IIWXXVII

INTERNET IDENTITY WORKSHOP 27

ENDORSED BY HISTORY

Book of Proceedings

www.internetidentityworkshop.com

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

Notes in this book can also be found online at
http://iiw.idcommons.net/IIW_27_Session_Notes

Photo credit #IIW @Nobantu

October 23, 24 & 25, 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

REGISTER FOR IIW XXVIII
April 30 - May 1,2,2019
HERE: https://iiw28.eventbrite.com



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 14th year and is Co-produced by Kaliya Hamlin, Phil Windley and Heidi Nobantu Saul. IIWXXVIII (#28) will be April 30 - May2, 2019 in Mountain View, California at the Computer History Museum.

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

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

Upcoming IIW Events in Mountain View California

IIWXXVIII #28
April 30 May1 & 2, 2019
REGISTER HERE

IIWXXVII #29
Oct 1, 2, & 3 2019

IIW 27 Session Topics / Agenda Creation

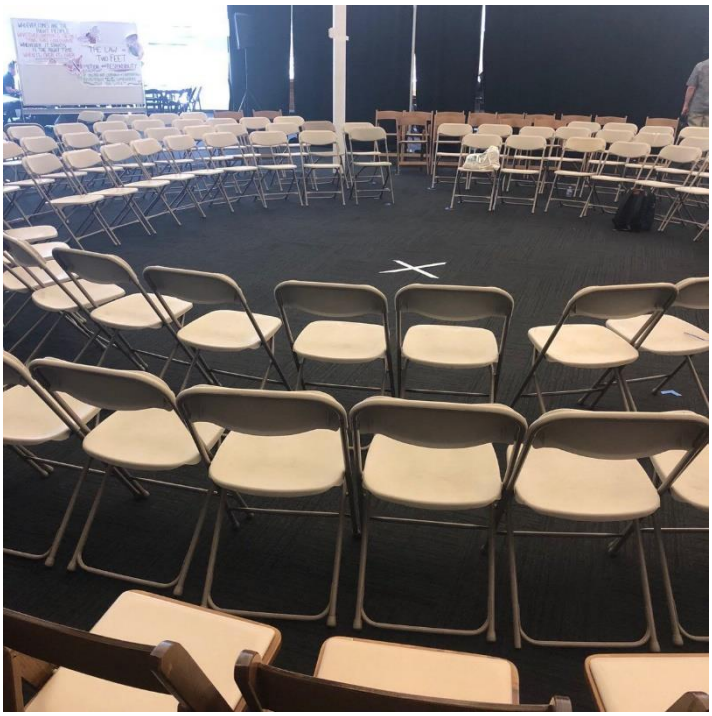


PHOTO CREDIT

Beyond Bridges @jgphilpin Oct 24

It might look empty now … but that's because everyone is in session. Come back in 90 minutes or so.

118 distinct sessions were called and held over 3 Days. We received notes, slide decks and/or white board shots for 102 of these sessions.

Thank you each person who took and submitted notes for sessions ~ You created this Book of Proceedings!

Tuesday October 23, 2108

Session 1
1A/Centralized + Decentralized Identity Standards OAuth + DID w/Code!
1B/Introduction to OAuth2 (101 Session)
1C/IIW – LAB-in-a-BOX for Communities to Be In Living Experiments
1D/Blockchain TLD's
1E/CULedger is Working to Improve Member's Experience *Better UX *Lower Fraud – We See FB Added Value BUT They Were Creepy – Help Us Get It Right and Natural
1F/An Interactive Sovrin Network Demo
1I/Machine Learning/Computer Vision & Internet Identity

Session 2
2A/Sovrin Credentils and IoT
2B/Intro to OpenID Connect (101 Session)
2C/Blockchain 101 + Why You SEE BC Identity Projects
2D/How Can We Enable/Support Individuals to Grow/Create Their Own Credentials
2E/Identity and Trust in Healthcare
2F/ FIDO FAQ
2G/Domain Specific Trust Governance Frameworks Healthcare Worker Identity + Credentialing
2H/Device Bindings & Session Control w/ ADC/OAuth (ingredients for zero-trust)
2I/Review W3C User Consent & Permission
2J/Guardianship – When Users Can't Manage Their Digital Wallet

Session 3
3A/A Catalyst For Trusted Digital Ecosystems
3B/Intro to User Managed Access (101 Session)

3C/Impact of Apple ITP2 On OIDC & SPA
3D/ Decentralized Kay Management
3F/ World-Scale DID Methods On Top The Blockchains/Ledgers of Today
3G/How Do We Bring "Tribal" (group) Identity Online With Us?
3H/Cyber Security Data Breaches Fight With AI
3I/Australia's Tsunami of Data Laws – ID, Open Data, Cyber Front Doors. What + Why
3J/Sovrin Stewareds – Feedback Onsite

Session 4
4A/How THEY Consent to OUR Terms
4B/Introduction to FIDO (101 Session)
4C/ We Need a Working IdP Discovery Mechanism (for RISC, Fast Fed, and more)
4D/DID Resolution + Registration
4E/Question re DID Standard ~ What is with the changes from V1 to now, including how verifiable credentials claims attest as work?
4F/Deep Dive on 'Identity Hubs' Encrypted Personal Datastores for All Types of Identity Data, and a Platform for Decentralized Apps
4G/ How Do We Do Digital Consent Forms & Share As Claims W/Multiple Parties?
4H/A Standardized Information Governance Label
4K/Design an Undergraduate Blockchain Course

Session 5
5A/A DID For Everything!
5B/Self-Sovereign Identity 101 (101 Session)
5C/ Unintentional Consequences of What We Build
5D/MyData @ IIW
5E/Personal "AI" / Self-Sovereign Identity & Personal, Private Internet
5F/Sovrin AMA
5G/What Questions Should I Ask Myself Before Clicking The 'I Accept' Button?
5H/ OIDC FED
5K/ The – ABACUS: A New Approach to Authorization

Wednesday October 24, 2108

Session 1
1A/Beyond OAuth: Transactional Authz
1B/Verifiable Credentials 101 (How the Sovrin Demo Works) & Concept Map of Verifiable Credential Specification
1F/HL Indy Ref Agent – Sovrin Demo + Future Work
1G/SSI in Europe – Getting To a SSI Agenda With Politiacal Backing #SSIpaper
1I/"Moon Coin" Tying the Digital World to the Physical (a discussion) & SSI is Coming Here
1K/Signed Data (JSON – LD vs JWTS or something else)

Session 2
2A/7 Myths of SSI
2B/ Identity & World Bank Funding. 1Billion in Loans to African Countries for Aadhaar Like Systems??? Could this go to SSI Systems?
2C/Usability for Developers Applying Lessons from TLS to the Blockchain
2D/A Interactive Sovrin Demo II
2F/PRIVACYCHAIN: A blockchain-based system for consent management for data supply chains.
2G/Fixing Enterprise IAM – Automation – Self-Service – Security – Rapid Adoption

2H/CYBORG Future of ID
2I/OAuth for Single-Page Apps (javascript apps) Best Practices Recommendations
2J/GS1 Digital Link: Defining Digital Identity for 100's Millions of Every Day Things
Session 3
3A/Best Practice for Managing Tokens or How to Avoid Being the Next Victim After FaceBook
3B/Digital Life: Stage 1 – Surveillance Capitalism + Re-engineering Humanity
3C/Identity in the Academy
3D/Continuous Access (long-lived session update sync across clients)
3F/ DID Web API's Including: Contexts, Operation classes, Identity Hub
3G/Decentralized Ecosystem Governance with Blockchain
3H/M.E.S.H. Managed Ecosystem Superdistributed Hashes

Session 4
4A/Self Sovereign Identity Technology Demo and Ask Me Anything
4B/Sovrin AMA – Part II
4C/Data Transfer Project – Universal Data Portability for All
4D/Blockchain TLD's, Identity Key Management
4E/Consumer IOT – A Perspective of Retailers, Brands, and Manufacturers
4G/ the HumanOS As An Identity Generator ~ Implications on the Digital Domain
4F/Part Deux! Permitify – dFlow in Action
4H/Identity Proofing w/Open ID
4I/ How To Build –[Context-Aware] – Systems to Avoid [Context Breaches] in a World of [Intelligent Agents, IOT and AI]
4J/Identity, Ethics and Digital Inclusion – the IEEE DITA Program
4K/ Civic AMA – Product + Partners
4L/Subjective vs Objective Identity

Session 5
5A/Seed Quest + Didery – 3-D Game Mnemonic DID Keystore
5B/Decentralize The Internet With a Simple Link
5D/The Identity.com Eco-System – Introduction + AMA
5E/Manifold – Give Your Things an Identifier
5F/Id(enity) Relationship Management, What, Why, Where
5G/Overlays 101
5H/Making OAuth Work on the Open Web
5I/Data Store Interop?? How Do We Bridge Private Island of Users?
5J/What's In Your Wallet? + Who Is In Your Wallet?

Thursday October 25, 2018

Session 1
1B/OAuth Security 4 Dummies
1C/Canonizer! Distributed Governance ~ if we can establish indemnity
1F/ ME2B: Creating a Non-Surveillance Capitalism Market
1G/ DIDAuth + Obj. Cap.
1H/ Bliss & Emptyness ~ A Buddhist Approach to Identity
1I/What's In It For Governments? (Potential Use Cases)
1J/Overlays 101

Session 2
2B/Dual Tokenomics – Virtous Behavior – Mechanism Design – Fixing the Broken Single Token Model
2F/MyAI – Gaining Insight Into Your Own Data
2G/Consent Management – Receipts Practices Standards
2I/How Should a Blockchain Social Network be Moving on Digital Identity Now?

Session 3
3B/Sovrin Interactive Demo III
3C/Blockchain Myths & FAQ
3F/What Every Identity Professional Should Know ~ An Introduction to IDPro
3G/The Orgbook – Watch Us Create A Concept Map!
3J/Ask A Millennial About Identity
3K/W3C Strong Auth & Identity Workshop Dec 10 – 11 ~ Ideas + Design of Workshop

Session 4
4B/R&E Identity – Where Do We Go Next?
4C/LifeScope Demo & AMA
4D/Defining the SSI OS
4F/ The Great Dalmuti ~ What we should consider about Identity as Learned from a card game –
4G/When Standards Don't Suffice

Session 5
5B/How Data Analytics Will Change Thanks to SSI
5C/LIfeScope Demo & AMA --- continued
5D/Democracy.Earth – Exclusive Announcement
5F/Vegan Atheist Crossfitter ~ Which do you mention first?
5G/IIW Wikipedia Page! Help Us Strategize to Get One Finally
5H/Defining SSI Layers Workshop

Tuesday October 23

Centralized & Decentralized Identity Standards OAuth + DID w/Code!

Day/Session: Tuesday 1A
Convener: Orie Steele
Notes-taker(s): Orie Steele

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

Two links to presentation slides:
https://twitter.com/OR13b/status/1054813581735149568

https://docs.google.com/presentation/d/1xsiQ6ndb33kzhF8kl1cF_EpWxWmNFwhd0o3KExe6eSw/edit

We talked about OpenID Connect / OAuth Centralized Identity Providers, User Directories and How to go from a Decentralized Identity to a JWT issued by a centralized OAuth provider.

We also talked about blockchains, and how they relate to decentralized identity and GDPR and the right to be forgotten.

We talked about PGP and tradeoffs between reputation and privacy, and the tension between the two.

Key insights included that we (community) seem to believe that deleting an encryption key is equivalent to deleting data. OAuth can be decentralized, but it requires users to run their own servers...

Introduction to OAuth2 (101 Session)

Wednesday 1B
Convener: Justin Richer
Notes-taker(s): Daniel Johnson

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

What is OAuth 2.0?

- Delegation protocol

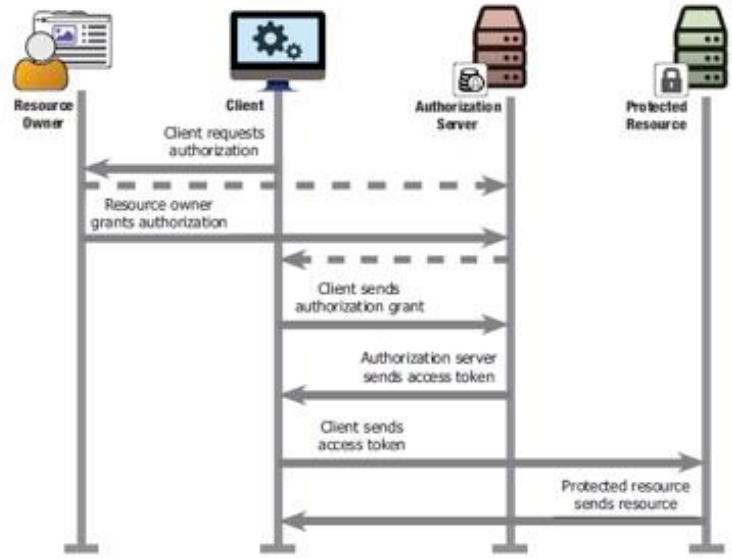


Figure 1.8 The OAuth process, at a high level

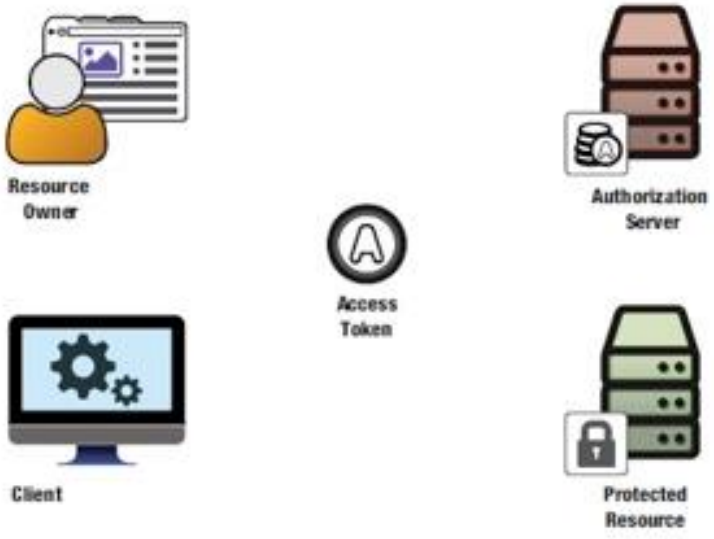


Figure 2.9 Major components of the OAuth 2.0 protocol

Resource Owner

- Person/entity/policy/server with access to a web browser or API
- The right to delegate access to API
- Delegating access to the resource
    - Works with anything accessible on the web

Shares to client (piece of software access protective resource API) mobile app, server, javascript within web browser

- Could be native or mobile

Trying to solve the problem of giving away access insecurely

- Steal keys user it to log in as someone else
    - Only works if credentials can be stolen
    - Men in the middle attack (taking something someone used to prove identity and using it)
- Ask for keys to share across apps, websites, etc
    - Ask for resource owner credentials and reply them to protected resource
        - Most people willingly give up info to share across resources and make life easier
- What if instead of personal keys, there is a universal key (API key) to unlock anything (like an axe to break down the door and gain access)
- Works really well in closed enterprise access

LDAP server with API Keys

Problems

- Client must be completely trusted to be impersonating user
    - Does not work across security boundaries
- Users may not be aware any share is happening

Service-Specific credentials

- Special password (or token) only accessed by user
- Doesn't leak user's password
- Security great, usability is crap
    - More credentials to manage and lose
    - User transfers credential to app (usually by hand)

Automating the Process-Auth server dedicated to managing service specific tokens

- Tokens given to client
- Authenticates resource owners (users)
- Authenticates clients
- Manages authorization

OAuth Access Token

- Represents delegation
- Issues by auth server
- Used by client (opaque to client)
- Consumed by protect resource
- Tokens can be many formats (it doesn't matter)

We've all used it! Even when we don't know it! (android phones, spotify, steam…)

Brief History OAuth 2.0

- Circa 2006

- HTTP password authentication common for API access
    - "Give me your password"
- Internet companies have proprietary solutions for delegated access
    - BBAuth, AuthSub, a few others

