, 3.1 million patients in Austin, like a medical society.

Q: Are they assuming they are going to monetize the data?

The data is worth $3000 a year on average versus the cost of operating this technology. Paying for Uport, Sovrin, Microsoft Azure, somewhere between zero and $300 a year. Apple iOS 11.3 is $0. $300 is all the software in HIE of One provide white glove service. Might cover that.

Q: People need access.

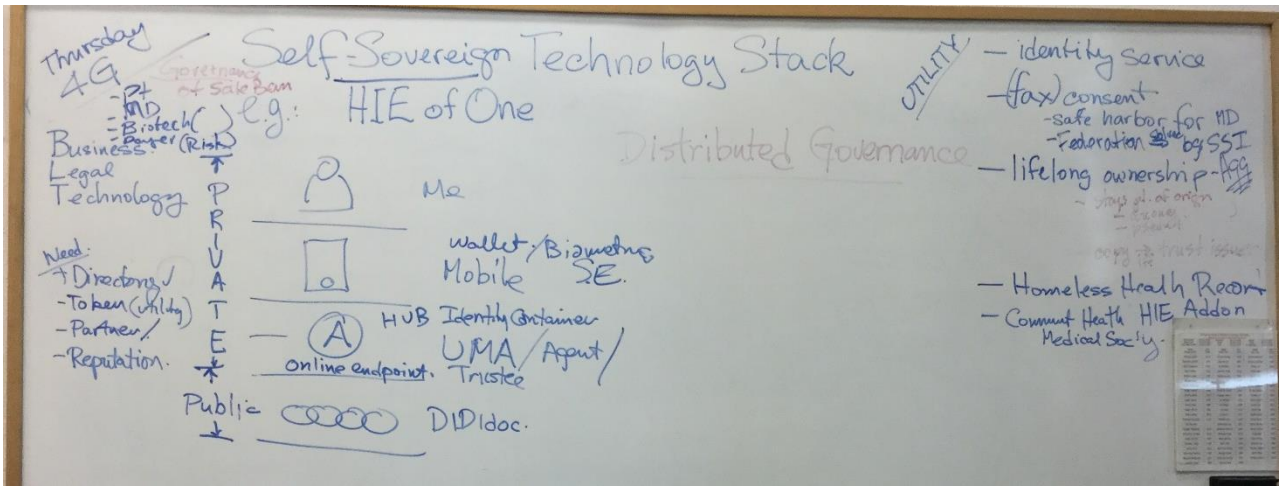
In the U.S. we have a trillion dollars of waste and fraud. Divide by 300 million people, $3000 a year.

Q: Part of that is price fixing.

Q: Missed diagnosis.

Overcoding.
Q: The hospital bill I got was $250,000. Kaiser negotiated it down to $80,000. You can call that fraud. It made more sense when Adrian called it price fixing. When we disintermediate that, where does that value go?

In terms of funding a business or making a solution, unless we can deal with the actual value of the data, what have we at HIE of One invented since the last IIW. I put a checkmark next to the directory. We've introduced a concept of distributed governance. If you have $3000 worth of data sitting in your aggregator, in your identity container, you want to monetize that in different ways. Not necessarily Google. Not the government. In Europe they're willing to take that bet. And certainly don't want Mass General to monetize that. So there isn't any centralized way of apportioning how that $3000 of value is going to be split among these four – patients, doctors, biotech, payers. In the case of the payer, they're basically worried about risk adjustment. Some patients will want to sell their data. The doctor also has an interest in monetizing this. Maybe it's a way to have concierge medicine for all. Austin has raised taxes to improve maldistribution of healthcare.



Digital Divide & Gender Equality in Indian Emerging Markets

Tuesday 41
Convener: Munir Mohhamed
Notes-taker(s): Heidi N Saul

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

Munir is part of the IEEE Team that will be producing and hosting an IIW inspired and supported event, in Bangalore – July 10 & 11, 2018.

#inDITA = India Digital Identity & Trusted Agency OR India Digital Inclusion through Trust in Agency
Both of these will represent the intent and spirit of this new ongoing IIW Like Open Space unConference in India.

In this session Munir brought up the common circumstance of families (mostly in rural?) India who all share one phone. This phone is often provided by whomever the husband works for, and is the only wi-fi connected digital device the family has access to or owns. The husband would usually have the phone/smartphone during the day and in the evening the wife and children would have the opportunity to use it.

Facts and/or Issues with this 'shared resource' include:

- Phone usually provided by the husbands employer – so husband has phone all day
- Wife and Children primarily get to use use the phone in the evening
- It is often used mostlyto watch videos/films & social media rather than education and related
- Currently no way for Wife's viewing/communication to be private from Husband
- How to encourage use for educational purposes – window to a bigger world

This would make a great session at the upcoming Identity Event in Bangalore –
#inDITA July 10 – 11, 2018 at the **International Institute of Information Technology, Bangalore**

Value Network Mapping Market Models 4 Self Sovereign Ecosystem

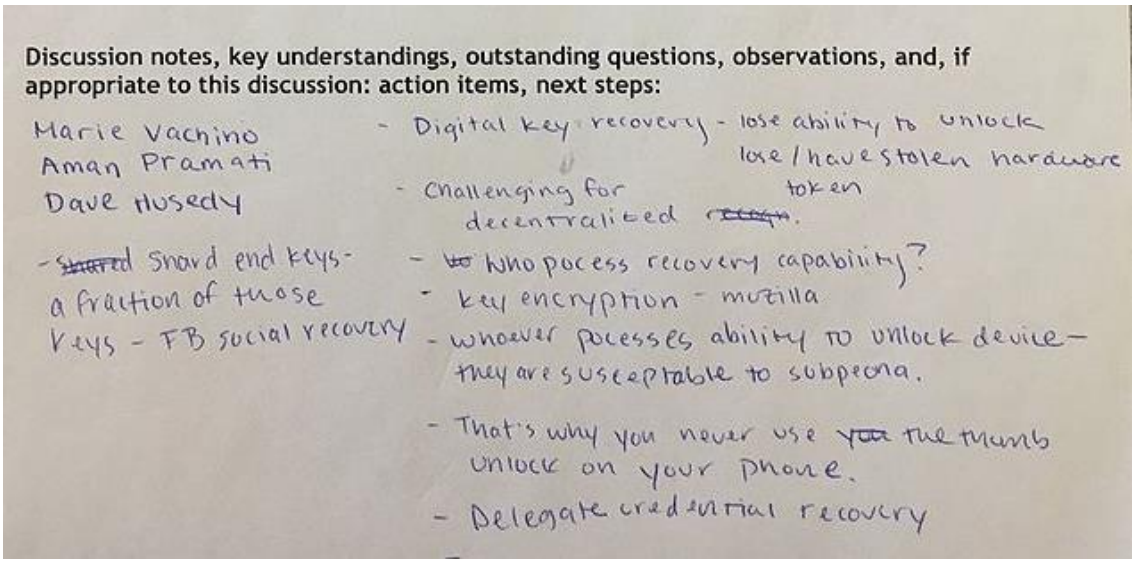
Thursday 4J
Convener: Kaliya @identitywoman
Notes-taker(s):