OpenID comes along(no password)
Problem
- 2 smaller sites want to connect their APIs for their users
- Both use OpenID for users
    - No username/password to pass
- Neither wants to use a proprietary solution

New Standard born
- OAuth 1.0 published independently
    - No formal standard, people just use it
- Session fixation attack found and fixed (intercept of information)
    - New version called OAuth1.0a
- Community document is standard RFC5849 in IETF

People Use
- OAuth1.0a solves major pain points for many people in standard and understandable ways
- Google, Yahoo, and others replace their solutions with new standards

People Abuse
- People decide to start using OAuth for off-label cases
    - Native apps
    - No use in loop
    - Distributed authorization systems

Version 2.0 framework
- Modulization concepts
    - Separated previously conflated components
    - Added explicit extensibility points
    - Removed pain points of implementations
    - Standardized in RFC6749 and RFC6750

What does this mean?
- Not a single protocol
- Meant to be building blocks to use it for your own needs
- Different ways to mix and blend ingredients
- Not a single standard, it's a set of standards for different use cases
    - Don't use implicit tokens with native apps causes vulnerabilities

What OAuth isn't
- Not defined outside of HTTP
    - Core protocol defined only for HTTP
    - Relies on TLS for securing messages
    - There are efforts to use OAuth over non HTTP protocols
        - GSSAPI
        - OoAP
- Not an authentication protocol
    - Relies on authentication in several places
        - Client authentication to token endpoint
        - Resource owner auth to auth points

        - Doesn't communicate anything about user
        - However, authentication protocols can be built using
            - Auth (OpenID connect)
    - No user to user delegation
        - Allows users to delegate
    - No authorization processing
        - Tokens represent scopes and other auth info
        - Processing info is up to resource server
    - No token format
        - Opaque to client
        - Needs to be issued by auth server and understood by resource server, but free to use however they want
        - JSON web tokens (JWT) provide a useful common form
    - No cryptographic methods
        - Core OAuth relies on TLS for protecting info in transit
        - JSON
    - Not a single protocol

The authorization code flow-Canonical OAuth 2.0 transaction

Back Channel (no user involved)

- Back channel uses direct HTTP connections between components, the browser is not involved

Front Channel

- Front channel uses HTTP redirects through the web browser, no direct connections

Authorization Code

Step 1: add queries, get request

Step 2: Resource owner authenticates to the authorization server

Step 3: Resource owner authorizes client (OAuth allows to ask user allows cross domain authorization)

Step 4: Authorization server redirects resource owner back to the client with an authorization code

Step 5: Client sends the authorization code to the authorization server's token endpointclient authenticates using its own credentials

Step 6: Authorization server issues an OAuth access token to the client

Step 7: Client accesses the protected resource using the access token

Tuple of token

- Resource owner approved
- Client that requested
- Access rights delegated

Interpreting token

- Shared data source
- Pack info in token to parse and interpret (JSON Token)
- Online lookup system

Client Credentials Flow (formally two-legged OAuth in 1.0)

- Has no user or web browser making request
- Autonomous client
- Not acting on behalf of a user

Implicit flow

- User and client are one unit
    - Implicit front type uses only the front channel since client is inside the browser

Resource owner password flow

- Don't use!
    - Don't pass passwords… just don't do it

PKCE: sending the challenge

- Client generates code verifier and challenge (hashed secret passed from user to server), includes challenge in front-channel request to the auth server

PKCE: sending the verifier

- API key, pass, and hashed secret passed from client to auth server)

Unifying Challenge

- Regenerates challenge from verifier and compares it to previously sent challenge

Additional Notes: Jin Wen

What is OAuth means to you:

- It is a delegation protocol, not authorization

the following is a commonly mis-understood terminology: Client in OAuth.
A client: piece of software accessing resource on behalf of resource owner
Problems with universal keys: one key to unlock them all!
Problem of service-specific credential:

- Yet another credential for users to manager and manage to lose
- has to transfer the credential to the application, by hand

History of OAuth 2.0:
The problem started: Two smaller sites want to connect their APIs for their users starting at 2006
earlier OAuth 1.0 is RFC5849
session fixation attack change it to OAuth 1.0a
Cons of 1.0a:

- Native app
- No user in the loop
- Distributed authorization systems (RSA signing)

Version 2.0: The framework

- Modularized concepts
- Separeted previously conflated components
- Added explicit extensibility points
- Removed pain points of implementers
- Standardized in RFC6749

Killer pain in OAuth 2.0: using implicit flow in native app -- a big security flaw

What OAuth 2.0 is NOT:

- Not defined outside HTTP
- Relies on TLS for securing messages
- There are efforts to use
- NOT an authentication protocol --> OpenID Connect is,
- NOT an person to person authorization protocol --> see UMA
- No token format: JSON Web Tokens (JWT) provide a useful common format
- Token is opaque to the client
- No cryptographic methods --> see JOSE

The Authorization Code Flow: deep dive
Resource two type of comm channel: Back Channel and Front Channel
Front Channel: uses HTTP redirects through the web browser, no direct connections Back channel: client communicate with Auth Server

LAB-in-a-BOX for Communities to Be In Living Experiments

Day/Session: Tuesday 1C
Convener: Mei Lin Fung
Notes-taker(s): Scott Mace

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

Mike Graglia, New America – Registries
Bob Craig, CIO, 100-year-old law firm
Sherry Stein, CETA Lab,
Jess Harrison, Stop Child Traffic dot org.
Bruce Conrad, Pico Labs, BYU. We have to remember hundreds of passwords easy for us to remember
Sari, Stenfors, working on digital divide & disabled people. We have been thinking about a lab, bring these future concepts to people today, especially different types of people.
John
Chris Mellon, New America – how SSI can help us to crowdsource a lot of data gathering
Mike – Chris has recently been to Puerto Rico
Mei Lin – People centered Internet, cofounded with Vint Cerf. Local communities have no idea who is doing what. Trading posts help people discover the frontier. The idea of Lab in a Box, how can we help the trading posts be more effective? Even an initial set of small checklists or principles, what would that be?

- What we want, what we fear
- Problem statement
- Proof of concept
- Field test
- KPIs / criteria
- Duration
- Start/finish
- Assess performance
- Feedback / revise
- Scale
- The problem statement needs to be ratified with the community before you start
- Focus on children
- Field test in community centers, schools, libraries

Mike – SSI, credentials go in my wallet. In real life, how do you use your DID or public key to assert things to vote for resource allocations, maybe using a device to confirm they are actually on the island of Puerto Rico. A way to push credentials down but get opinions back in a timeline that matters, rather than paying a consultant for insights months later

Chris – Mediation between individuals and governments, to let adjudication counsels evaluate claims
Can community self-adjudicate? Conflict

Jess – issue of trust. How can agencies build and keep trust?
What is an appropriate verification process?

Mike – Trafficking issue.

Jess – Parents giving up their guardianship for the kid to have a better life, but then the child is trafficked.

Sari – Refugees often lie about their identity in order to get access to the next country. Create a profile. Claiming neighbors & sister's kids as your own to get them a better life. Here in the U.S. you get a [FICO] score, really scared when everything is digital & rigid, if I get sick, I'm still a pretty good person, how do we create these fuzzy gray spaces of identity. How do we introduce the human side to it?

Loss of our humanity when digital eliminates gray (grace) spaces

Mike - Rare disease space, have an app, as soon as kid presents with diagnosis, take a picture, we want to build a registry of what this morphology looks like, we can with some accuracy say this kid has a rare disease. But if I happen to run a country that has too many people, send them to be cannon fodder. Should you have the luxury of constructing a new identity?

Mei Lin: What's going to be in the lab in a box? Things to start with

Sari: It's all about governance. Who is on the board? What are their rules?
Social credit scores limit opportunities

Facial / video recognition – arbitrary use without humanity

Mei Lin: The U.N. has set up a high-level panel on digital social technical protocols.

In a Box Solutions:

- Community
- Tools / platforms
- Pen & paper / writing
- Discussion group (F2F, Email, online)
- Digital wallet (duration?)
- Library-in-a-box example (Wikipedia, where to find water, aid)
- Document safe (physical & cloud)
- Power source
- Format
- Scientist / testers
- Publications
- Journals
- Newspapers / flyers

Training

Data collection
Simple
Capacity to demo
Opportunity to opt in
Obvious place to interact

Channels

How can it work?

Phone / iPad / tablet / Pi
Digital lockers / post-disaster
Radio / TV
Meetup groups

Usable

Engaging, get buy-in
Incentive?

Mei Lin – Indian story of how the shopkeeper is king – spilled over into call centers

How do we take into account social norms?

Westerner takes photo of girl, puts photo on the Web, the family kills them. But it was innocent

Sherry – We have to understand the conditions of the environment

Cultural primer

Collaboration

Communication

Change

Cultural denominator

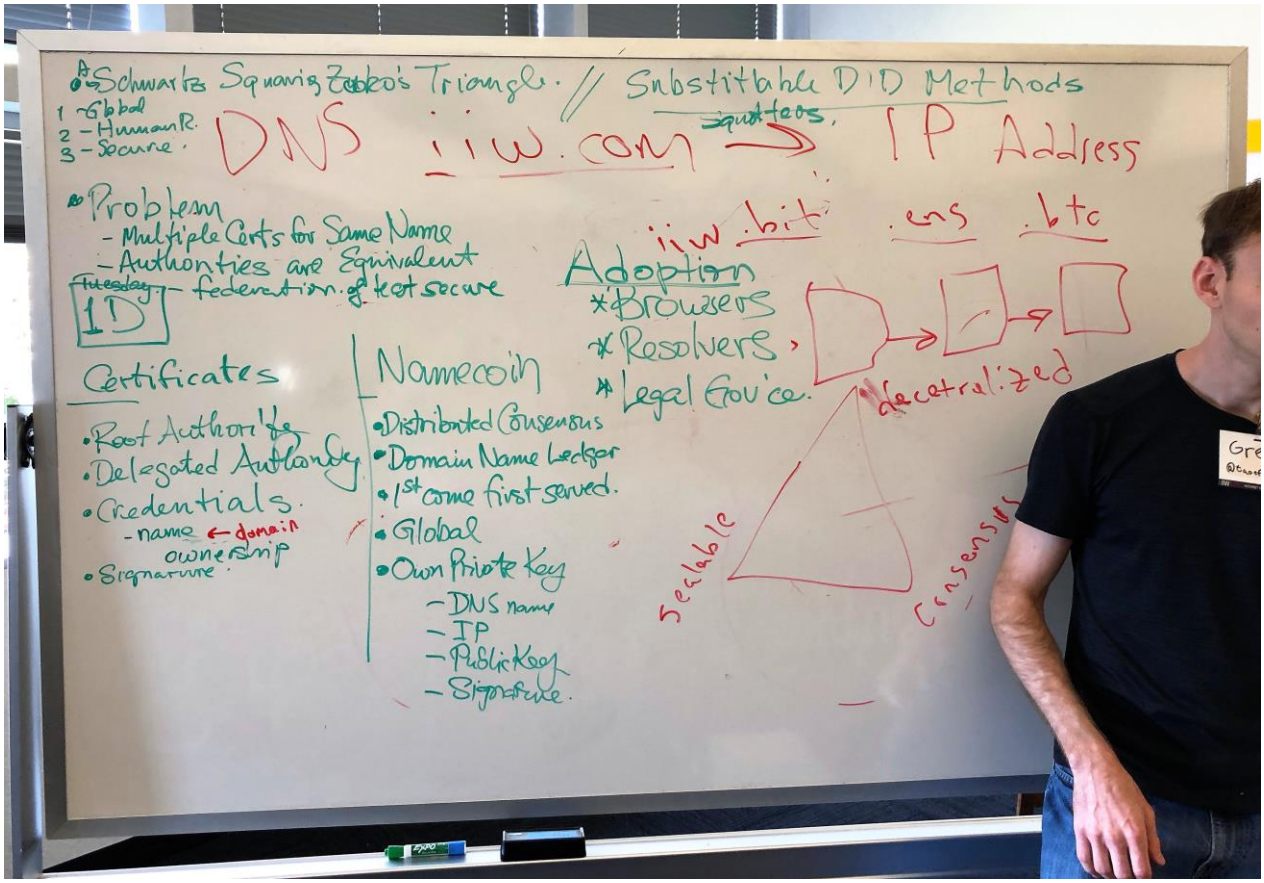
A context filter all the way from the village up to the country

Partner with anthropologists & ethnographers in order to do lab in a box, plus community leaders, local business

Blockchain TLD's

Day/Session: Tuesday 1D
Convener: Greg Slepak
Notes-taker(s): Adrian Gropper

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



CULedger Talk

Day/Session: Tuesday 1E
Convener: Darrell O'Donnell
Notes-taker(s): Darrell O'Donnell

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

Led by Darrell O'Donnell and Rick Cranston ~20 attendees
Overall Discussion statement: tweet

> *#IIW talk today: @CULedger is already working with @SovrinID and @Evernym to create better Member UX that lowers Fraud.*
>
> *Next: We see that Facebook added value using identity but they have been creepy; We would like to discuss how to get it right and make it natural.*

General idea was to gather ideas of what Credit Unions could offer to Members and others now that they have a SSI-enabled "MyCUID" (note: the term MyCUID may change over time - it is a credential issued to a Credit Union Member by a Credit Union).

CULedger is a Credit Union Service Organization (CUSO) owned by 42 member Credit Unions. Its initial mandate, the creation of an Identity Service based on Sovrin and Evernym technology aims to provide answers to the following three questions:

- Who are you?
- Can you Prove it?
- Can I trust the proof.

These questions are bi-directional - applying to both the Member and the Credit Union.

Once those questions can be reliably asked and answered, there is an opportunity to open the Credit Unions up to offering new services. That was the focus of the conversation on Day 1 at IIW.

Many ideas were brought up including:

- Delegation - the ability to delegate (e.g. CPA access to read-only in different ways if personal CPA or business CPA) and the role that Credit Unions may play in setting standards ("hmm, your CPA is asking for more access than is normal").
- Overlays - the ability to use common schema but not over-share is crucial.
- Trust Hubs - how do we list the "trusted" Issuers (e.g. bona fide Credit Unions).
- Credit Union Marketing - can a Credit Union appropriately leverage the relationship with a Member in a marketing context.
- Backup/Restoring Wallets - what is the role that a Credit Union plays (or could play)?
- Deviceless and Feature Phones - how do Credit Unions serve members that don't have devices like smartphones?
- Interoperability - a key role for CULedger to provide in this space.

Machine Learning/Computer Vision & Internet Identity

Day/Session: Tuesday 1I
Convener: Liam Broza
Notes-taker(s): Nick Roy

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

Half the people asked them to build this tech on OAuth, half on Sovrin, so decided to come here to hash it out
LifeScope.io
Building a person information manager
Build a database of yourself - where've you've been, what you own, etc.
Don't trust/can't control stuff run by the big internet identity/services companies
Built a tool with about 7 other people - lifescope
Have web browser extension for a bunch of browsers
Uses ETL tricks to figure out all your interactions, string this together into events
Could be put into an exascale model of the self
Tag things - semantic metadata on top of all of this
Return personal data ownership to the user
25-30 integrations
Search/sort through the info captured
Easy to search and share the info
Wrote about 100 scrapers for the top sites on the web
Parsers produce graphs
API - graphql - ingress and egress of data
Hang out with a lot of AR/VR people - want to do an AR visualization of your stuff, where you've been, etc
Liam has 7 TB of LifeScope data over 11 years for himself
Can do data science and visualization on it
Thinking about a human report card

Q: How are you categorizing people on their human report card?
A: Don't make up your own. There is a lot of existing work on this
Storage: on nodes you control or a private blockchain
Machine learning - computer vision scared Liam. You can use stuff like TensorFlow to do all sorts of elaborate tracking/modeling on a phone, browser using computer vision. Detect every object in the scene and how they all fit together, for example. Do pose matching on subjects. Facial recognition, not just the face, but the expression. Pathing - how things relate to each other in the scene.
Photogrammetry - push photos and videos together from the same place and create 3D models - completely passive. Facebook could create a reproduction of Street View just from people's photos.
You can compile the computer vision models into shaders - you can run as many as you want at the same time, and will do as much machine learning as the computer is capable of. The performance is improving on a weekly basis.
Talking about how to capture this daata and relate it to all the other data you have. Alternative to the closed computer visions systems out there.