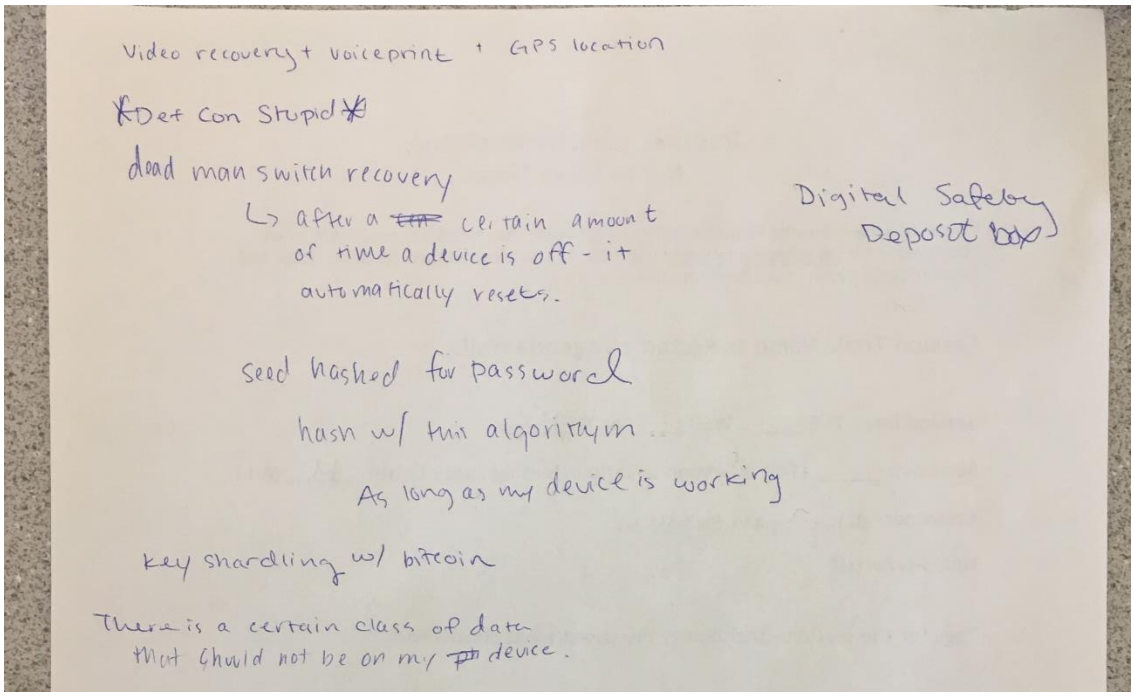
Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

We didn't do Value Network Mapping - I was too tired.
Here is a link to information on the method and how it might be used.
https://identitywoman.net/value-network-mapping-an-ecosystem-tool/

A Conversation About RECOVERING…. A Forgotten Credential Security

Thursday 4K
Convener: Elizabeth Grothues
Notes-taker(s):





CRBAC: Cinnamon-Roll-Based Access Control

Thursday 5A
Convener: Justin Richer, Eve Maler
Notes-taker(s): Eve Maler

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

Source material: beautiful cinnamon roll & Source material: UMA2 slides

The notion of CRBAC came from an UMA2 presentation of last year.

The Winter Soldier (Bucky Barnes — two identities!) is a precious cinnamon roll, it turns out. What if you had a system that could handle someone, like him who, it turns out, was brainwashed and didn't know who he was?

Sometimes he's a reasonable person to allow access to, and sometimes he's really not.

A guy in NYC started asking people in stores if he could get the "nice guy discount". One time out of five he got a discount! The real world is malleable; the digital world, not so much.

At Consumer Identity World on a consent panel, Justin contended that consent in the real world is straightforward: you let something happen and you're okay with it. It's not always explicit. Trouble happens when the reading of it is in opposition to events. In digital systems, subtlety goes awry and we get lots of checkboxes.

Could we have a system where somebody is a precious cinnamon roll and they're okay?

Discussion: Thought this was going to be about RBAC! Getting away from binary yes/no sounds great. Binary yes/no leads to a lot more no's than yes's. Where would one of these systems be most useful? It would be a huge improvement.

This is not the same thing as contract-bound employee access to lots of stuff. Sure, there are people who know how to "work the system" and get a better work laptop.

This isn't about "prove you are you". This is about "you are awesome and you grant unto others the right to give you stuff". It's like hotel room rates.

Frank Abagnale, the guy who spoke at CIS, got all the "nice guy discounts". In a digital world, it's the lack of clarity and nuance, and the explicitness that these systems have. In the real world (ahem), if you want to wield Mjolnir, you have to be worthy. How do you define worthy? Some attributes aren't checkbox-y.

Would behavioral analysis be relevant here? Absolutely. Also the ability to game systems. You can go a long way with the right look and a lot of confidence — that's why they call it a confidence game. That's why we're scared of having digital systems be expressive in this way.

Some cases are higher-consequence than others. Gaming a TSA line is different from getting a discount or not. We often treat digital systems as if they're always the most important thing ever and we sometimes don't have good ways of modeling risk.

Sounds like this is complementary to risk-adaptive access control. If the risk is high, you'd better be a really precious cinnamon roll.

This sounds like multi-source signaling for access control, where there's no limit to the number of sources. It's sort of heuristic. This works quite well in meatspace, regarding things like reading faces. Risk and fraud analytics do get used.

A lot of our social systems are built around such signals. Digital systems aren't yet this sophisticated. Or is that true? Ad systems seem to have gotten sophisticated. They're just not working entirely on our behalf.

The physical world enforces scarcity, while the virtual world doesn't.

Can the digital world even have precious cinnamon rolls? Doc made the points that in the virtual world there's no "distance" as there is in the physical world. The "nice guy" discount is actually unfair and inconsistent. As engineers we don't tend to think about building such systems. The PCR is nondeterministic. Although, ironically, an awful lot of identity systems are made to be loyalty systems.

Sometimes, when you're shopping online, you have no idea you're getting a discount. Sometimes you're just dealing with incomplete information and trying to figure out what you're dealing with, so it's not about unfairness.

Judith shared the headline of an article from 2014 discussing a machine learning algorithm that identified which customers to give steeper discounts to: the PCR algorithm! And the Wall Street Journal recently started giving free access once again to articles to some people, if it determined that it can upsell a subscription to them.