Q: You do realize you're weaponizing this as well.
A: It's an arms race, everyone else already has this - intel, military, etc. Question is do 'we' have this?
If individuals have access to this data, then it does certain things about what a third party correlator

could do with the data. So a tthird party couldn't tamper with the data. You now have the ability to refute that.
For individuals that are non-state actors, if you have a data sharing agreement (GDPR), you could use this as a motivation to say that collecting data about other individuals has to come with their consent. All data everywhere should be self-sovereign.

Q: How do you trust who collected that data? How do you know the data wasn't modified when it was collected? How do we go back and say that is the thing that really happened?
A: Have to be completely open-source and people own their own data. We each need a private mesh that owns our own data.
If there are multiple copies, those multiple copies can be used to build a verifiable authenticity. We all become correlators for each other. Then you are protected against a malicious third party doing correlation. (How?)

Q: Who do I sue if something goes wrong with this?
A: Put in a github pull request.
I want to have my data vault and have the great machine learning trainers come to me and use my data to make suggestions to me about things like the best place to fish based on my preferences, skill level, etc.
Need an obfuscated ID - decentralization system to act as a trusted broker. Want to build as little of this as possible, leverage data soverignty built by others.
Leverage an authentication system that is operated by others, but decentralized. Right now using OAuth 2 to get claims/scopes - who, what, when, where and how.
Suggestion to look really seriously at DID.
Did it in OAuth, everyone wanted Sovrin, questions was 'what's Sovrin?'
There are at least 6 nodes doing DID stuff.
If you're doing a test thing, Sovrin's really the only game in town. As long as you're using DIDs, you don't have to pick one.
Broke the infrastructure up into Kubernetes pods
Each node types come together in clusters
The clusters network together
API layer talks to the data cluster
Have looked at ledgers, blockchain stuff, etc.
Ingest is via OAuth with their own scope system, but it's modular
When you go to manage your stuff, want you to be able to turn off components, etc.

Q: Don't get why you built this, other than 'you want us to have this.'
A: Looking for $4M (slide). Wants a Ray Bradbury house as an alternative to the Internet. How do we right the ship? Want to make it easier to find 'objective truth.' You're losing insight about yourself that the big companies already have, if you're not collecting this stuff. Trying to prevent social engineering as an attack vector.

Q: Is this trying to enable free will versus societal programming?
A: That is the moonshot idea here. Want to build a predictive personal chatbot to help you run your life.
COEL - Classification of Everyday Life
Want a pseudonymizer between attribute bundles and consumers of that data

Q: Don't know that I get exactly what you're saying, still, and how does an average person use this? A: Right now it's a cloud service. Q: Where is that data stored?
A: Currently launch a microcluster of mongo, mint credentials to encrypt storage, but person doesn't

fully control the key.
In order to do the machine learning, you have to decrypt the data. You could do machine learning just on your own data.
Data cleanliness is a huge problem.
With 5G around the corner and IoT there will be a massive amount of data collected on everyone.
Projection: By 2025 there will be 180 zettabytes generated by edge devices. Most of it will be collected, processed and dumped.
If you have a computing infrastructure that is decentralized, you can process it privately - no one else has all the data. All the processing happens off the central infrastructure.
Encryption will continue to get broken - every three letter agency is collecting all this data in Utah and in a few years the crypto will be broken.

Until homomorphic encryption is practical, there is no real privacy, there is only point in time privacy.
State actors have unlimited resources, so privacy by obscurity doesn't apply. Non-state actors are disincentivized to correlate if you make it inefficient for them to do correlation.
We fall over ourselves on privacy at the expense of data access and understanding.
A credential is a way of making an attestation about the final product - but should be self-sovereign.
Transactions are all about exchanges of value. I want to get value from my data.
Post-privacy and post-secrecy world. How does the individual maintain control? You can't maintain control. There is a time window- where you are right now is much more valuable than where you were 10 years ago.

In the edge space, want to control how much footprint you left behind. How do we manage post-privacy and post-secrecy? Supremacy of control is access.
AWS DeepLens or connect for Azure. You take a camera and couple it with a LIDAR sensor. The big internet companies are all working on productizing this. They want to put two edge device cameras in every room on the planet. Then they can run reports on who is doing what all the time.
Felt that privacy was an unapproachable topic full of jerks before - but privacy is about having a bit of space to reflect outside of the public domain. It has to be nuanced. ltimately we will learn things about ourselves. 90% of the world's data has been collected in the last two years. Have to think about privacy in the same way we think about identity - contextual, fleeting, situational. An opportunity to reflect - a screen we own that reflects upon what's happening with my data.

"The Known Citizen" - A history of privacy in modern America (Sarah Eigo book)

Introduction to OpenID Connect (101 Session)

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

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

Link to my PowerPoint & PDF: http://self-issued.info/?p=1930.

Blockchain 101 + Why you SEE BC Identity Projects

Day/Session: Tuesday 2C
Convener: Riley Hughes
Notes-taker(s): Steve Fulling

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

Blockchain 101 (not 102) and Why you see Blockchain Identity Projects by Riley Hughes

Notes by Steve Fulling

Allegory: We are medieval farmers. Some wheat, some pigs. Some want to expand farms. Some have extra money, some have extra pigs. We all write down in our notebook. A lent $50, B lent $100, C got $150 for expansion, etc. We do this in a ledger. We each have our own notebook which records the whole ledger. If there were a central notebook that could be bribed/corrupted. With all the notebooks it would be tough to corrupt. Every Sunday we compare notebooks and sync them, of sorts. We keep our books in order. But this can be costly and arduous. Lots of friction here. This is a distributed notebook system, of sorts.

So, we invented banks. This is a middleman, someone we trust. This middleman's best interests is served by keeping accurate records. Banks are managing the ledger and get the shit kicked out of them by the government if they allow fraud or corruption. This is much lower friction.

Everyone uses middlemen. Generally, this makes society better. But there are problems with middlemen. Like balance of power. Censorship problems arise.

A blockchain is at its core: going back to everybody having their own ledger. But, it's now automated. There is no middleman. It is all peer to peer. There are downsides. This is more expensive, we have many ledgers, not a single one like a bank would have. It can be more expensive, energy wise. It can be inefficient. There are also higher learning curves.

We still may have centralized services like Coinbase to help people use decentralized protocols (move BTC into fiat currency or vice versa).

Resources to learn more:
Sovrin.org
Wiki. Google. YouTube.
Crypto Zombie – to learn crypto coding.
Vitalik Buterin – clear but very technical
Play with stuff. Download Blockchain and Coinbase

Why would a ledger be good for digital identity?

There are 2 models of identity:
Traditional (Facebook, Bank, administrative)
Federated (OpenID)

How do we get to DLT is a better way to manage digital identify??
What are the problems with administrative identities? Lack of privacy. Closed system. Honeypot (it could be stolen). Can be impersonated. Scale.

What is the reward for breaking into one large system, or hundreds of smaller systems?? Do you want to rob a bank or rob 1,000 homes??

Comments:
We talked about smartphones and grandmothers. We need smarter grandmothers. Ha.
Have we considered keeping something physical like a digital key that stays in your pocket?
In emergencies people resort to physical systems: cash, birth certificates, etc.

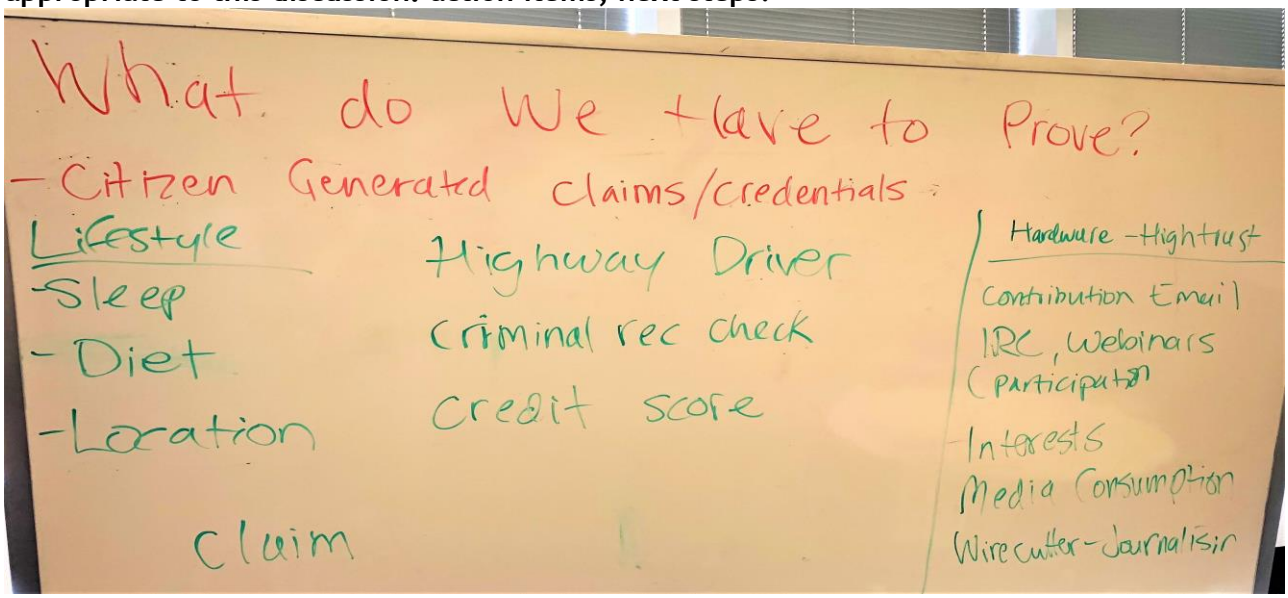
Framework to gauge legitimacy
Privacy
Lights Out test
Community / interoperability standards
Context independent?
Viable for at-risk populations.

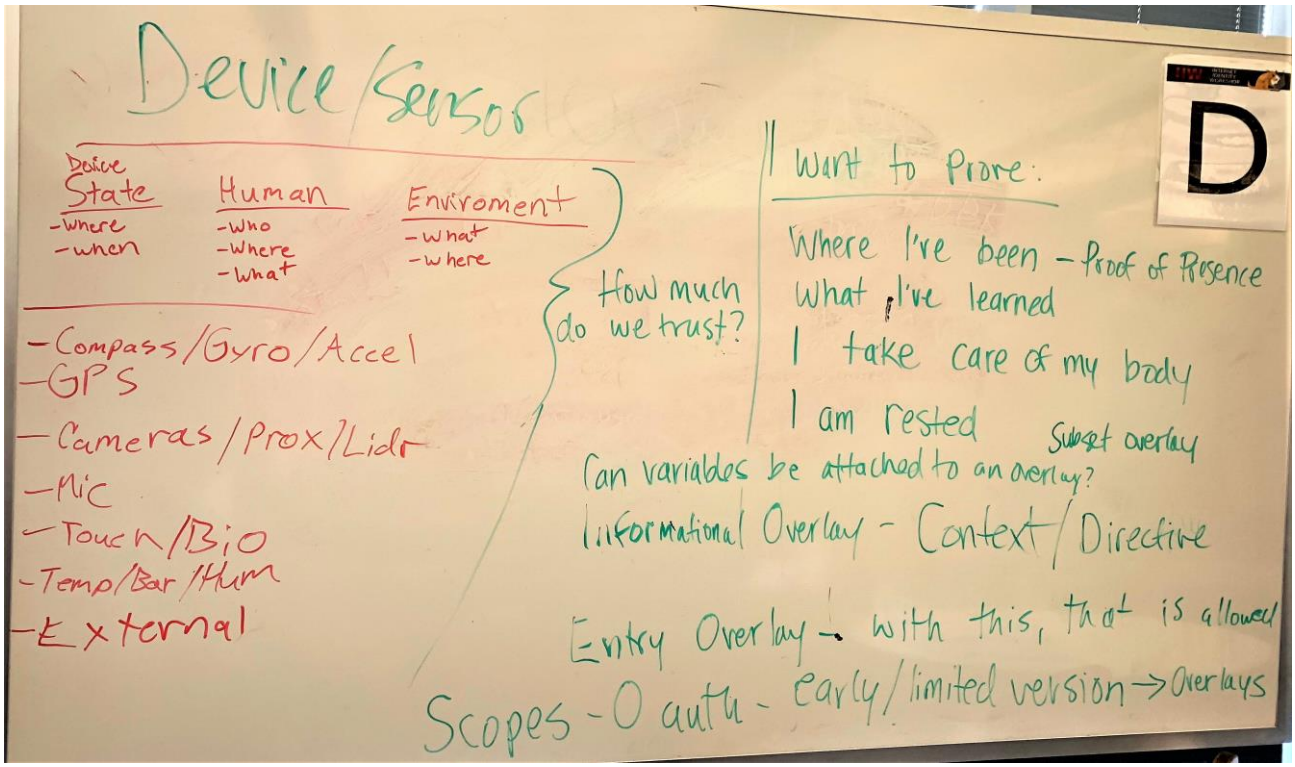
The End.

How Can We Enable/Support Individuals to Grow/Create Their Own Credentials?

Day/Session: Tuesday 3D
Convener: Sammantha Crush
Notes-taker(s): Sammantha Crush

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

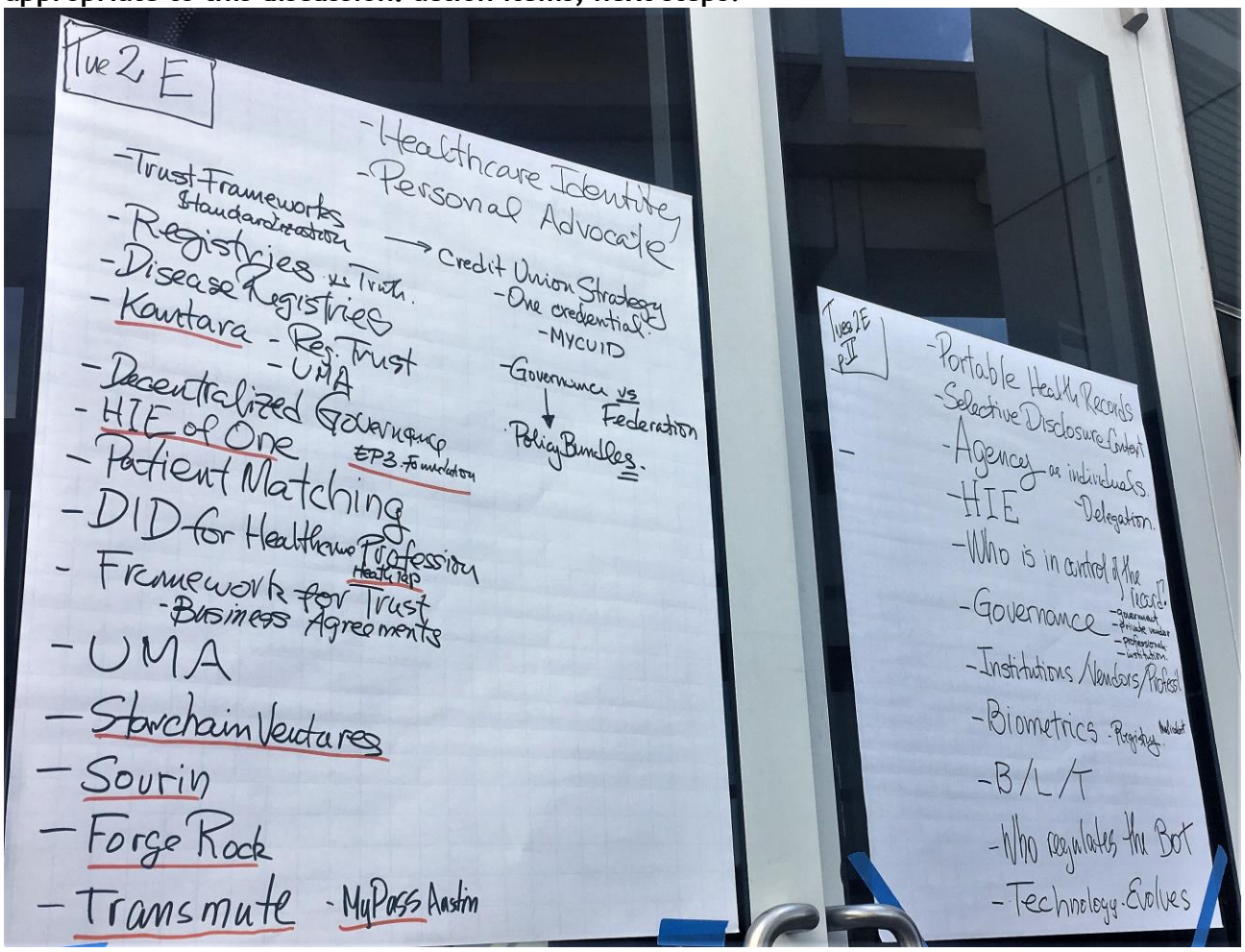




Identity & Trust in Healthcare + How Can Someone Create an AI Healthcare Advocate?