The property of Bucky that makes him a PRC is very context-dependent, because as soon as he hears those 17 words, he changes.

Do you need to be a PCR just to exist? "I'm sorry, you need to be a PRC to vote." Digital identity is becoming a forced intermediary to important life activities. That is a big problem.

Then again, if everyone is a cinnamon roll, is anyone a cinnamon roll? How does one even learn how to become a PCR? How does one protect against discovery?

What you need to be in order to be a PCR is different for every store clerk.

What we appear to mean here by PCR is describing the application of stereotypes. Inferences are already being made by every system. An idea brought up yesterday was that the notion of "self-owned identity" is a misnomer; identity exists only in relationship.

Then there is a web-of-trust notion where a community can say who I am. "The Internet has decided that Bucky is a cinnamon roll, and that Falcon mostly is.

The Internet is not as forgetful as the store clerk. It's in your best interest to remember who was a PCR last time. "If the Internet were more forgetful, it would be more benign."

Algorithm example: https://www.forbes.com/sites/adamtanner/2014/03/26/different-customers-different-prices-thanks-to-big-data/#7e341a057305

The Sovereign Web-Of-Trust Model / Dynamic Web of Trust?

Thursday 5B
Convener: Drummond Reed, Jacob S
Notes-taker(s): Drummond Reed

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

This session was given by Drummond Reed, a trustee and Chair of the Sovrin Trust Framework Working Group at the Sovrin Foundation.

The session started by recapitulating the basic concepts of self-sovereign identity (SSI) from the SSI 101 and 102 sessions on Tuesday and Wednesday morning, especially the roles of Issuers, Holders (Identity Owners), and Verifiers of digital credentials. See the first slide deck below.

It then reviewed the content of the second slide deck on the core concepts of the Sovrin Web of Trust model in order to explain how digital credentials can be scaled into any size trust network, from a small network for a single school, town, church, or business to a global network like Visa or MasterCard.

- **Identity owners** are the core participants in the Sovrin network. They hold digital credentials issued by Issuers and then they present them to Verifiers in order to access a protected resource or authorize a transaction.
- **Trust anchors** are recognized as the authoritative issuers for a particular set of digital credentials. For example, governments are trust anchors for government IDs; universities are trust anchors for degrees and transcripts; credit unions are trust anchors for credit union memberships, etc.
- **Trust hubs** are "trust anchors for trust anchors", i.e., directory services that allow verifiers to efficiently verify that a trust anchor is authoritative for a particular type of credential for a particular trust network under a particular trust framework.

This was followed by a long Q&A about different aspects of this model, including how it compared to and was different than conventional hierarchical PKI models of trust (main answer: it is a superset, i.e., any number of PKI trust hierarchies could participate within the Sovrin web of trust).

Drummond invited anyone interested to join the Sovrin Trust Framework Working Group by the Sovrin Foundation contact page, https://sovrin.org/contact/, or by joining the Sovrin Slack and sending Drummond a direct message.

Links:

1. IIW Introduction to Self-Sovereign Identity
2. The Sovrin Web of Trust Model
3. The Sovrin Glossary
4. The Sovrin Trust Framework
5. Sovrin Trust Framework Working Group Meeting Page

ID & Connected Vehicle

Thursday 5C
Convener: Carol Tang
Notes-taker(s): Carol Tang

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

Carol started the session with a brief overview:

Looking ahead, automotive is moving into inevitable future of autonomous, connected, electronic and shared usages. With these driving forces, challenges on identify are many. This session is to discuss and hopefully identify some challenges that we are going to face in the new era of mobility.

Discussions:

1. Challenges in terms of identify
   - Identity for vehicle and/or passengers
   - Many internet ID issues will appear in vehicle which need corresponding protection
   - How to protect the identify and provide a seamless user experience with the new mobile living space

2. Challenges of security in connected vehicle space
   - In vehicle connected modules
   - Connected modules to cloud
   - V2X

3. Challenges in privacy
   - Concerns on data sharing with law enforcement, medical/emergency first responder
   - GDPR?
   - Concerns on data collected in vehicle

Other concerns
Supply chain management, dealership management

Machine Readable Asserted Terms for Privacy – an IEEEE Standards Working Group (SA 7012)

Thursday 5F
Convener: Doc Searls, Joyce Searls
Notes-taker(s): *Scott Mace*

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

7012 – Standard for Machine Readable Personal Privacy Terms.

Joyce: How one joins. About to go up publicly, will be announced to all IEEE members as a person. Our committee is three people – me, Doc and David Reed.

Doc: All the smarts in the Internet are the end points. He has a PhD in IT.

Phil: And wrote Reed's Law.

Joyce: The network effect.

Doc: He has some of the most brilliant and sometimes withering emails ever written. This language is crafted so as not to replicate any other standards effort going on. It's also confined to just hearing and agreeing to not address privacy policies. Terms require agreement. Privacy policies do not. Maybe privacy policies could be expressed in a machine readable form, but it won't be this.

Joyce: David brilliantly said we want to do this low-level thing. Once that channel is open, you can say whatever you want to say. It's on the title but the idea is to build something super low-level, not in email, to an enterprise machine.

Doc: Jlinc has a protocol that is a way to record provenance onto servers which they call the A server and the B server. Left open whether it's on a blockchain. The protocol itself has a GitHub thing. Not a whole lot on it so far. Committed to open sourcing the parts that matter.

Joyce: To be clear, that's not the standard. Just they will show up. Eve Maler will show up with UMA and her BLT stack.

Wendell: What is the scheme under which you're licensing this? Patent licenses?

Joyce: It's IEEE whatever their standard terms are.

Wendell: They don't do open source. They all people to standardize on patented stuff. That would be helpful if super open open, not patent stuff.

Doc: A big part of the protocol is the moment you sit down in the WG you have to put your patents on the table. There is still a regime for doing that.

Joyce: Commitment is a meeting a month, plus subgroups.

Q: Possible to lurk?

Joyce: Make sure the people on the WG want to contribute. The chair needs to say contribute. Chair perogative to kick people out. The WG puts out a progress report quarterly.

Q: This is a protocol?

Doc: No. David hopes a protocol will come out of it. Will be a functional specification, may include a data model. Deliverables. Serialization. Ontologies?

Q: Who wants this and why will they want it?

Doc: The carrot is better signaling from demand side of the market. Signal to the sites and services of the world. This is a way to do it.

Joyce: I can imagine I will request something and somebody can build a way to listen for a certain type of request.

Joe: The real opportunity is flipping the DNT conversation. This is about how to create value.

Phil: Somebody has to write this in software on both sides.

Q: We have a company that talks to customers and retailers.