Day/Session: Tuesday 2E
Convener: Radhika Iyengar-Emens & Susanna Schick
Notes-taker(s): Radhika Iyengar-Emens

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



Domain Specific Trust Governance Frameworks Healthcare Worker, Identity & Credentialing

Day/Session: Tuesday 2G
Convener: Manreet (Manny) Nijjar
Notes-taker(s): Manny

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

Session Summary:

The session discussed the importance of assuring a healthcare worker is who they say they are and qualified to a standard to care for and or treat individuals.

We know current standards and checks are inefficient and there have been a number episodes of fraud and negligence which has lead to patient harm.

The discussion was based around the use of self-soveriegn/decentralised identity as a tool to improve these standards and reduce harm. The challenges to implement and adopt the technology would be dependent on a domain specific governance framework, facilitating individual healthworkers to be in control of their identity and qualifications and equally important allowing different oraganisations in the healthcare ecosystem to trust each other.

The discussion focused around the of a trust framework we have developed for doctors in the UK.

Review W3C User Consent & Permission

Day/Session: Tuesday 2I
Convener: Wendell Baker
Notes-taker(s): Titus Capilnean

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

Workshop based on conference notes and position paper here: https://www.w3.org/Privacy/permissions-ws-2018/cfp.html

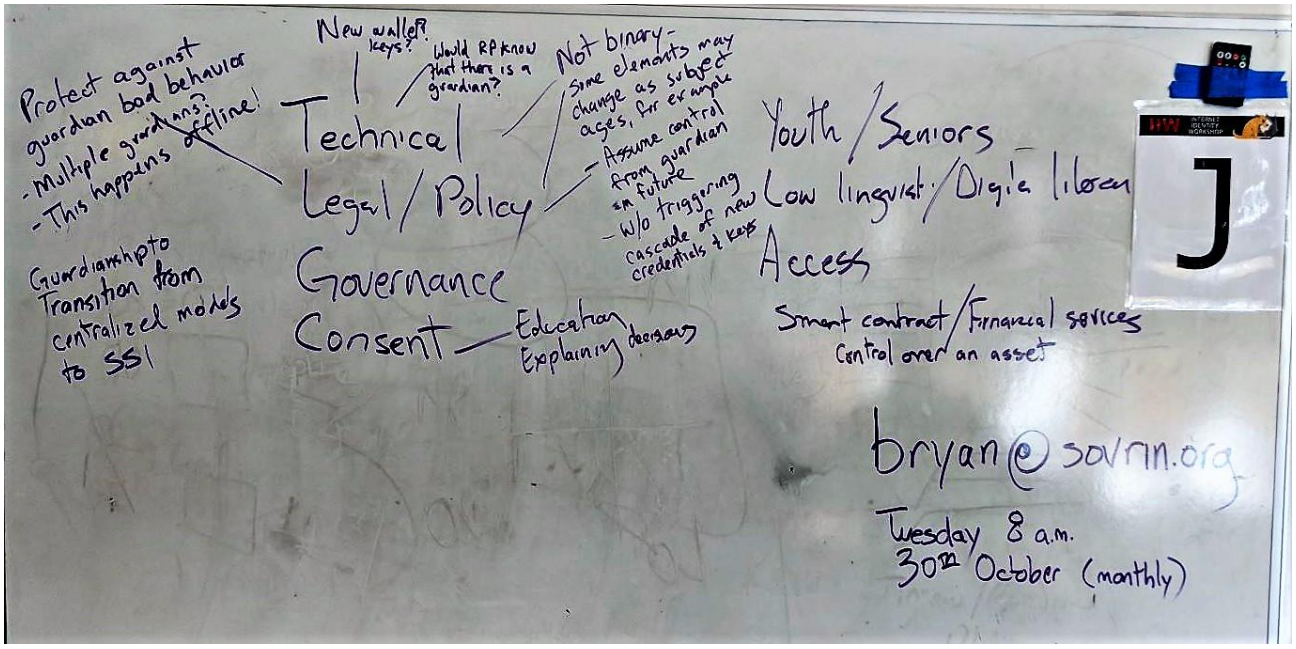
- How do we provide continued consent online?
- Confused deputy problem - how do you name activities and permission and when do you solicit it?
- e.g. Firefox file upload dialog box - consent perfectly timed
- How do you take location data and make it work the same?
- Tracking protection and GDPR are the biggest issues in consent
- For apple - 3rd party cookies don't exist
- Analytics problem - how do you explain them?
- Media and advertising challenge - how can you make it cheaper to track and serve ads with blockchain? Browser consent problem has not been solved at scale - your cost of serving is 1% of a 10,000th of a cent with legacy solutions. How can this be replicated at scale?
- w3c wanted to move all of it into the browsers - but it was late for GDPR, and adoption was slow
- Electron browser - mim, brave - brave is interesting, the identity fabric is interesting for the industry
- Privacy chain and oath - login with the browser identity - use case
- serve related content based on the user consent, need a mechanism for it
- ITP - intelligent tracking protection - tell your users or don't do it
- Usage insights: younger audiences - safari mobile vs older audiences - chrome, desktop
- A browser is a gate/door that needs a key - have to use it to enter a world
- Briefly discussed p3p - privacy for the web; obsolete protocol allowing websites to declare their intended use of information they collect about web browser users.

Guardianship: When Users Can't Manage Their Digital Wallet

Day/Session: Tuesday 2J
Convener: Bryan Pon
Notes-taker(s): Bryan Pon

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

For Questions write to Bryan (bryan@sovrin.org)



A Catalyst For Trusted Digital Ecosystems (Part 1)

Day/Session: Tuesday 3A
Convener: John Jordan & Stephen Curran
Notes-taker(s): John Jordan

Tags for the session - technology discussed/ideas considered:
#theorgbook, #government, #conceptmap, #verfiablecredentials, #hyperledgerindy

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

The session had the goal of sharing with the community the thinking behind the work the Province of British Columbia is doing under the label of the "Verifiable Organizations Network" and its first public service BC's Orgbook (https://theorgbook.pathfinder.gov.bc.ca --- soon to be https://orgbook.gov.bc.ca)

The idea here was to "talk over" our standard presentation slides (https://drive.google.com/open?id=1hElPRysMq7oAhIGVRgRLYiKpHTfqcbS_) in a kind of "Directors Cut" version that explains our reasoning for why, what and how are working through our efforts. The "Directors Cut" slides are here (https://drive.google.com/open?id=1frvLV5TApnUVNiFsfYYaA6WHjZpkLv-xfW2F1iqGjJM)

Some other useful links for background materials on VON and TheOrgBook

This is a short Verifiable Organizations Network Primer document with a high level overview of our work https://docs.google.com/open?id=1Pfu7S1JtLFNDvxvZqRgN3rvQCnnWIZBi1Dth8pglUQ0

This is our page pointing to all of our demos, APIs, GitHub repos and so forth. Everything we are doing is in the open and all code licenced under Apache 2.0 --> https://von.pathfinder.gov.bc.ca/clicky-things/

This is a 40 minute webinar recording I did which gives a decent overview of our work.
https://bc-von.s3.amazonaws.com/2018-06-VON-Webinar-for-Sovrin-Indy-Community.mp4

This is a link to a google folder with a variety of open documents in there covering various ideas and early specifications we have been considering
https://drive.google.com/open?id=10pco_o3WFfu1FVl_97LJh-g5izZj6o5Z

(Part Deux! – was on Wednesday Session 4F)

Introduction to User Managed Access (101 Session)

Day/Session: Tuesday 3B
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:

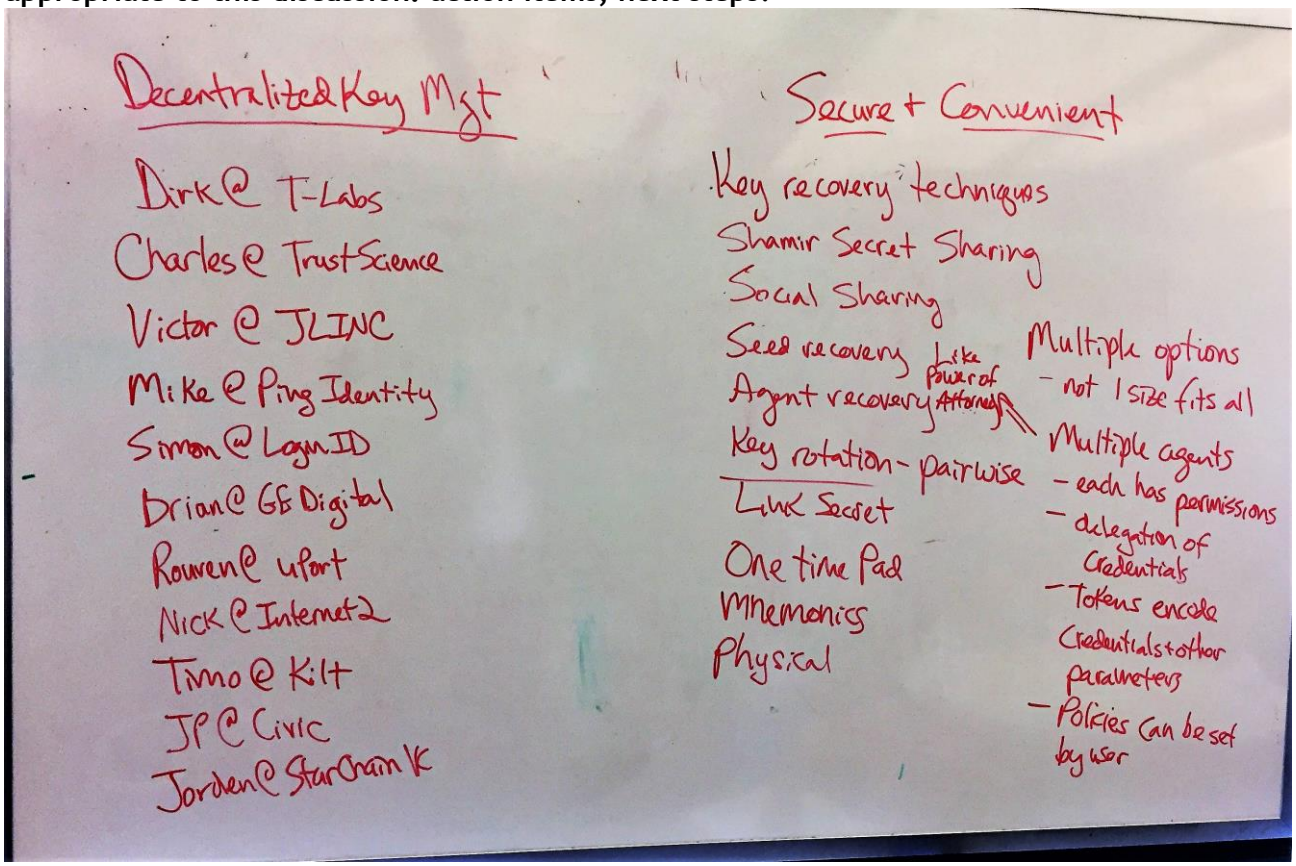
Link to the slide deck for the UMA 101 session which includes slides from a presentation given by some colleagues in the UMA group.

https://www.slideshare.net/gffletch/2018-oct-iiw-user-managed-access-uma

Decentralized Key Management

Day/Session: Tuesday 3D
Convener: Jorden Woods
Notes-taker(s): Jorden Woods

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



How Do We Bring "Tribal" (Group) Identity Online With Us? (Share & Tear)

Day/Session: Tuesday 3G
Convener: Duane Johnson
Notes-taker(s): Duane Johnson

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

Duane introduced his slides, and talked about "tribal identity" in the sense of "how we feel connected to our group or community" and how our tribes influence decisions, ethics, etc.

Duane talked about using verifiable credentials to prove membership in a community--for example, as admission requirement to an online discussion forum--and how that might work in practice. We talked about the "dispute resolution" process and how credentials currently don't offer a way to get in touch with the credential issuer and report the individual to whom the credential was issued.

We then talked about EULAs and terms of service related to both communities and applications.

Link to Slides:

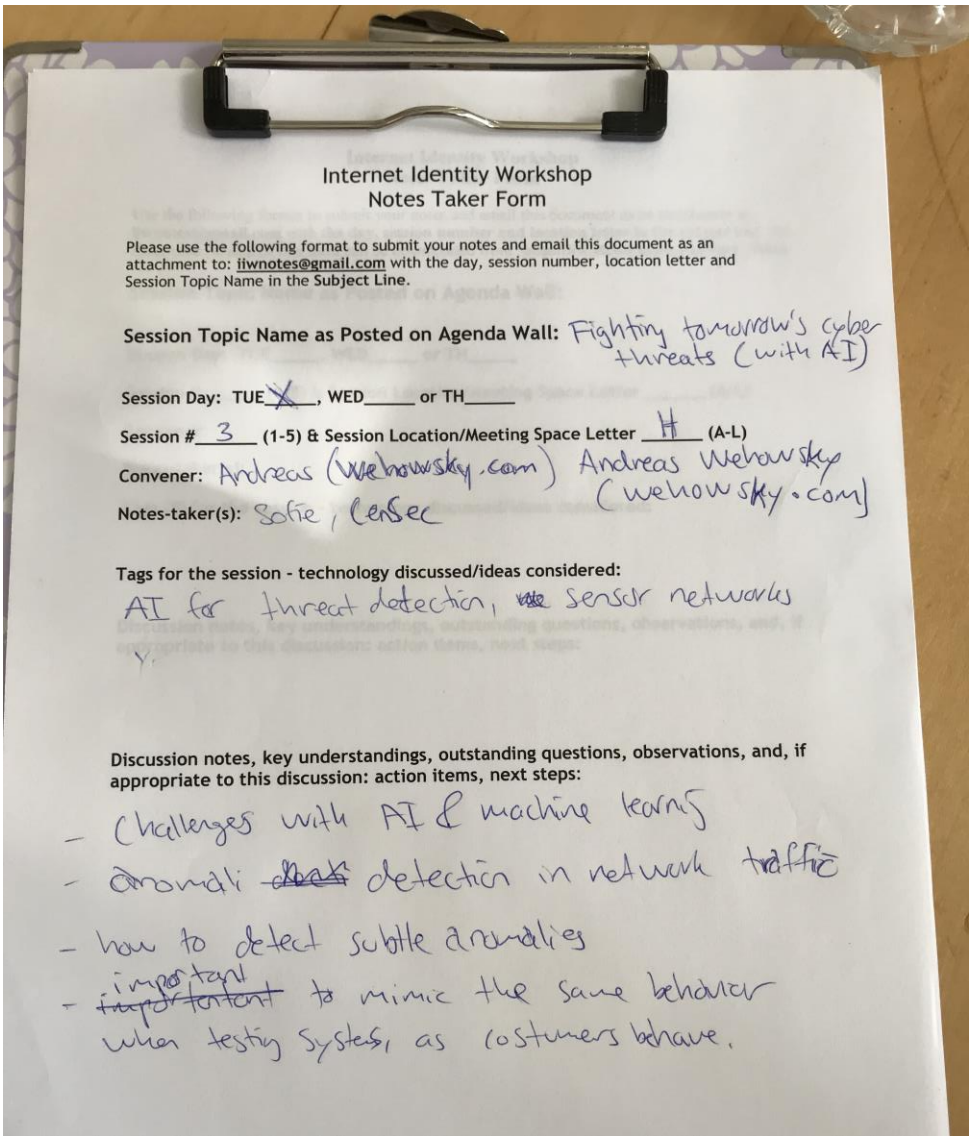
https://www.dropbox.com/s/ntesrgtzkz04rjw/2018-10-22%20Tribal%20Identity.pdf?dl=0

Cyber Security Data Breaches Fight with AI

Day/Session: Tuesday 3H
Convener: Andreas Wehowsky
Notes-taker(s): Sofie Kubel (CenSec)

Tags for the session – technology discussed/ideas considered:
AI for threat detection, sensor networks

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



Internet Identity Workshop
Notes Taker Form

Please use the following format to submit your notes and email this document as an attachment to: iiwnotes@gmail.com with the day, session number, location letter and Session Topic Name in the Subject Line.