Q: You as a consumer launch a request, I found this cute pair of shoes, where can I get it for the cheapest price.

Q: How does that fall under the word privacy?

Joyce: We described it to the IEEE as do not retarget. It's really about how to signal from machine to machine.

Wendell: That's an automated RFP process. That's great but seems expansive for what you are going to attempt here. A set of matching criteria. This is not about privacy but it will be hard to get away from that.

Joyce: It's not a policy. It's a term not a policy.

Doc: This comes down from our legal folks as a distinction that needs to be made. [Points to "The new frontier for CRM is CDL: Customer Driven Leads, post 10/6/16]. When the customer themselves qualify themselves as a lead. Glengarry Glen Ross. If you declare yourself a lead, that ideally comes with some terms for the use of the data that qualifies you. Basically making verified claims I suppose.

Q: Shut up and take my money.

Doc: A casual assumption no one is going to ask you for your name. This is one scenario in which this applies.

Wendell: This is what search engine marketing does. How to specify your interest and ranges for your RFPs by giving search keywords, price ranges, little expressions like that. A whole industry that would love standards. A little surprised IEEE would be a venue, but there's a thing there. I'll send you stuff.

Doc: Project VRM is an evangelical thing. John Haymond, Sean Bohan, behind this, they pursued us. Before we called it intentcasting we called it a personal RFP.

Joyce: Drummond came up with intentcasting. We want standards because we want to do it one way as an individual.

Wendell: SEO tend to have proprietary ways to do this. There aren't standards there. There's bilateral integrations. Google can dictate things. Nexttag. Amazon. Have their own ways. It doesnt mean you couldnt facilitate--

Joyce: Outside all those silos. If I'm going to buy a refrigerator, the search is from hunger. I start with the size of my space. Then I can look at any machine that's available.

Joe: There's a big conflation that might make this standard harder to do. Ventana Shopper, was working with Wendell and intentcasting. If you flip back to the other page, that's focused on terms, which is not about what washing machine I want to buy. It's a natural next step to get into intentcasting, but that's not what this is.

Wendell: Legal, or commercial?

Joyce: David just says do it low enough, machine responding to machine, the use cases can flow.

Wendell: You will have a dictionary of possible commercial terms and conditions, and a protocol that gets from one side to the other. The user can write this up and they will submit this.

Joe: If I were rigorous about what you just said, headers in HTTP does that you just said.

Doc: One of the reasons we have avoided headers is they're all occupied.

Wendell: They're extensible. In response, the server responds back to you, I understand you, but I gave you these things. There is that conversation there. Once you have a conversation, you have a protocol for how it has to happen. We're doing intentcasting, above the level he's at.

Joe: There is the transport of headers that happens.

Wendell: This happens in ad targeting through real time bidding all the time. There's a protocol for that, and a thing called deals for the seller and an equivalent thing for product/user. You may do the same thing with user as principal (not product). I want a refrigerator, white, 36 inches tall with a blockchain.

Joyce: RTB is where it could all happen. I'm happy to take ads on this, don't send me anything else. And it expires. We've been talking about it for 3-4 years.

Doc: A friend wanted to create project VRM and created largest RTB system in the U.K. His solution is can we make this apparatus that I've already built work the other way? What we're talking about here, a larger context in which this is happening, we're trying to stand up the non-guesswork side of commerce, hopefully through existing channels already built that have guesswork in them.

Wendell: Amazon syndicates out their catalog, order book to many other marketplaces to help them out with purchasing. Products like these. Preferences individuals have. All of the ad tech apparatus

could begin doing this intentcast response stuff. Now you've got a seller getting their order book, preferences ready to go. That's a match there.

Joe: That was the whole play with Ventana Shopper. The publishers don't even have to be part of the dialog.

Yogi: Profile matching could be the thing.

Nathan: Vocabulary becomes a problem. Enumerating all entities. The semantic Web tried. It's more of a best fit approach. I say my idea and you give me back what you think that means.

Wendell: That's the basic way search information retrieval works. What crushed other suppliers is Google applied all that matching tech to intentcasting based on search terms you typed in. In 2010 they let the algorithms slide. People larded up first few pages with same product. You could have a protocol that looks very much like search. Profiles are matched but it's a search information retrieval model. Maybe that's what you want to work again, doesnt solve other use cases such as health, but intentcasting about ecommerce and experiences is well known in the search industry. You're codifying what's already known.

Yogi: The Jlinc could be the profile for GDPR things.

Nathan: Another way out, limit the vocabulary. If you try to define it as generic search, the evolution of terms isn't tenable.

Joe: If users can express arbitary terms...the reason the Web works, users can't express arbitrary terms.

Yogi: That's the idea behind Customer Commons.

Nathan: How do you bind the scope of what can be asked when.

Delegated Authority using DIDs and Verified Credentials

Thursday 5G
Convener: Stephen Curran, John Jordan BC Government
Notes-taker(s): Stephen Curran, BC Government

Tags for the session - technology discussed/ideas considered:

#delegation #sovrin #verifiablecredentials #hl-indy #bcgov

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

The session began with a presentation/strawman of a proposed approach to the issue (background, challenges, goals and proposed approach) and continued with a discussion of the pros, cons and improvements on the proposal.

tl;dr - The goals of the approach are worth achieving, and the mechanisms proposed can work. However, the use of DIDs and Verifiable Credentials are not required for the approach to work. Other mechanisms (SAML tokens, JWTs) that have the same "proof attributes" of Verifiable Credentials would work just as a well. The proposed implementation of capabilities is both sufficient for simple implementations and arbitrarily extensible.

For practical implementations allowing arbitrary chains of delegation, it would be useful to embed the full chain of proofs to prevent the need to retrieve and query each proof interactively from the delegates involved in the chain.

Background
The presented discussion will be Hyperledger-Indy (Sovrin)-centric - because that is what we're using on our project

There is an associated, evolving paper about this that describes the mechanism:
Delegated Authority Capabilities using Verifiable Credentials
(https://docs.google.com/document/d/1yZaBGWHv-ogzN6S2wZ95d1T_Ykeq0GTGGZv9trGc6Ws/edit?usp=sharing)

HyperLedger Indy's implementation of Verifiable Credentials (called "anoncreds" in Indy) are the "transport mechanism" for delivering the Delegated Authority

- They are not being used in this overview to (for example) proof Experience/Academic Credentials, etc.
- That is a parallel, but separate, issue from Delegation of Authority

Challenge
- Organizations are made up of people
  - Some inside the organization, some outside
  - A person can be "Organization" - delegating authority to family members, powers of attorney, etc.
- Services offer capabilities to the Organization
- People access Services to work on behalf of the Organization
- Organizations delegate authorization to people based on their function
  - What capabilities they are permitted to perform on the service

Current models:

- Services don't offer delegation - accounts are shared
    - Simple - share passwords (Really Bad!)
    - Sophisticated - controlled account available for multiple people - e.g. Hootsuite-controlled access to an Company's official Twitter account
- Services provide functionality to allow Organizations to manage Delegation - for that Service
    - In the government - every Service does this

Goal:

- Enable access to a Service by the Organizations, not to individuals
    - Simplify Service "User Management" functionality - track the Organization, not the individuals using the account
- Enable the Organization to Delegate Authority - inside the Organization
- Enable the Service to express the Capabilities they offer and understand
- Enable a Delegation protocol
    - Organization Delegates Capability X to Person Y
    - Person Y accesses Service for Capability X on behalf of the Organization

Verifiable Credentials - Important Attributes

- Uses the W3C-Model of Issuer, Holder and Verifier
- The verifier can prove:
    - The data was not tampered with
    - Who issued the data
    - That the data was issued to the Holder
    - That the data can be checked for Revocation in real time

Mechanism - Registration

- Organization establishes relationship with Service
- DIDs are exchanged as IDs for each party - Organization and Service
- Service retains DID of Organization
- Service provides Organization with list of Capabilities
- **Aside**: Traditional Handling of this in Government Services
    - Functionality offered to users are controlled by Permissions
        - Eg. List Transactions, Create Transaction, Print, etc.
    - Arbitrary Roles can be defined as a set of Permissions
    - We envision for Government Services, the expressed Capabilities will be "Roles" understood in the Business Context
        - E.g. for the "Patent Office" Service, the roles are "Patent Attorney", "Inventor", "Paralegal"

Mechanism - Delegation

- Organization uses a common schema (format of Verifiable Credential) to issue a Verifiable Credential to a person
    - Assumes a relationship between person and Organization
- Verifiable Credential schema includes:
    - Service Name
    - Issuer Name
    - Capability(ies)
    - Signed DID of Issuer
    - Optional - Identifier of Delegate (Organization ID, Name, etc.)

- Delegate may issue a Verifiable Credential to others...and so on
    - Attorney to Paralegal - perhaps with a subset of Capabilities

Mechanism - Login

- Delegate initiates login to Service
    - Not recognized
- Service requests Proof of Delegated Authority
- Delegate provided proof of issued Verifiable Credential
- If necessary - Follow chain of Proofs to get to recognized Issuer
- Check revocations
- Recognize identity and capability
    - Organization
    - Delegated Capability(ies)
- Separate Issue - May require other Proofs to use the Service
    - Eg. Capability to use “Patent Attorney” capability may also require Proof of Attorney in Good Standing from the Bar

Improvements/Optimizations:

- “Delegateable” flag - prevent chain of delegation
- Hyperledger - Indy - normal flow is for each Issuer to have a published (on ledger) DID and Credential Definition on Ledger
    - Could instead, embed the DID Public Key, and Credential Definition in the Verifiable Credential so the Service receives the full chain
    - Still has to check revocation for each Issued credential in the chain

Observations from the Discussion:

The general feeling was that the proposed flow is appropriate. However, the use of DIDs, decentralized ledgers, and Verifiable Credentials (as defined by W3C or Hyperledger Indy) are not required. There are other mechanisms that could be used that they have the same "proof" attributes of Verifiable Credentials (listed above), including SAML tokens, JWT, etc.

We also agreed that the underlying transport mechanism for the Delegated Capabilities (e.g. Verifiable Credentials, SAML Tokens, JWT) should have a native credential expiration mechanism. This will reduce the instances of revocation for routine handling of the delegation.

The Capabilities model that we describe above (the "Permissions and Roles" model commonly used by Government Services) could be made arbitrarily more complex, depending on the domain, complexity of the use case and the effectiveness of the user interface in supporting users. However, we agreed that is an "implementation detail" that does not affect the proposed mechanism. Having said that, if there is a goal that such a Delegation Protocol be generally deployed and used across Services, we will want constraints to support interoperability. For example, if the User Interface used to delegate authority for the Organization is an Active Directory-type application that maps Service Access to People, then supported Services will have to express the offered Capabilities and understand the presented Delegations in standard ways.

Harri Honko (Tampere University of Technology) has implemented this mechanism using Hyperledger Indy and standard W3C Credentials in a slightly different use case:

- A Electric Utility Service stores data about a user in their system - in this case Electricity usage
- A user wants to provide an Application limited access to their data on the Service
- The user Delegates Authority to the Application via a W3C Verifiable Credential

- The application presents that Delegation to the Service and is given access to an API to access the user's data.

A full presentation on Harri's use case and implementation can be found here: https://docs.google.com/presentation/d/1aeWAexMmD0rBNAmS_mNvZwf_0xHVfxD4j7N6LRI5SGg/edit#slide=id.g373a1094a5_0_0
As well, here is a link to the implemented code: https://github.com/TrustNetFI/authcred-demo

The following is a W3C Standard version of the Credential that was used in this project:


```
{
  "@context": [
      "https://w3id.org/credentials/v1",
      "https://example.com/credentials/v1",
      "https://w3id.org/security/v1"
  ],
  "type": [
      "Credential",
      "DelegatedAuthorityCredential",
      "CustomerIdentityCredential"
  ],
  "claim": {
      "id": "TaVE1pAaummu3wfbWtVbyu",
      "claim": {
      "authorizedscopes": ["electricity_metering_data",”read_access”],
      "customerid": "192873465"
      }
  },
  "issuer": "VJkTdbQZTRnJneZAR245n6",
  "issued": "2018-04-04",
  "credentialStatus": {
      "revocation": "http://example.com/revocation/c73fcffb-5cb0-4bc4-
b97c-816048166cbf"
  },
  "signature": {
      "type": "Ed25519Signature2018",
      "creator": "VJkTdbQZTRnJneZAR245n6#key1",
      "created": "2018-04-04T12:18:44.202Z",
      "domain": null,
      "nonce": "c73fcffb-5cb0-4bc4-b97c-816048166cbf",
      "signatureValue":
"SeZ0fqLYteuVBa7WI27dQcJPy0lS0CC3vuyvqsa9AqXDUVfX91hKSwgpwUnn9l7l0EBBcPz6
CqDkI1gzmAfMBw=="
  }
}
```


Honko's approach is a vast improvement over, for example, the current Mint cloud service that operates by getting your "normal" Banking Credentials (userID and Password) to download, analyze and present your financial information. Those credentials give Mint and comparable services full access to your Banking capabilities - download and create transactions - vs. only the download transaction history needed to operate the Mint service.

What is your problem?

Thursday 5K
Convener: Chris Buchanan
Note Taker: Chris Buchanan

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

This session was created to collect potential research project ideas that would have an impact in the identity space. Some brought ideas that were not specifically identity but most were.