Session Topic Name as Posted on Agenda Wall: Fighting tomorrow's cyber threats (with AI)

Session Day: TUE X, WED ____ or TH ____

Session # 3 (1-5) & Session Location/Meeting Space Letter H (A-L)

Convener: Andreas (wehowsky.com) Andreas Wehowsky (wehowsky.com)

Notes-taker(s): Sofie, CenSec

Tags for the session - technology discussed/ideas considered:
AI for threat detection, ~~the~~ sensor networks

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

- Challenges with AI & machine learng
- anomali ~~detect~~ detection in network traffic
- how to detect subtle anomalies
- ~~important~~ important to mimic the same behavior when testing systems as customers behave.

Australia's Tsunami of Data Laws - ID, Open Data, Cyber Front Doors. What & Why?

Day/Session: Tuesday 3I
Convener: Greg Adamson
Notes-taker(s): Greg Adamson

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

The session looked at a large number of digital changes in Australian this year, and whether this is similar to other countries. The lower level of protections in Australia, particularly absence of a Bill of Rights, means that poorly structured ideas (from a consumer perspective) could be adopted in Australia and then be introduced into other countries.

1. **The Digital Transformation Agency** is currently implementing the **Trusted Digital Identity Framework**, an enormous digital identification initiative. This is advocated based on a definition from the UN Commission on International Trade Law. Work on this project is well advanced, with 16 documents running to hundreds of pages released this year.

2. **World Bank Identification for Development (ID4D)** is a World Bank program to implement digital identity systems across Africa in particular, supported by the Gates Foundation, Omidyar Network, and the Australian Government. The program is modelled on the Aadhar biometric identification system in India, introduced without a legislative framework. Australia has taken on as its mission the introduction of identity systems to vulnerable populations in Africa.

3. **Consumer Data Right**. The Treasury Laws Amendment (Consumer Data Right) Bill 2018 is the first legislative step in the creation of an "open data" environment in Australia. The **ACCC CDR Rules Framework** supports the sharing of data by consumers with Accredited Data Receivers (ADRs) "for any lawful use". Because the benefit is framed as commodification of personal data, including of minors, rather than an increase in public good, the design focusses on preventing any block to the release of that data, rather than on protection of the individuals from avaricious company behaviour. If a customer is given a warning, it is okay to share data with an organisation anywhere in the world, without limits.

4. **Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018:** The government takes a dim view of encrypted information. In this bill the government significantly lowers the barrier for demands that it can decrypt encrypted traffic for: Enforcing the criminal law and laws imposing pecuniary penalties; Assisting the enforcement of the criminal laws in force in a foreign country; Protecting the public revenue; or the interests of Australia's national security, the interests of Australia's foreign relations or the interests of Australia's national economic well-being.

Outcome from discussion

In discussion, two interesting points emerged:

First, some equivalent programs can be found in Europe, particularly: **electronic IDentification, Authentication and trust Services (eIDAS)** provides a framework for use of digital signature. This is a guideline for national legislation, as is **Revised Directive on Payment Services (PSD2)**, guidelines for payments. The missing part in Australia is a data protection framework equivalent to the **General**

Data Protection Regulation. Unlike guidance, this is a regulation applying throughout the European Union.

Second, a key insight from a global corporate perspective was that within the Australian market attitudes to privacy are considered to be similar to those in Europe. Therefore, we face a potential mismatch between community attitudes to privacy, and intrusive legislation and programs introduced without concomitant protections.

Sovrin Stewards: Onsite Feedback

Day/Session: Tuesday 3J
Convener: Matt Norton
Notes-taker(s): Matt Norton

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

Session Summary:

The purpose of the session was to gather feedback from Sovrin Stewards who had participated in the Steward Onsite meeting the day before. No Sovrin Stewards attended, but others did to gain more insight into a Stewardship and Sovrin basics.

We described the 3 layers of the Sovrin Network architecture, found in the Sovrin White Paper. We spent much time talk about Zero-Knowledge Proofs, the purpose of the public ledger, the nature of verifiable credentials, and the aims of the Sovrin Foundation. For more information, please see the notes for Phil Windley's Ask Me Anything about Sovrin session or Heather Dahl's Session with the Executive Director of the Sovrin Foundation. The questions covered in those sessions describe the details of what we covered.

How THEY Consent to OUR Terms

Day/Session: Tuesday 4A
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:

GDPR made it much worse.

Here are all these Web sites. All of a sudden every one of these has a thing on the bottom or top saying do you consent. In the next session Andrew will have a cool idea for addressing this.

How do we do this right?

Lots of sites obtain your consent. There are ways to obey the letter but not the spirit of GDPR. What happened instead is we're still stuck in a world where we're being tracked everywhere. New book, Surveillance Capitalism, another book, Reengineering Humanity. What we're doing at Customer Commons, for terms, what Creative Commons is doing for copyright. We have a repository where terms we can proffer as individuals can be pointed to. First is #NoStalking. It's beta, no machine readability built into it yet. Creative Commons is human, machine and lawyer readable terms. We intend this to be a big jump beyond ad blocking. We have so far one publication ready to hear those terms, Linux Journal. The legalese has been written by the Cyber Law Clinic at Harvard Law School. Also Berkman. Rather than this entity always agree to these things, if you're a publisher, we're fine with your advertising, just don't track us. Do not track with teeth. A question last time, on the floor again, because DNT is a gargantuan fail, should we take over DNT? =1. Requesting a file. HTTP header, request they not shove cookies in there. But that's not obeyed. Several approaches to recording an agreement. In the last IIW, another called JLINC, server to server approach, Victor Gray wrote it, he's here, also Jim Fournier. An A server, a B server, an information sharing agreement between those two. Salesforce can be the B server. JLINC, but it's outside the browser. Second approach, we have a cookie we set ourselves as individuals. Server usually gives us a cookie, we could have a cookie that speaks to existing IAB standard in Europe that will say, don't track me. I don't consent to being tracked. Doing that in a default way. Had a large session at MIT, hack day, to take apart the downstream. Github. With that spawned, even though Sam was on the road and had a life, a couple developers working with Don Marti at Mozilla came up with the Global Consent Manager. It is a little hard to find but it is on Github. Available for Firefox now. I have it, looks pretty cool, does what we talked about last time. User-controlled GDPR consent cookies. Don at a session at Mozilla's Mozfest in the U.K. next week. It's rather large.

Q: I had this concept on consent receipt.

Doc: Kantara doing it. Doesn't solve it. It memorializes it. I've not participated in that conversation. My interest is can we make sure it works the other way. It works both ways. Bravo for that. A very positive thing.

Mary Hodder: The spec has a schema, allows for recording of consents in both directions. There is a section for terms. The entity to some degree under the GDPR has a lot of control. The idea is if there is a set of terms that are offered, there should be a response, and how do you do that.

Q: More a tool for accountability afterward?

Mary: Yeah. It's a contract. It's owned by both parties. It's co-created.

Q: It's trying to give agency before & during the agreement.

Doc: The system we have now, actually a non-system, it gets fig leaf GDPR compliance. It becomes unmanageable for us. Jim Pasqual wants to do a session on Digi.Me to show all the consents you've given. Consent receipt may be involved in that. The problem with the world as we know it now but it doesn't have to be, in 1995 we settled on client/server, but the Web is underneath inherently peer to peer. We have a way of giving them better signals. It moves into the realm of contract, which by the way most consents are. No reason we can't have them going the other way and make much better signaling happen. The ad choices thing tells you you're being tracked, but even if you check all those off, no way of going back and saying what happened there. Start with publishing problem area. The third rail that no journalist wants to touch, they're just as bad at tracking you too. Getting them out of that business is not hard. Get Oath to serve up ads that are welcomed. One way to start scaffolding up better ways to interact.

Wendell: Vocabulary for expressing parts of the consent. I think you guys have that. Been hugely controversial even within IAB. Cross product of that relative to the entities that participate in those things. And the jurisdictional realm.

Doc: One reason we're focusing on publishing, publishers not willing to track people. If all you're doing is saying what from the site's POV is a first-party ad. You're Nike, want to be on a fitness site. Hiring Oath to place that ad on that site, fine as long as they don't place a tracking cookie on the site. Let's start there and work out the ontologies and the rest of it.

Wendell: A lot of people know what that means to have only first-party ads. Given that, we have publishers whose advertisers want to know who saw the ad.

Doc: Possible.

Wendell: Do I get rights to go visit them?

Doc: This gets to a division between two types of advertising. In analog world, go to a bar, watch a game, it doesn't know who is watching. I know Ford makes trucks called Ford Tough. That's to their benefit. That's branding. Brand advertising doesn't need to know who everybody is. Direct marketing is. There's the notion that the only worthwhile ad is one that's fully accountable. With this case, there are number of publishers and operators, like PRX, willing to participate in this. Other publications would like to be able to that. Who's the third party who could help us with that. Maybe Oath could help with that. Love to have it. Linux Journal, though they have a sales person, if there were an ad agency that wanted to do #NoStalking advertising, like Intel, we're fine with telling them how many people saw the ad.

Q: Heard of the Cloudal Network? They were an ad network that did no tracking. He was losing the battle against tracking. Maybe he could become our engine.

Doc: There was an American ad agency that did non-tracking based stuff. We met them through Mozilla. I think Blog Ads when Henry Copeland ran it was similar. We've had a land rush to direct marketing. We expected enforcement of GDPR. That didn't happen. Instead the user experience is much worse. Andrew came up with a clever idea.

Wendell: We can talk about why the DNT header fell down, could be asked and answered in your browser, never leave your machine, well received at W3C. A stream a lot like a preferences page, ask and answer these questions. A lot of sympathy now. ITP blocks third-party cookies. IAB questions, asking and answering in browser is a good deal. (??) Your idea is a good one. Get browser vendors to put it into a release. Not get involved with what happened to DNT. Then don't have to have the current body of work is a lot of engineering.

Doc: The key is if we get some uniformity across the browser makers, that makes it easier for you guys.

Wendell: The taxonomy of your permissions is good. Controversy in IAB about what permissions shall be. You have one in Customer Commons. Get that into one of the mainline browsers or make your own browser using like Electron. Then send that out as a header and exhibit what a client side should do. From the server side, it's a much easier conversation to have something to expect.

Doc: Make this as concrete as we possibly can.

Wendell: You have how many things you can consent to?

Doc: Right now it's one. Consent is a thing because GDPR made it a thing. Basically it's an invitation. We're saying to the Web sites, be like it is in the physical world. Vogue, I had no problem with advertising. Just don't track me off the site. That's normative enough for pretty much everybody to understand. Trying to think what a browser maker would install that would do just that. DNT, advertiser wasn't on the table, it's just tracking.

Wendell: In order to show this is a choice, you have to have an affordance in the browser, they could have it turned on. There was an instance where Microsoft turned it off (??). Conversation with Brave at W3C user consent workshop, Thomas, PM of the Brave browser, you are expecting and consenting to no tracking. All these defaults turned on. If you want a secondary screen, turn the other way, okay, but it's not going to be easy. It's only when there's not the control…

Doc: The IABs and Oaths of the world are cool with that?

Wendell: Yes. As opposed to browsers having no control. ITP, blocks single-page web apps with open id connect, and reasonable experience for non-tech consumers who have a multi-domain experience. i.e. Oath, multiple domains serving content. More collateral damage than I think they expected. One design for DNT that was abandoned was a separate cookie jar, separate pop-up. Header sent out to websites as communication ordered, website was ordered to respect that. We could make enticements to turn that on, other side could say don't do that, and that's fine. But your idea is a great one. A lot of sympathy at this point to build that into the very browser.

Joyce: So now there's an opening. If DNT showed up right now, much more openness to allowing it to be there.

Wendell: They were fighting the default. When a browser is installed, sign on first launch, would ask you all these questions, squirrel away all this knowledge never to be seen again. PC vendor would answer all these questions first. Or the used browser problem, and no way to go see that. Current environment is different law and different technical affordances. A lot of debates from the past 5 years could be replayed with a different outcome. A lot more education at this point. More sophistication on our side with chains of custody, tracking through the pipelines.

Doc: If DNT had never been invented, but came along now with that simple thing, there would be more friendliness to hearing that on the part of advertising.

Wendell: Publishers are proud people. Some are not so proud and operate differently. Some of us believe we have the privilege of asking the consumer base for their data. Might grant tracking to Yahoo and friends. Who are these friends? Current regulations, you have to list them. But also anyone you might do business with. That's a giant list. That's puzzling to people. The proposal of the header needs to express who else can get this. You could ask, on yesterday afternoon, did that data actually get over to that company?

Doc: Interesting, could watermark data in a way that's traceable.

Q: I'm uncomfortable with the European Court being the arbiter of Web settings.

Doc: Don Marti found this, before Google started fudging their Google Trends graphs, a linear correlation between searches for retargeting and ad blocking. Ad blocking took off when retargeting took off. The Onion, woman stalked across 8 Web sites by obsessed shoe advertiser…intent casting. Project VRM Wiki, 20 some companies doing intent casting. Amazon is making big gains in the advertising world right now.

Introduction to FIDO (101 Session)

Day/Session: Tuesday 4B
Convener: Chris Streeks
Notes-taker(s): Romain Lenglet

Tags for the session - Technology discussed/ideas considered:
#Web Finger #DNS

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

"How to authenticate a user given its identifier?" boils down to "How to find the user's IdP?"

- WebFinger specifies well-known URIs
  RFC 7033
  https://<domain>/.well_known/webfinger
- Proposal: use 2+ levels of DNS subdomains instead
  <whatever>.well_known.<domain>
  It's easier to setup a DNS subdomain / CNAME than well-known URIs, redirects, etc.
- Problems with this proposal identified by audience
  - The discussion is limited to resolving an IdP from an identifier that has a domain name, esp. an email address
  - It wouldn't work with other identifiers, e.g. employee ID, phone numbers, bank account numbers
  - Also, this solves only a small part of the overall problem of connecting an SP with an IdP
    - The IdP must also be setup with the ID+secret of the SP etc
  - Need to protect against MITM, which is easier with DNS
- There is already an RFC draft specifying the use of an "_openid" TXT records for OpenID: https://tools.ietf.org/html/draft-sanz-openid-dns-discovery-00
  - But it's not user-friendly: one can't "curl" a TXT record
- There is an RFC to do DNS queries over HTTPS
  - However, that standard is underspecified

The responses are binary DNS replies in HTTP reply bodies, which makes that protocol hard to use

We Need A Working IdP Discovery Mechanism (for Rise, Fast Fed, and More)

Day/Session: Tuesday 4C
Convener: Darin McAdams
Notes-taker(s): Darin McAdams

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

The attendees confirmed the pain points of hosting WebFinger services under the root domain. One participant had previously built dynamic discovery based on domain. Many corporate customers were blocked because they were unable to host services under the root. Solution was a proxy as described below in (3).