The projects that would be most likely to get funded would have the following properties:
1. Nobody other than MITRE (https://mitre.org) is better suited to do the work
2. Not in competition with a for-profit company
3. Easily transitioned to someone else for production and/or operational use
4. Research increments of one year or less

Below is a list of people who participated and the ideas they proposed:

Name	Idea
John Philpin	Battery based home power system for Puerto Rico
Peter Simpson	Portable retinal scanner for patient ID
Table Discussion	Private key recovery
Sam Weiler	Permissionless Delegation under FIDO2
Sam Smith	FIPS certification of Libsodium encryption library
Sam Smith	Key Recovery process (non-multiparty interactive)
Sam Smith	Key rotation using prerotation which prevents inherited compromise
Sam Smith	Build a library that supports decentralized autonomic data for data streaming applications.
Sam Smith	Advanced crypto into open source software. Libraires that would include things like collective signatures and blinded signatures.
Adrian Gropper	Security analysis of the self-sovereign medical record technology stack (Harvey Reed)
Michael Boyd	Self-Sovereign education for understanding how it's good for you.

Additional people left a business card indicating that they should be contacted later.

The intention is to ask the community to endorse their favorite ideas and allow Chris to carry those endorsements forward into the competition phase.

For anyone who missed it, you can send your topic to Chris Buchanan (cjb@mitre.org).

Some AV Recorded Notes by Josh Fairhead

There are recordings here for a variety of sessions -
https://www.youtube.com/watch?v=q-jedgdSFYQ&list=PL-sU4FCUDRCcyPnURf1NsmCQK5hfb2cPg

Photo Credit @TranSendX Apr 3 Internet Identity Workshop **#iiw**

All of the attendees/participants, in photo above, created the agenda for Day 3 of #IIW, in photo below, in a little over 30 minutes!

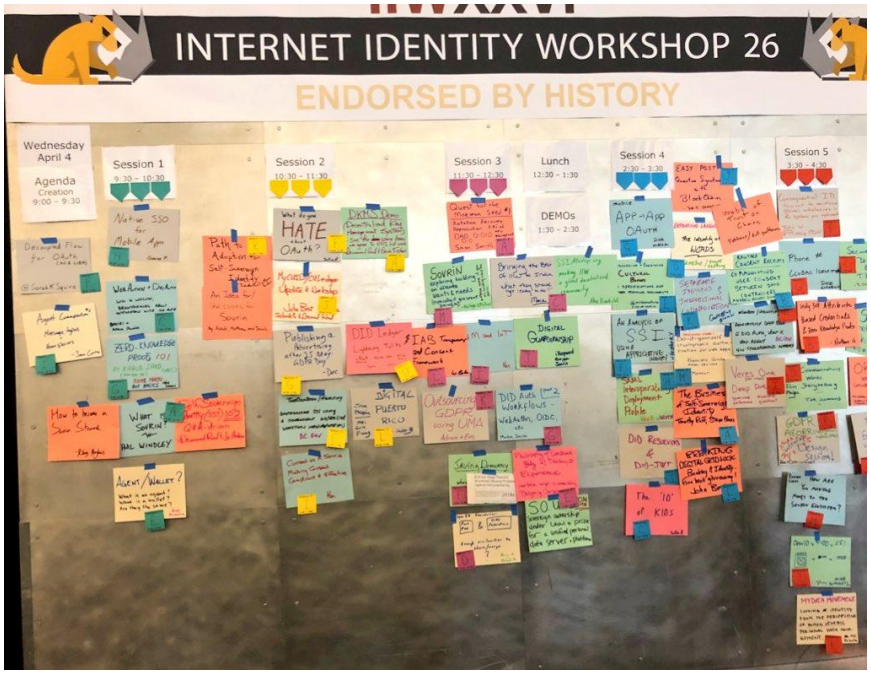


Photo Credit @windley Apr 4
Now this is an agenda wall! Lots of sessions today at #iiw

Demo Hour

IIWXXVI #26 Community Sharing / DEMO LIST
Wednesday April 4, 2018

Thanks to our Demo Hour Sponsor

1. **Danube Tech - DID Resolver and DID Auth:** Markus Sabadello
   URL: https://github.com/decentralized-identity/universal-resolver/
   Decentralized Identifiers (DIDs) are the base layer of new decentralized identity protocols. We show how they work and how they can be used for authentication (DID Auth).

2. **VERES One - Get a Decentralized Identifier on the Veres One Blockchain:** Manu Sporny
   URL: https://veres.one/
   We will demonstrate how to generate a Veres One Decentralized Identifier (DID), register it with the blockchain, and update its related DID document. A DID can be registered and its DID Document updated by performing a proof-of-work or by using an Accelerator.

3. **digi.me – current PC/Mac, iOS/Android version application:** Jim Pasquale & Julian Ranger
   URL: http://digi.me for product & http://digi.me/video for vision
   Demo will show what users can do when they own and are in the driver's seat of their own data on their own devices(s). More privacy through our new Consent Access feature, using two new external apps providing social analytics and monetary insight from financial data inside their library.

4. **JLINC Labs - CRM to VRM:** John Wunderlich
   URL: http://www.jlinclabs.com
   The paradigm of the Vendor controlling all of the customer's information is inverted when you implement an Information Sharing Agreement and the software to enable the Customer to control their information inside the Vendors Salesforce instance and have dynamic control over their marketing consents.

5. **Technical Associates Group, LLC - Real-IT:** an awareness space related to expanding the discussion, recognition and management of our presence the non-physical digital environment, which reflects into our physical environment: Jeff Orgel
   URL: https://www.youtube.com/watch?v=VECmh2rpt70 .
   Who's Wearing the Collar? Developing language allowing us to put handles on thoughts with words regarding base human nature & how the impact of IT forces affects our behavior. The idea that Real-IT, our relationship choices w/IT, reflects into our Reality. What is your Real-IT?!

6. **Pomcor JavaScript Cryptographic Library (PJCL) Do-it-yourself cryptographic authentication with PJCL:** Karen Lewison and Francisco Corella
   URL: https://pomcor.com/pjcl/
   PJCL is a JavaScript library that makes it trivial to implement password-free cryptographic authentication, avoiding phishing attacks and password-compromise notification requirements under GDPR and US regulations. A sample web app will be demoed and its source code provided.

7. **Evernym:** Timothy Ruff, Dale Jones
   URL: www.evernym.com
   Witness the first cryptographically verifiable credentials exchange that's truly peer-to peer (no IDP or other intermediary). Built on open-sourced Sovrin, Evernym's VCX establishes trust between people, organizations, and things, while enhancing privacy.