The discussion circled around 3 alternatives:

(1) Subdomains.

-- Example: Instead of "https://<domain>/.well-known/webfinger" , flip it around into "https://webfinger.well-known.<domain>"

-- Pros: Easiest for everyone to implement. Just works for HTTP GETs. Enables CNAMES, which is nice when using 3rd party hosted IdPs and you want to point your domain at the hosted service.

-- Cons: No well-established patterns for reserved subdomains. More difficult to standardize. Subdomains existed in early versions of WebFinger but were cut because of these challenges.

(2) SRV records

-- Example: DNS SRV record for "webfinger.<domain>" that points to the location of that service.

-- Pros: There exists a well-established SRV registry.

-- Cons: More difficult for application developers to integrate with. Can't make a simple HTTP GET to a URL. SRV require an explicit DNS resolution first. Some environments, like javascript in browser, don't allow SRV queries.

(3) SRV records + Proxy

-- Example: Same as above, but run a proxy. For example: "webfinger.org". Make the WebFinger request to the proxy using a regular HTTP GET. Behind the scenes, proxy resolves the SRV record and invokes the authoritative WebFinger server.

-- Pros: Preserves the simple experience for developers. Uses standard mechanisms like SRV records behind the scenes.

-- Cons: Somebody has to run the proxy.

Finally, there was discussion about whether WebFinger was truly necessary here, as opposed to simple static configuration at an endpoint. WebFinger is necessary if multiple IdPs are used for a single domain. (WebFinger allows discovery of the specific IdP for a username in that domain.) There was mixed feedback from the room.

DID Resolution & Registration

Day/Session: Tuesday 4D
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:

DID Resolution is the process of obtaining the DID Document of a DID, for the purpose of interacting with the DID subject in a trusted manner. The most important parts of a DID Document are public keys and service endpoints.

At the Decentralized Identity Foundation (DIF), we've been working on the Universal Resolver, which is an implementation of multiple DID methods:

https://uniresolver.io/

Within the W3C DID standardization process, we are planning to have a document that defines the details of DID Resolution (currently a skeleton document):

https://w3c-ccg.github.io/did-resolution/

There are several technical details to consider when performing DID Resolution:

https://github.com/WebOfTrustInfo/rwot7/blob/master/topics-and-advance-readings/did-resolution-topics.md

Also, we are now working on a Universal Registar tool that can create, update, and revoke DIDs across different DID methods:

https://uniregistrar.io/

For more information on how to use these tools and contribute, get involved with the W3C Credentials Community Group, Decentralized Identity Foundation, or email markus@danubetech.com.

How Do We Do Digital Consent Forms & Share as Claims with Multiple Parties (Healthcare)?

Day/Session: Tuesday 4G
Convener: Alan Viars
Notes-taker(s): Alan Viars

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

The group started off talking about the problem of multiple consent forms and the common need for consent aggregation. Participants included representative from Capital One and the Kantara Initiative. The group suggested the term "consent form" is confusing and instead we should settle on the terminology "user permission" or "user stipulation".

We discussed at length the Kantara Content Receipt Specification (https://kantarainitiative.org/confluence/display/infosharing/Consent+Receipt+Specification) This specification results in an JWT that is a receipt for the user stipulation. Immutability of the receipt is an option but not required by the specification.

It was pointed out that to copy with GDPR and forthcoming laws in California, a feed loop is needed. A user must be able to select specific elements within the user permission dialogue. A user only needs to agree to the minimum necessary to achieve the action. The systems can say "ok" or "sorry I cannot complete the transaction without X or Y".

We discussed the notion of typing/codifying different types of consents. this is something that has been recognized in the Kantara Initiative as a need and is being worked on, but it is not yet a standard.

The group discussed different ways to handle the need for signatures and receipts. One method is to simply state that the paper form with a signature is on file. Another method is to store the signature within the consent receipt, although this results in a much larger JWT.

The group also discussed identity assurance.

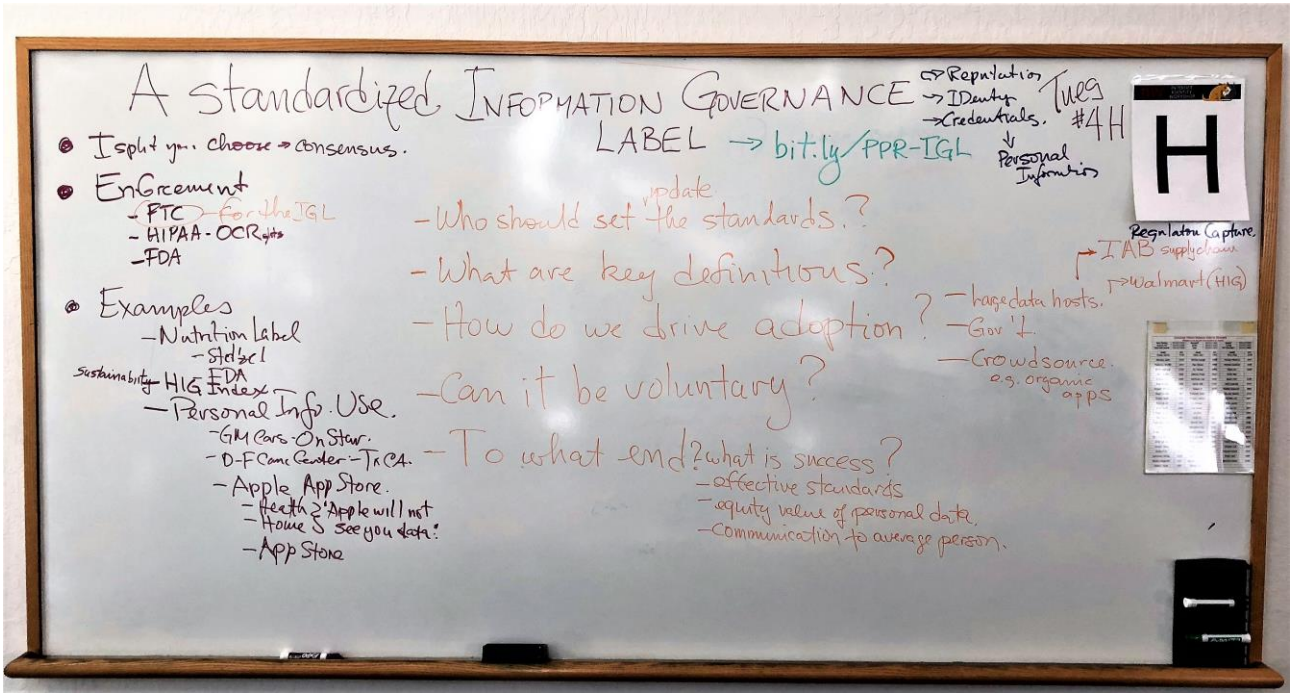
We discussed the difficulties of managing identity for the homeless or those without email or a consistent mobile phone. It was stated that often times in these cases, identity assurance is less important that consistent identity. We also discussed how identity assurance decays over time. For example, when a person presents a utility bill to prove he or she lives at a particular address, this information may at some point in the future no longer be true.

A Standardized Information Governance Label

Day/Session: 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:

Proposed Label is at bit.ly/PPR-IGL



Design an Undergraduate Blockchain Course

Day/Session: Tuesday 4K
Convener: Kent Seamons
Notes-taker(s): Kent Seamons

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

A Princeton textbook has been adopted at 50 universities. Videos, homework assignments, and implementation framework for hands-on experience building a permission-less blockchain.

There is code for automatically check for correctness. This textbook focuses on Bitcoin and permission-less blockchains. We discussed how to expand the scope of a course to cover permissioned blockchains.

Why block chain and why not? Students learn whether a problem is suitable for a blockchain solution and develop a healthy skepticism on blockchain as a solution to many problems.

Talked about platforms and frameworks that students can leverage to gain hands-on experience building permissioned and permission-less blockchain constructs.

What application areas that can serve as projects for a Capstone-style course?

Existing courses in Denmark, Germany, Oxford, Princeton, Stanford.

A DID for Everything!

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

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

Link to my slide deck:
https://github.com/SmithSamuelM/Papers/blob/master/presentations/DID_Everything_IIW_20181023.pdf

Self-Sovereign Identity 101

Day/Session: Tuesday 5B
Convener: Heather Vescent & Kaliya Young
Notes-taker(s): Heather Vescent

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

101 overview of SSI, slides based on this talk (youtube): https://youtu.be/gfi11GZjbWM?t=925

Other referenced materials are from the Comprehensive Guide to Self Sovereign Identity. Available here: https://ssiscoop.com/

Unintended Consequences of What We Build

Day/Session: Tuesday 5C
Convener: Annabelle Backman
Notes-taker(s): Annabelle Backman

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

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

Two modes:

- Negative human behavior applied to/within technology, i.e., badly behaving users
- Technology that behaves badly itself, i.e., biased AI algorithms
    - This is technology codifying negative human behavior

Online disinhibition leads to worse human behavior
Do we have a responsibility to prevent users from themselves? No consensus.

- Users can't be responsible for something they don't understand, e.g., massive Terms of Use.
    - Aggregating forces, snowball effects create pseudo-coercive effects; "opt-in" may not truly mean "opt-in"
- Users should be held accountable for the contracts they agree to.
    - Users happily click through consent prompts then complain when their data is used in unexpected ways.
- Regulation is expensive, inhibits startups and new competition.
- Need to actually fix the way people think or don't think.
- Are we always responsible? Or never responsible?
    - Responsibility to advise and inform.

What happens when things go wrong? Example: Aadhar being misused, leading to fraud

- Similar to SSN; a lot of very useful properties, natural for people to use it
- Need to consider if all the properties of a system/solution are desirable.

My Data @ IIW

Day/Session: Tuesday 5D
Convener: Paul Knowles & Henrik Biering
Notes-taker(s): Paul Knowles

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

Here is a link to Paul's slide deck for this session: http://bit.ly/mydata_IIW

Sovrin AMA (Part 1)

Day/Session: Tuesday 5F
Convener: Phil Windley & Jim Fenton
Notes-taker(s): (1) Phil Windley & (2) Jim Fenton

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

(1) Notes from Phil Windley:
Jim Fenton had read the Sovrin White paper (https://sovrin.org/wp-content/uploads/2018/03/Sovrin-Protocol-and-Token-White-Paper.pdf) and had questions.

We worked our way through the white paper with Jim asking questions and Phil answering with the help of others. Jim's questions sparked other questions from participants.

The discussion focused on areas like:

1. The need for decentralized identifier discovery in an adversarial environment

2. The details of Sovrin credential exchange

3. The architecture of Sovrin

(2) Notes from Jim Fenton:
This session was an open discussion of questions and answers about the Sovrin white paper, available at:
https://sovrin.org/wp-content/uploads/2018/03/Sovrin-Protocol-and-Token-White-Paper.pdf

Questions were seeded by Jim Fenton, who recently read the white paper, and most answers were supplied by Phil Windley. Other questions and clarifications were supplied by others in the session.

The questions included (page references are to the above PDF):

- (page 6 bottom) Given that there is an existing trust relationship, why doesn't the verifier already have the issuer's public key?

- (page 7 bottom) The issue with PKI seems to be with the CAs. Why not just have the issuer sign the assertion with their key?
- (page 9 middle) The link for Validated transactions points to a bitcoin document. Validation is undoubtedly different for Sovrin; what does it consist of?
- (page 9 bottom) Why is immutability of records important?
- (page 9 bottom) What is "self service"? Isn't this done by stewards, not users?
- (page 10 top) "No registration authority": Isn't the blockchain, in effect, a registration authority?
- (page 11 top) Who signs the public key assertion on the Sovrin blockchain? You need to trust that signature, too.
- (page 13, top) Why not use one of these , like DNS?
- (page 13, middle) "never be taken away" Why is this a threat?
- (page 17) How does one get claims for new DIDs? Do you need to give all DIDs to each claim provider?
- (page 22) Comment: quantum computing will cause problems for Sovrin public keys as well.
- (page 23, bottom) Does the past failure of ZKP to catch on stem from lack of infrastructure, or from desire by relying parties to get as much information as possible?
- (page 26, top) Access to Sovrin is not necessarily password-free.
- (page 28, bottom) Compliance costs for businesses are often low: direct financial losses akin to shoplifting for financial institutions, and arguably low penalties for breaches of personal information. As a result, there was little interest in deploying earlier federated technologies. Are the incentives high enough for deployment of a very new technology?

What Questions Should I Ask Myself Before Clicking the "I Accept" Button?

Day/Session: Tuesday 5G
Convener: Andrew Hughes @idimandrew
Notes-taker(s): (1) Scott Mace & (2) Andrew Hughes

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

(1) Notes from Scott Mace:

The Agree Button (andrewhughes3000@gmail.com)

Starbucks general privacy notice

The only concept here is, whenever your agree buddy detects an “I accept” button, reminds you of the questions you should ask yourself before you agree to anything on the Internet. If you’re okay with the answers, fine. If not okay, don’t click. If you object and clicked anyway, there’s a problem.

Version 5000 of the agree buddy would be actual buttons on this little popup thing. Keep your internal statistics, or maybe there’s a reporting service. I’m scared, I don’t want to do this. I’m unhappy but I

want WiFi. Assume a nonprofit that will receive all these clicks against the domain all your customers are unhappy they are having to accept the terms but they are doing so anyway.

Q: I have no idea what kinds of questions to ask.

Q: Are you going to share my data with a third party?

Q: Putting more thinking on the user.

My hidden motive is I'm documenting consent management practices. Which ones are good, which are bad. If red flag goes off, would you leave the Web site? What would you like someone else to do? Tell a regulator to investigate?

Q: How risky is it?

- "Safe browsing" service – Google Search (this exists), Mozilla
- Community-sourced views about the site
- Anti-phishing scripts are a good source
- "How did I get to this site?" – Don't click on stuff!
- What are the top fraud-against-people situations?
- Capture why the user is ok / not ok agreeing?
- Micro-feedback companies do exist
- Plain English translations of a contract
- Is there a general expression of the tradeoffs?
- Shows that the company actually cares

What would you want the service provider to inform you about?

- We are / are not tracking you
- Does your tracking stop once I'm gone
- Are you sending my info to someone else?
- Is someone profiting from my data directly?

Doc – Better boilerplate With case precedent

Joyce Searls: Chrome plug-in called Magnify. Online dispute resolution company.

Privacy Chain by Live Ramp

- Explainable
- Understandable
- Fair
- Non-discriminatory
- Not objectionable
- For public good
- Can I object
- Can I change my mind
- How do I benefit?

(2) <u>Notes from Andrew Hughes:</u> Link to slide deck: https://www.slideshare.net/AndrewHughes6/the-agree-buddy-andrew-hughes-iiw-slides-2018-1023

OIDC Federation (OpenID Connect Federation)

Day/Session: Tuesday 5H
Convener: Roland Hedberg
Notes-taker(s): Nick Roy

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

OIDC Federation - Conveying trust via a federation in OpenID Connect

Entity statement - a JWT that contains iss, sub, iat, exp, but added to that we have metadata, authority_hints, jwks

Every entity has an entity_id - a URL, doesn't have to be, could be a URI, but has to be resolvable to a URL

Add a query part to the entity ID
If issuer and subject are the same, you are interrogating a subject about its view of itself, using a self-signed jwks
Authority hints point to superiors - organization, federation
Then ask the organization about its view of the entity
Then ask the federation operator about its view of the organization
(n levels)

You'd ask about all entities of a specific type within that organization - common view of those from the federation's point of view. That is how you collect the trust path. Follow authority hints upwards until you hit the trust anchor. Then you go downwards again. You have the public key of the federation operator (obtained out of band). You use that to verify the signature of the FO's jwt. Inside of that, you have the public key of the organization's signing key, and you obtain that, and use that to verify the signature of the deployment.

Now you trust that nothing has tampered with the trust path.

You take the metadata stored in the jwts and you do flattening. You compare metadata at all levels - each level can only issue stuff allowed by the level above it. Cannot add anything that is not allowed by the level above it (for example cannot use elliptic curve if the federation has not allowed it).
Authority hints could contain more than one - so you can get back a tree. If you are an OP and you want to know about the RP, you could, for example, get back multiple federations, and eliminate the ones that are not in your list of trusted roots.