8. **DID Whisper pastebin:** Dmitri Zagidulin
   URL: https://github.com/digitalbazaar/did-whisper
   A quick demo of an encrypted pastebin service using Veres One DID Documents, a way to send private encrypted messages using recipients' public DIDs.

9. **Blockstack Sign-in & Storage using Graphite & the Blockstack Browser :** Jack Zampolin
   URL: https://app.graphitedocs.com/ and https://browser.blockstack.org/
   Graphite is a Google Docs replacement where you own the data, but don't give up any of the collaboration or sharing features.

10. **Gluu Gateway:** Mike Schwartz
    URL: https://gluu.org
    Gluu Gateway is a new linux package distribution of Kong and two Gluu plugins. The first plugin enables your clients to use any OAuth authorization server for client authentication. The second enables you to use UMA to protect your API's, turning Kong into an UMA resource server!

11. **Building a Sovrin-linked Public Permissionless Ledger for Data Analytics:** Paul Knowles
    URL: https://we.tl/BWtMWMxRZk
    Introducing a new ledger and data warehousing model that would enable developers to build statistical algorithms and analytics applications on pre-verified data without compromising either GDPR compliance or self-sovereign identity. The future of data analytics.

12. **Government of British Columbia - Permitify Proof of Concept:** Stephen Curran, John Jordan
    Permitify demonstrates the use of Verifiable Credentials to simplify complex processes - government permitting - while improving data quality. Permitify provides dynamic recipes to guide business users looking to open businesses (e.g. "Open a Restaurant in Vancouver").

13. **Interplanetary identifiers:** Jonathan Holt
    URL: Https://www.github.com/jonnycrunch/ipid
    Implementation of DID method on top of IPFS (interplanetary File System)

14. **Yubikey - FIDO has Browsers:** Chris Streeks, Solutions Engineer; Terry Shofner Yubico Fellow
    URL: https://www.yubico.com/products/yubikey-hardware
    See FIDO U2F standards working in browsers from Firefox (Nightly) and Google. And let's talk about what's new! The W3C's Web AuthN specification is maturing and we are aiming at standardizing hardware-backed strong authentication across browser clients. And don't forget we also support open standards such as PIV, OATH, OpenPGP and FIDO U2F.

15. **The_ABACUS: Jacob Siebach**
    No URL yet - A new attribute-based access control system.

The IIWXXVI Demo List can also be found here
http://iiw.idcommons.net/IIW_26_Demo%27s

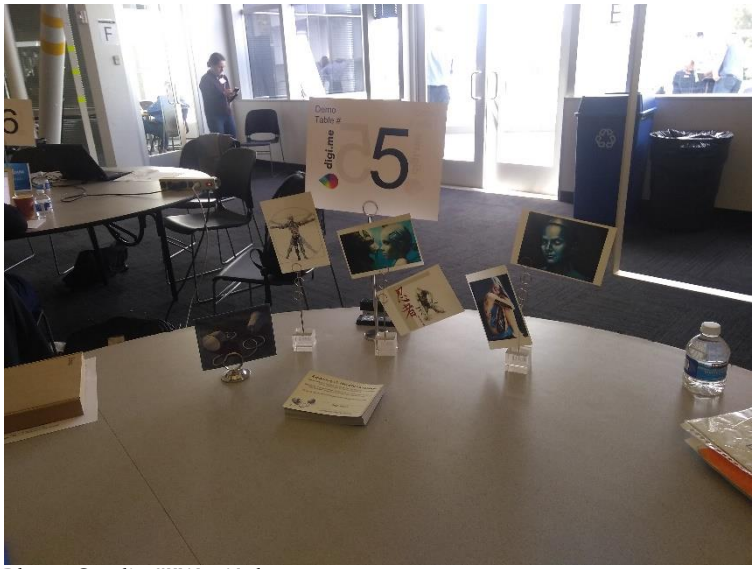


Photo Credit #IIW @Nobantu

Photo Credit #IIW @Nobantu

Closing Circle Reflections

Wednesday Closing Session

Shared by attendee Samantha Matthews. Upon the request of many in the group here is the speech I delivered the end of day on Wednesday.

"I've had a really challenging time being here today. In fact, I spent the afternoon in my car in the parking lot trying to figure out how to approach any of you. You're all talking at a level that you assume is common and it's not. Identity is a common person problem. If identity is not a common person problem then common people are the commodity.

There is a difference between knowing something and understanding something. There is a fundamental difference between access to information and access to insight.

We've allowed for information overwhelm, we've allowed for disinformation overwhelm, as a common practice, born from this very city. We have allowed for watered down words and veiled intent.
while the tools of insight, what makes the whole thing tick, lay in the hands of a few.

This insight sadly has been gained through platforms that in the most bizarre and blatant way, make all of their money by delivering an emotional state to serve you ads in. Privacy laws in the age of big data in ad tech have built a new kind of intelligence. The masses can be wired at their pleasure centers like atomic donkeys.

Psychographics, engineered consent, are only in their infancy.
You're welcome to continue with a top-down approach to identify, you're welcome to work on all the different kinds of persistent IDs attached to users that exist in that system. It will be great that you've all been building these types of identities and ledgers. I'm not comfortable, however, with the severe lack of user-centric conversations. Users being us, people, humans.

We cannot let an idea as powerful as Self Sovereign Identity become a buzzword. We cannot dilute the meaning or its power. Data sovereignty and human rights laws will be achieved around and in spite of the Self Sovereign Identity movement, but it would make more sense if this community was the groundswell of leaders guiding the way.

I humbly ask that you continue your great work, but that you spend some time contemplating what a world would look like if people interacted with their own data layer from their sovereign server out.
They could download programs for self-insight, they could train AI's that help them exercise. They could gain insight into the exact combination of activities and imagery they need to feel better.

Imagine if instead of Apple and Microsoft collecting all this data on your kids and selling back tablets and games that hold their attention, we collect our own data on our kids. Perhaps a mother sees that her child's heart rate entered a stress state when the teacher mentioned fractions. Mom can download a fun baking learning lesson for that exact fraction level and make it into a game at home together. That is parenting!
Imagine having your own body avatar rigged to a dance teacher that can lead or embody you like a ghost and

show you where to move? None of these things will be built unless we help people grow their own kind of intelligence. We are moving into spatial computing, rapidly. That means that we'll be able to see whatever we want to see or whatever companies want us to see. We can't fix all the people, but we can give them the tools to fix themselves and reflect on their own self-insight before we troll ourselves to war, be it global or civil.

Our online identities are inextricably entwined with our real-world bodies, minds and behaviours, and the data that we generate every moment of the day tells as much about us as individuals as a photo describes our appearance. More so even, since this data can be interpreted in such detail as to predict behaviour and create models of our consciousness.

If I may impart anything to you, let it not be my frustration, I am so impressed with the work all of you do. Please let me impart to you the urgency. This psychographic profiling, the tensions being created all just to keep us engaged with a machine.
IT WILL NOT END WELL.

We have to quantify, acknowledge, educate everyone at every level what their data can mean to them and what it means to them now if things continue on this path.

I am launching this prize as the fundamental enforcer and gatekeeper of digital human data rights. There is already a bot that will legally ping and collect your data from all the platforms affected by GDPR. Each person in Europe has been given an oil field. I am building the very first drilling rig. The magic people create with their data will be a new enlightenment. I would like North America to be a part of that enlightenment. We need to study identity from a human rights perspective, immediately.

I humbly ask that you join me on this mission to create the biggest prize in the world. Because no matter what the final purse becomes, this is the prize where everyone wins."

My current strategy map for S.O.U.L is here. It's a work in progress, I need lots of help filling in the meat but the bare bones plan is there. Money is pledged, a team is growing. I am looking for the brilliant minds of this gathering to partner with me in any way they can. For more detailed and digestible media and to stay informed please enter your email address on the site www.soulprize.global

Thursday Closing Session

Comments scribed by Scott Mace – Thank you Scott!

Seems to be a lot of forward movement in IIW.

≈ This is my first IIW. It was really cool on day 3 to be able to hold a session. A nice format.

≈ This is my first IIW. Really fascinating. Completely thrilled. Looking at the openness and flexibility here, a really fun thing.

- ≈ I have a friend in Sausalito who is a poet. He specializes in box poems. They are ten lines long with ten syllables in each line. Reads poem. (see below for poem)

- ≈ Bill Wendell is forming a real estate WG and will do a Webinar next week.

- ≈ As far as next steps, if any of you want to continue working on these ideas, W3C credentials community group meets Wednesday 9am Pacific plus 8am Pacific verifiable credentials community group

- ≈ Drummond: My favorite tweet I sent out over this IIW was a photo from the back of the room. I've never seen so many adults fascinated by math in my entire life. [Zero proof] Kazooie (??) oozed such credibility and such warmth.

- ≈ Doc: Linux Journal doesn't have a limit on length. Would love podcasts, open source-y, Linux-y story.

- ≈ Kaliya: Diversity Caucus now has a mailing list.

- ≈ As people who are designing the future, maybe we can have a place to share these use cases. Let's make that happen.

- ≈ I remember thinking, I've been to a bunch of IIW's, I was looking at a bunch of new people, thought, they have no idea what's coming. It was really neat to have that thought. This is such a wonderful community and I am grateful to those who make it happen.

- ≈ Yogi: This is my first IIW. I had no idea. I wanted to say thank you everybody.

A Box Poem - 10 lines, each of 10 syllables

This one by Jim Woessner / Read aloud by John Philipin

By the numbers there's my driver's license,
car registration, license plate, zip code,
various accounts, street address, birthdate
home, work, and cell phones, passport, credit cards
debit cards, PINs, social security
frequent fliers, internet passwords, stocks
checking, HMO, IRA, museums
library card, land and enneagram.
I know it's a lot to remember, but
thank god I finally know who I am.

The book can be bought on Amazon here.
More of his work on Amazon here.
One of many posts I have written in many places about my friend Jim Woessner

IIWXXIV #26 Photos

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

It is Doc's practice to take time during every IIW to sit in the opening/closing circle or wander the workshop to take candid photos of attendees and white boards and the general goings on. Here are links to his great photos from IIW 26

https://www.flickr.com/photos/docsearls/sets/72157694778829834

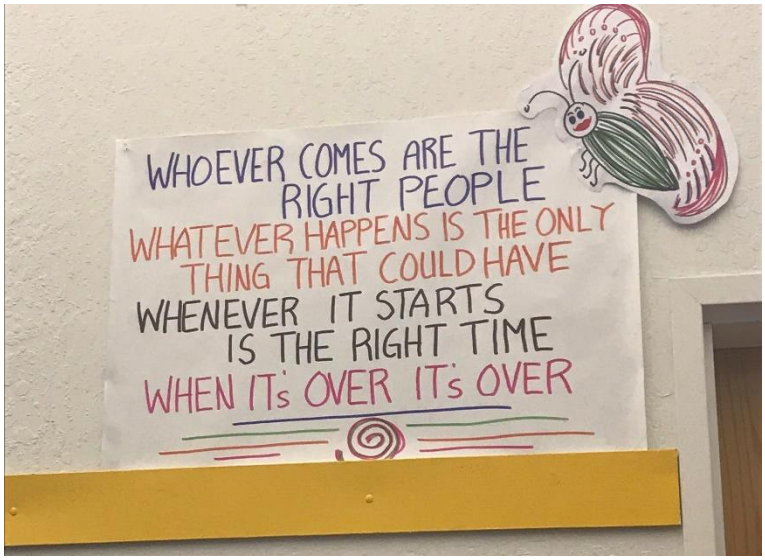


Photo credit #IIW Elizabeth M. @hackylawyER Apr 3
In line with my general life philosophy #IIW #privacy #identity

Photo credit @AdamMGunther
Love these guiding principals for a great (un)conference **#iiw**

IIW is an 'Open Space' unConference, ***(a format for highly effective conferences in complex areas) that leverages the power of self-organizing through fully engaging the 4 Principles and 1 Law of Open Space Technology as outlined by Harrison Owen in 1982 or thereabouts.***

Post Event Blog Posts and Articles

From Francisco C @ Pomcore – Easy Password Free Crypotographic Authentication for Web Applications

https://pomcor.com/2018/04/13/easy-password-free-cryptographic-authentication-for-web-applications/

From @identitywoman in Coindesk – There's An Alternative to Facebook Called Self-Sovereign Identity

https://www.coindesk.com/theres-alternative-facebook-called-self-sovereign-identity/

From Doc Searls in Kupplinger Cole Blog – Some Perspective on Self-Sovereign Identity

https://www.kuppingercole.com/blog/guest/some-perspective-on-self-sovereign-identity

From Mike Schwartz / @nynymike – SSO v. SSI

https://www.gluu.org/blog/sso-v-ssi/#.Ws5D783bBUg.twitter

NYT Article about Doc Searls & VRM Day – After Cambridge Analytica, Privacy Experts Get to Say 'I Told You So'

https://www.nytimes.com/2018/04/12/technology/privacy-researchers-facebook.html

Photo credit #IIW @Nobantu /A day after ~ but this photo is a great representation of #IIW ~ leave your logo & your baggage at the door for a most rich and productive time! #openspacetech #unconference @idworkshop

See you October 23-25, 2018

for

IIWXXVIII

The 27th Internet Identity Workshop

www.InternetIdentityWorkshop.com