Now we have a way of managing metadata in a way where we can handle distributing metadata in a controlled way.

When you do provider configuration discovery or client registration, the metadata is used.
For client registration, there are two different types: implicit and explicit.
Implicit means that there is no registration going on between the RP and the OP. The RP will have the same metadata, disregarding what OP it's talking to. In implicit registration, you register with the federation, but you don't have to register with the OP. There doesn't have to be an RP client ID in that case. It can use the entityID as its client ID. Then the OP can traverse the trust tree to discover that the RP is a trusted client in the federation. The RP sends an authorization request, sends its entityID as its

client ID, uses its private key to sign the authorization request.
OP can cache all of this so it's not doing this lookup chain all the time. How long is the registration valid for? The OP will reevaluate the chain something like every 15 minutes. If something happens, say the organization is kicked out of the federation, the trust chain gets broken, then the registration just goes away. Otherwise, all the attributes of the metadata jwt have expiration times, and you have to do new metadata registration to renew the jwt/path.

There are variants of metadata: openid-client - openid-provider

Those are the ones we're playing with, but already have use cases for other types of entities which may or may not have metadata.

Roland described how you could use a SCIM federation using this about a week ago.
Producer has keys, consumer has endpoints in signed metadata
Federation operator can specify that a different level can do anything it wants, by not specifying that in the jwt that it signs for the organization.

You can do stuff like baseline expectations by interrogating the clients of an organization using the federation operator's keys to access the interrogation endpoint.
You could do SIRTFI using its own federation, which would be used to define the trust path for SIRTFI organizations/entities.

Format of authority hints is a dictionary where the keys are the superiors, and the values are the trust roots. So you can eliminate trust roots you don't trust.

Mike Jones suggests calling authorities hints, just authorities
If I have conflicting things from two trust roots, what do I do?
If you an RP and an OP use different trust roots, what do I do?

Roland sees this as a problem, but Andreas does not.

Federation A might say you have to use RSA, and Federation B has to use EC
Do you just have to keep trying until you get things to work? Except that doesn't work in the browser, breaks the login flow

There has to be some signal between OP and RP that hints what trust path to use.
That hint might have to be in the authZ request from the RP to the OP.
The RP could say, "I'm in A, B, C, D" at client registration, and the OP says, "let's use B" <-- this means you need explicit registration. Andreas doesn't think this is a problem because he's not thinking of this multifederation use case, maybe?

Example of sources of conflict: HEART and IGov profiles specify which types of crypto you can use, they could be in conflict in different federations that OPs and RPs could be in.
Flattening has nothing to do with OIDC, it could be applied to any protocol
Draft 0.5 of this is an ID in the OIDF right now, and Roland is hoping to have it done by the end of the week.

Testing: GÉANT project has funding to do this, for R&E
If there are others outside R&E, for example health, it would be nice to do testing in the OIDF for multiple sectors.

Swedish K12 use case: SPs want to get continually updated on things like groups, email address, entitlements. So you want to push that info from the IdP to the SP. The K12s in Sweden chose SCIM to do this. They need to find the SCIM endpoint, and need to have the keys to sign the information that you want to send to the SP. They put all of that into the federation.
Discovery isn't in this because you don't want to couple it too tightly.

What Andreas brought into the picture was usage outside of OpenID Connect, to be able to support other protocols. Andreas' use case is OAuth stuff - Authorization Server federation.
Not changing the OIDC OP discovery stuff, we just add new claims to the metadata.
Client is a private client on a cell phone, can you have that RP have its own metadata?
You could host the client metadata somewhere else in that case. But mobile clients probably only belong to one federation, and they can just do implicit registration.

Need people to read, comment and implement this
The implementation is kind of terse, need to add examples/rationale for different choices. Hopefully will happen within the next few weeks.

Until we get several people putting eyes on this and writing code, we won't know what's missing.
There are things currently left unspecified that may need to be specified

Mike Jones contributed an open issues section - one of the things that isn't in the spec is federation operator key rotation.

A cloud provider could run their own federation full of all of their tenants.
Federation represents a relationship of some kind, but different parts of a company have totally different relationships with themselves, and with parts of their customer base.

The_ABACUS: A New Approach to Authorization

Day/Session: Tuesday 5K
Convener: Jacob Siebach
Notes-taker(s): Jacob Siebach

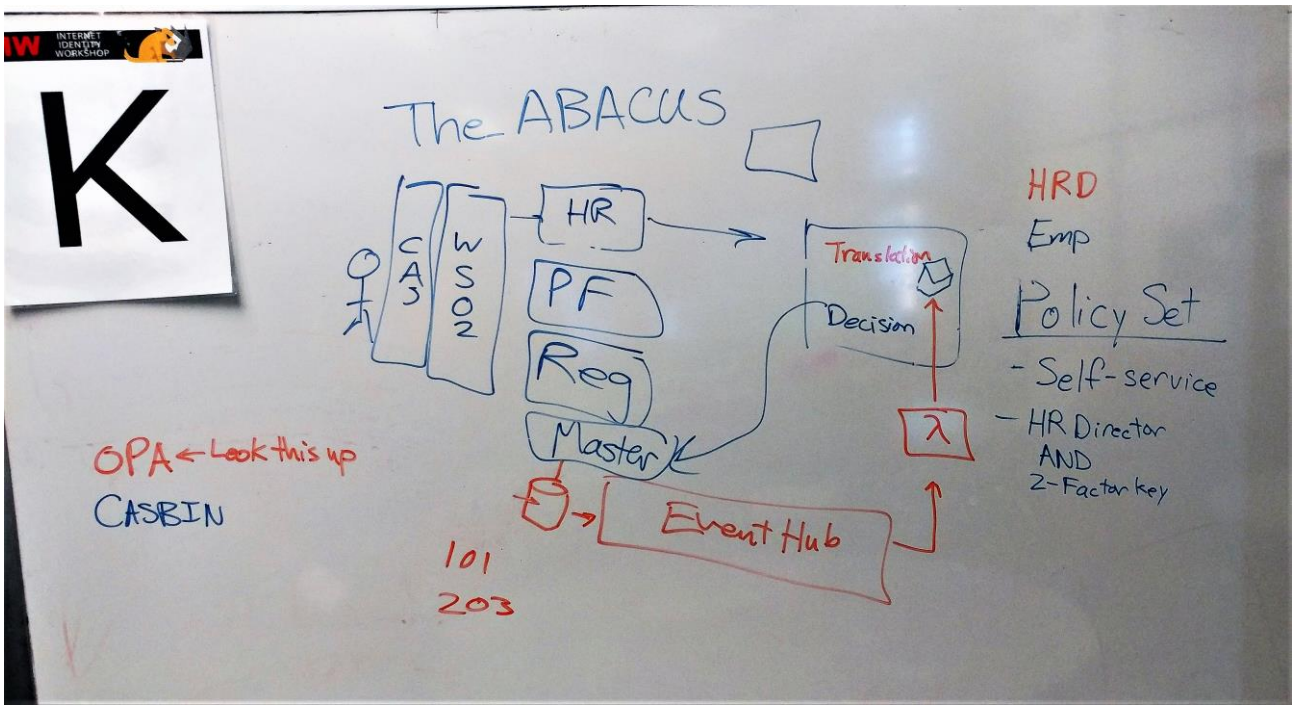
Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

We discussed a method of calculating attributes with no token passing, using request data and attributes.

The_ABACUS is a new type of authorization engine. It begins with a requirement of separation of duties: identification, authentication, and authorization are individually processed.

Policies for authorization exist in real life. If you walk up to someone and ask what the policy is for who can use their car, they'll probably say that they can use their own car, their spouse, their children under certain conditions, and explicitly authorized individuals. Computer systems have similar policies, but usually the policy is tied to the application code. The_ABACUS separates the policies from the authorization check, allowing the business owners to set the policies while the system developers only need to call The_ABACUS to find out if there is authorization.

The_ABACUS accepts requests from services, checks the associated policy, and returns "Permit" or "Deny". The engine is not susceptible to common compromising attacks, it does not have the difficulties of delegate confusion, is optimized for efficiency, can return several decisions in one request, and it allows for complex policies. Additionally, attributes can be updated in real-time with events that are pushed to AWS lambdas. This allows the engine to remain online without ever needing a redeployment while event consumer code can be updated as needed.



Wednesday October 24

Beyond OAuth: Transactional Authz

Day/Session: Wednesday 1A
Convener: Justin Richer
Notes-taker(s): Tom Brown

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

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

Session is related to recent article:
https://medium.com/@justinsecurity/moving-on-from-oauth-2-629a00133ade

See Identiverse talk "What's Wrong with Oauth 2"
https://www.youtube.com/watch?v=OLwz7pIXOWQ&t=6s

Front channel unnecessarily puts a lot of stuff there, so it's a big target

Do not assume syntax and structure will be compatible with Oauth 2

Adding server side call to AS prior to redirect which addresses the following (where I = client app):

1. Who am I? e.g. name , logo (not redirect uri nor grant type. In fact grant type eliminated). This replaces static and dynamic registration
2. What do I want?
3. What can I do? e.g. redirect, display code, open app, do CIBA (replaces grant type)
4. (possibly) Who am I?

After first time, AS can say "next time you show up, instead of sending all this, just prove I gave you a handle"
Design goal of Oauth 2: make clients as stupid as possible

AS possibly boils down to one url with this approach

Client: I want to start an authorization transaction. Here's everything you need to know for what you want to do and I need user to approve this

AS tells client "I need you to do this and when you come back to me, present a transaction handle

client sends user to AS...here's where things are very different (but similar to UMA)

...just send transaction handle (today we call an auth code) with encapsulates everything

state param for CSRF needs to be sent before front channel

mixup problem discussion

only two possible results to send back to user: either the handle or failure. If the user clicks no, then still send handle

session fixation is why we need 2 handles

1. need to prove front channel closed properly
2. binding to back channel

front channel is optional because you might be able to supply enough info that user does not need to interact with AS

Implicit grant is gone!

No more response modes or types.
Downsides: More chatty, roundtrips. Mobile devs don't like to open more sockets.

Verifiable Credentials 101 (How the Sovrin Demo Works) & Concept Map of Verifiable Credential Specification

Day/Session: Wednesday 1B
Convener: Tyler Ruff
Notes-taker(s): Tyler Ruff

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

Link to the slides used: https://www.slideshare.net/SSIMeetup/verifiable-credentials-101-for-ssi-and-decentralized-digital-identity-tyler-ruff

Link to a video of the slide presentation: http://ssimeetup.org/verifiable-credentials-101-ssi-tyler-ruff-webinar-11/

We covered how credentials are currently being created and issued on the Sovrin network, briefly touched on how we're doing Zero-Knowledge Proofs, and covered the blinded master secret approach to credential issuance.

HLIndy Reference Agent: Sovrin Demo + Future Work

Day/Session: Wednesday 1F
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:

Goals and scope of the Ref Agent
https://github.com/hyperledger/indy-agent/blob/master/python/scope.md
[it is not the mobile app]

Dev group: Sovrin Foundation folks, Unveil Social (Nader, Bryant), BCGov

Recent Work

- Built out by HL Intern Kuzma
- Modular message handling by message family
- VueJS frontend framework for Admin UI

Current Work

- Dev Environment [Docker based]
- Agent Specific Getting Started Guide
- Credentials Exchange via UI
- Agent Messaging Protocol Serilization Format
- Tagging code releases to preserve demoability with rapid changes.

Further Work

- Refactor UI messages into Admin Message Families
- Test Agents via Agent Test Framework
- Wallet connection via command line args
- Dynamic User Messaging

Join Us / Rocket Chat: chat.hyperledger.com

SSI in Europe: Getting to an SSI Agenda with Political Backing #SSIpaper

Day/Session: Wednesday 1G
Convener: Kai Wagner
Notes-taker(s): Heather Vescent

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

Link to my google docs:
https://docs.google.com/document/d/10FDsXGI6wEx00F7X520LY4qw3vhfRm_j2ox5Z-AoSKg/edit?usp=sharing

Attendees:
Kai Wagner - Jolocom
Martin - Civic
Heather - SSI Report
Adam - ID2020
Sebastian - Co-IT
Gert - Alexandra Institute
Dominik - Danube Tech
Bryan - Caribou
Kaliya - Identity Woman (pop in)
Alice - uPort
Estee - Gray

- **Introduction Round**
- **Heather:** Report "Comprehensive guide to SSI", SSI needs to be successfully globally. Get informed about different European perspective. Gain comprehensive understanding about SSI throughout the World.
- **Martin - Civic**, have a SSI product, was closed source and now an open source part called Identity.com (targeted to the US KYC market), want to understand the European perspective, Europe has a top down approach and what role Civic can play in the european market
- **Adam Cooper**, ID2020, lots of background from government.
- **Sebastian Miller**, interested in SSI for using it in future for our own identity product. How does this be used in the future. Product/Company - Co-IT, IDconcepts.
- **Kai Wagner**, Jolocom, building an infrastructure technology, token & blockchain agnostic, identity wallet for end user and support IOT identity, Co-founds of the German Blockchain association. Political board based on parties from the German parliament. Gives a state channel with politics. Just published a position paper.
- Position Paper on SSI, published October, 23 2018: https://www.bundesblock.de/2018/10/23/position-paper-self-sovereign-identity/
- **Gert, Alexander Institute**, background in cryptography, working with SSI before that was the name,

- **Dominic, DanubeTech,** similar stuff as Jolocom. Interested to push this idea in Europe because it is important and need to work together to push it.
- **Bryan, Caribou Digital**, more to learn about the EU model. Also do things with Sovrin Foundation.
- **Motivation:** No unbiased documentation around SSI with concern around out of the Box interoperability.
    - Paper contains Glossary that introduces single Terminology.
    - Regulation Chapter around EIDAS and GDPR. How to make EIDAS work with SSI / DIDs.
    - List of interesting use cases, e.g. City of Antwerp, BC Gov

We all know this is a business field and we want to make this a business, but there is an area of cooperation and an area for competition. Which levels/layers do we work together and where do we compete. There is no reason to compete on the lower levels of the stack.

Funded by people who want to do this - it's all voluntary from the people by they are paid by their organizations for partial participation.

Goal for the report: to stand out there for 1 year as a source of proper basic information.

We want to have this concept of SSI put into the EU - European Commission, EU Parliament. But also the Dutch Blockchain coalition, and other actors interested in pushing for this. Pushing for this on an EU perspective, scoping one vision of what we want to accomplish with SSI in Europe. Consensus on the regulations and what we want to achieve. Vs the technology goals.

What are the specific regulatory goals we want to achieve? (more SSI funding to roll it out?)
What are the specific European goals with SSI?

Impose standards and Levels of Assurance for member states. This is what we understand and trust about this.

Two levels of regulation
1. electronic identity
2. trust services

Does there need to be a SSI regulation?

Leverage the trust we have in national identity schemes. The real usage is in private sector services, not public sector services.

Competition -

Can there be two approaches? Private sector and public sector adoption?

To get accepted on a smaller level - there are tiny pilots. There is no good place to go to find out where are the pilots and how they are going? There is one common understanding of SSI in europe.

W3C should play a role, but one of many…
Same with DIF.

There needs to be a thing to tell the concept, telling the layers, what standards.
A European SSI perspective. We are informed by W3C and DIF… but it's a good place and resource for european politicians to check in with SSI and to be updated. To position SSI in Europe. Providing an actor/entity that people can discuss blockchain and public sector.

Examples of this type of thing?

- Horizon projects, eg Horizon2020
- Decode Product (Barcelona & Amsterdam)
- MyData

These are limited time projects. And maybe a research project with a time horizon, might be able to address these concerns.

There is a research consortium forming in Austria - maybe we can bring them together? Why not try a horizon application and build a EU coalition ourselves?

Funding gives you commitment, funding to an initiative, it says you've made up your mind. Not a lot of money channeled, but there is a lot of talk…
Unfortunate because there is a discussion.

How can we get a few actors to commit to this idea?

Idea: Might be helpful to pitch it into a policy objective.
Banking authority around KYC - the banks are interested in doing identity because of that.
Banks are interested in cross-border, because they are linked.

Final thoughts

- Dominic: I like the horizon project
- Gert: Doing an application is a start
- Sebastian: interested in how I can use SSI (use cases)
- Adam: Funding point, SETH?

SSI is Coming & "Moon Coin" Tying the Digital World to the Physical
(a discussion)

Day/Session: Wednesday 1I
Convener: Mike Graglia & Jacob Siebach
Notes-taker(s): Timothy Robustelli

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

"SSI is coming/here, society is built on registries, how must registries evolve given SSI?"

- Registries connect people to stuff
- How do we connect people to the digital
- Future of Property Rights at New America > job help people in property rights world think about emerging technology to help them do their job better

- Property rights is great for socioeconomic development
- Blockchain for land registries last year
- Write paper that explored Everest, Sovrin, and uPort
    - Arguably three important players in space

- Assume SSI is successful worldwide, what does registrar do
- IADB > builds asset registries, collatarize asset, get loan against that asset
- Rare disease registry space > shitshow
- What does a registrar do > buy land, spend money on notary to prove you are you, and sign document
- As world becomes digitized, registrars are spending more time on identity
    - Recognize utility of SSI

- Registries go from source of truth to issuers of verifiable credential
- WB spends so much time updating registries, then 10 years later, its helplessy outdated
- If transactions are held in wallet, registries can be automatically updated
- In the real world, when SSI is a thing, what will all the registries we depend on have to do differently?
- Registries won't go away, but will have to change

Discussion

- What prevents registry updates from happening?
    - Why would some people bother?
    - Will says I have land, why would I take time out of my day to tell registrar
    - Leverage tech to automatically update it?
- Titus: more than tech, think of incentives for people who don't participate in the system willingly or properly
    - Punishment?
        - Taxes if you don't update every 6 months or a year

        - Sell property and don't update, fined
    - Punish people for life happening?
    - Punish people for not following worlds?

- Punish for not complying with system…people say that you need to change the system

- Data flow?

- Registries, go away? Who issues credential?

- Data that people don't want in the domain, but that we still need to record

    - Bankruptcy?

- Sari: Oracle problem
    - What do all these legacy systems and businesses do in the future
    - 2 new spaces
        1. Organization deals with oracle problem
            a. Land physically changing over time
            b. Somebody needs to connect physical to digital
        2. Different businesses that offer services for data disclosure
            a. Keep some private information private
            b. Services that help me curate information in the right way
            c. Help me self myself to digital services
            d. "Digital Bridges"

- Can't just have the carrot > need the stick?
    - Has been shown throughout history

- Trust system has both
    - Good actors
    - Bad actors
    - Trust score fluctuates based on behavior
- Can't just hide stuff that we don't like about ourselves, not OK

- Fix them or deal with them as they are
    - Not showing credit score
    - Not showing medical history

- Trying to hide stuff?
    - "Have to disclose" is not the best way to approach it

- Moon Coin > redeem coins for physical value

- Push something into digital domain, extract it into digital domain seamlessly
    - How?
    - Do you need a registry to do this?

- That's just an exchange…I can convert my crypto

- Registry creates value
    - Own house, protected by state, because I have record that says I own my house
    - Build something difficult that is of value

- Abstract representation of value
    - Piece of paper is representation of something of value

- Registries are valued because the public is interested in the information in the registry
    - Taxes
    - Cars
    - Animals?

- Very differently handled in different countries
    - Denmark, land degradation
    - Valuation, property taxes, in govt interest
    - Some countries, jurisdictions have open data, some do not

- Digital Identity of land, asset within registries?
    - Can't use that identity even though data are public
    - Can't see service end point?
    - Create secondary registry?
        - Making copies of registry?
        - Adding photographs of assets
    - Need end point to use data

- Public registries, registries that state, organization manages
- Today, many are digital
- Society allows them to exist b/c they create value

SSI and how do registries change?

- Don't just have SSI, and don't just have state
- Liminal time, things are changing

- SSI w/ bad credit score, out there publically in a black box
- W/ SSI build other things into it, that gives a bigger picture
- Credit risk worth taking, based on recent positive behavior
- Tool for redemption
- Show more about what is in black box
- All registry things will be richer for it
- Role for state, get taxes, not going to go away

Birth registries > services?

- State credentials denied to kids in border states b/c of midwives
- Hospitals are trusted entities to issue birth certificate
- Birth registry entitles person to request citizen from state
- Same refugee from village, with SSI, village elder, aunt at birth, matches up to footprint, builds up a claim
- Imagine it as a richer world

- Digital and physical world coming together
    - Really want to tie it up

- Gaming?
    - Are virtual worlds
    - Start up from Korea
    - Identity for gaming for next 5 years
    - Already be source of identity for Korean kids because already met them in digital world

- 1.5 billion w/o birth records?
    - People living totally in physical world
    - Should be able to enter digital world

- Titus: credit scores are not black box, more encompassing and transparent
    - Know how to increase score
    - Good to bring in circumstances through SSI

- Titus question: fundamentally strange to talk about SSI, states, registrars, one core power of SSI is to generate identity?
    - SSI believes that I am sovereign as myself
    - Now: tied to passport, driver license, bank account, birth certificate
    - Singular, atomic entity

- Don't exist in a vacuum

- Jamie: e-government space, connecting people to registries
    - SK, Cananda
    - Allow people to register digitally
    - Can use verifiable claims based on their behalf to level up
    - Instead of creating identity on platform, can you bring SSI onto platform
    - Can it be transferable?

        - Should be able to take across jurisdictions

- Lot of talk about people coming into fed govt
- Innovation at local level
    - Recognition of property rights
    - Mayor wants to provide services

- Going to start to see federal governments confronted local solutions that are better
- SK solution > consumable at federal level

- Question: who are you working with in SK, scale?
    - 2015: build up in province
    - Working now with provinces and fed govt
    - User centric first, attaching things to user, and then making in consumable
    - Business using identity to having confidence that I am who I say I am
    - Confidence that people are who they are, digitalize interactions across lots of miles

- Proves that it works bottom up

- SSI = chooses to associate, others don't

- Some people choose not to be part of community, society
    - Attach myself to this

- What you're talking about is really agency?
    - Continue to have agency that you have in the physical world
    - Concept from Middle Ages, Catholic Church, subsidiary, means decisions should be made at the lowest government level possible
        - More buy-in along the way
    - Remarkable thing that we trust higher-up

- But we can't just build from top down for SSI, need to build from bottom up with agency and build trust up

- Titus: difference between land registries and voting registries (voluntary somewhere)
    - Passive land owner in certain country > benefit from roads, infrastructure, electricity
    - Want to take things for granted
        - But can't take those things for granted in SSI

- Crumbling from top down?
    - DMV
    - Know this is a known problem, but not telling b/c don't want people to not trust the system

- SSI, decentralized registry
    - Verified by people in community
    - Say baby is born
    - Have biometrics, put into system

    - Verified by people there in community, certain number of people
    - GPS feeds into it
    - Certain levels of info

- SSI allows us for richer, more complete data set
- Whoever is in charge, will still want a more or less centralized registry
- Why does mayor want that list?
    - Taxes, education, health, demographics
    - Vital records are step one

- Not mutually exclusive > SSI and registries
- Analogy
    - Plumbing and check valves
    - Check valves can be built into system
    - Data goes out for public services
        - Really want that as a society
        - But need to re-build faith in it
        - New generation
            - Need to understand that everything on registry can be trusted

- **HOW WILL IT FEED NEW INFORMATION?**
- Sari:
    - What mayor needs to predict public services
        - Data, statistics
        - Don't need registries, only need information?

- What if I don't want to share that data?
    - Community consensus

- Lots of services we take for granted, all informed by the census
    - Depends on society?
        - In some countries?

- Phil and Jamie
    - Someone from Canada
    - For something in Canada, need to prove name, using driver license, passport, tribal identification document
    - All of these things layered on top of it, need PCTF before you can do other things
    - PCTF (Canada)
    - Some people don't want to use tribal identification card b/c of discrimination
    - Foundational identity > service needs to know that you are a person, not that you're a tribal person
        - Layer between the two
    - Verifiable claims that sit on wallet, SK holds wallet
        - Future…sees holder as citizen, and citizen and government

- Denmark and Canada

    - Trust in state is high
    - How do we build pipes, user more and more in digital space, more control over data
    - How do registries stay current for purposes of state, and how do we still control our identity

- Jamie
    - Do transactions digitally through trust, confidence that I am who I am

- Jacob
    - Layered too high?
    - Communities do it their way based on local framework

- Mike
    - Rare disease registries
    - Have to document it, can't do research w/o registries
    - Registries are standardized
        - Researchers don't know where to being
    - Point: when we allow everyone to be a little different, no standardization, allow for problems in the future, problems for interoperability
    - Really nice to have standardization for land registries
        - Polygon
        - Owner
        - Rights

- Is SSI linked to registries?

- Drummond Reed:
    - Talk about SSI
    - Point of layers
        - Three layers
        - Bottom: IDs
            - High-level interoperability
        - Second layer: SSI
            - Exchange of verifiable credentials
            - Digitally signed using DID layer below it so we can have trust
            - Schema for any credential is registered on public blockchain
            - No enforcement to use schema, but interoperability actually favors that
            - Better chance of smaller number of schema, but greater interoperability of credentials
        - Third layer: Wallet?
            - Agent to agent communication
            - Hand is built into digital wallet

- Agent to agent communications at third layer?
- Land registry > associate with a DID, if owners have a DID, along as connections persist, maintain connections, capability that wallet can do is to build policy frameworks for changes that take place
- UPDATE, send message, update credential

- Helps, doesn't solve it

- BC Gov
    - Businesses change names, use different name, type in wrong name
    - Building software that updates names automatically
    - Name change comes from a verifiable credentials
        - Built on layer of SSI
    - One register to another > Europe, only need a credential once
        - Held in one country
        - Share registry ID, all other entities that need data, can query data
        - Credential given once by authoritative issuer
        - Other registries do not keep old data

- Titus: exchange of verifiable credentials
    - Registrars stop issuing credentials
    - Just use neighbors to start issuing verifiable credentials
    - Mike: 81% hackable
        - 4 neighbors just back me up
        - That's when registrar says "that's when you need me"

- SSI: create minimal set of information in registry that you couldn't before
    - Less risk of hack, less risk of honey pot
    - All valuable information is in the hands of the user

- Joyce: early days of computing, didn't put everything on computers and stop using paper, think that is what raised trust in what computers can do, but no everything gets hacked, mental shutdown, transitional time, add this and it will be richer, at some point, move things on register
    - Mike: registrars are going to need to interact with this for registries to begin

Signed Data (JSON – LD vs JWTS or Something Else)

Day/Session: Wednesday 1K
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:

There are pros and cons of json-ld-signatures vs JWTs. While this was a general conversation it was seen in the context of W3C Verifiable Credentials.

JSON-LD

Pros:	**Cons:**
- Semantics - Graph - Human Readable	- Difficult to integrity/canonicalization of graph for signing purposes - Canonicalization requirement - Difficult to understand what is signed - Cognitive overload when understanding data - Lack of diversity in tooling - You have to really know what you do to verify a signed json-ld document
Asks of JSON-LD community to make it useful for Verifiable Credentials: - Better Tooling (automatically resolve DIDs and verify signatures) - Better documentation for specific use cases - Middleware for various server implementations to automatically verify signatures etc of json-ld requests - Remove embedded schema	

JWTs

Pros:	**Cons:**
- You always know what is signed (easy to verify) - No canonicalization needed - Good tooling	- Key definition/lookup part is not very well defined - No built in semantics/schemas - Not Human Readable
Asks of JWT community: - Libraries should support DID resolution (eg implementation https://github.com/uport-project/did-jwt) - Help work on defining Verifiable Credentials using JWT	

Myths of SSI

Day/Session: Wednesday 2A
Convener: Rouven Heck & Timothy Huff
Notes-taker(s): Heather Vescent

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

Link to my google docs:
https://docs.google.com/document/d/1iflXWqPGTe9wIR5hfIvS1fyluyVUDiU-qq6opF3WqXc/edit?usp=sharing

Rouven Heck, uPort (RH) & Timothy Huff, Evernym (TH)

Seven Myths of SSI

1. Self-Sovereign Means Self-Attested
2. SSI vs Government
3. SSI = National ID
4. SSI = Absolute Control of IS
5. There's a main issuer
6. There's a main method for Auth
7. SSI vs user centric Identity

Detail discussion:
#4: Do you have absolute control or not?

T. Ruff: it's about a container. It's a wallet, but so much more. It might have a history of your interaction with others. It's more like a dashboard or control room for how you interact with people. Wallet is a limited word to call it.

Absolute control = if I get these credentials and I put them in my wallet, they are mine, I have the keys for them and DIDs for them, and no one can take those away from me. And I hold these in a service provider/wallet, but if I don't like that wallet, I can go to another. The apps are no longer a platform, they are now a service provider.

The possession of that license is mine.

Driver's License:
THe DMV is the issuer (this goes to #2). The DMV is an issuer and issue a digital driver's license. You have physical possession of the file. But then, I drive drunk (the license didn't expire), but the credential is revoked.

Revocation is important.
They can't take the credential out of my wallet, but it can be revoked.
I can prove that I have a revoked driver's license. But i can't prove that I have a valid driver's license.
Revocation gives the issuer the control.

Adrian: Seems you are missing a federated identity perspective. The fact we don't have those people up there, means we're missing something.

TR: Yes, but that is out of scope of this conversation.

Martin: The verifiability of the credential is not in your control.

Phil: What does sovereignty mean to a nation? You don't have control outside the border, you act as a peer. Same thing here.

RH: slightly different: as long as I have all my identifiers, I have "absolute control" over that. E.g. my ID card expires, but I am sure I can still use it in a bar, but maybe not to get on an airplane.

TR: Agreed. There are aspects of SSI that are absolute, they are mine and don't go to others without consent.

RH: Where are the use cases where this is critical, what are those use cases?

#6: There's a main method for authentication

Asked: do you use biometrics?

What did you mean?
TR: SSI is a set of protocols, it doesn't dictate which method someone uses. Some assume we are an IDP offering a service, and we do it a certain way. It's any authentication method you want to use...

MMPA = Mutually Massively Parallel Authentication

What it means, when I am interacting with my financial institution, we can be measuring credentials during the interactions - location, biometrics, email

Why do I want my bank to stop authenticating me?
And it goes both ways. No more phishing. Because I can authenticate the bank through these same methods. Out of band point to point connection - why is there any limit?

You can use any method #6 is a myth.

Question: Can you put DID Auth in context?

TR: it's one method? DID Auth is about protocol. I am talking about a modality of doing biomentics, a certain way of doing DID Auth.

Follow-up: I'll be more specific. Want to ensure the work we have done on authentication can be reused, and that is unclear - e.e. WebAuthN. Can that be used?

Ken: Yes, DID Auth is a protocol you can interact with. You put a translator device btwn OAUth service between that and DID Auth. So you can build a tran
Followup: DID Auth is more like DID AuthZ, instead of DID AuthN.

Ken: yes, but taken off line.

Adrian: Can a thing or a document have an SSI or just a DID.

RH: Yes…

AG: Does SSI apply to that agent?

TR: DIfferent between independent identity and SSI. Things. E.g. infant. But can't be self-sovereign. Sovrin has guardianship works for things. Btwn a SSI individual. An organization.

HV: asking questions about corporate, NPE Identity,
Are they SSI?

RH: not in agreement that companies are self-sovereign.

PW: Mutlisource identity. All SSI is necessarily multi-source, but not vice versa.
Someone or a thing under guardianship has mutlisource… someone else is making choices bc I am under guardianship.

RH & TW do not agree w/ PW

#7: What is the difference?

RH: FB is user centric, always about the user. But it's not under my control.
TR: I get mine from Christopher Allen - He goes into user centric identity, was supposed to be like SSI but the tech giants came in and co-opted the concept. But now user centric identity uses a 3rd party - and IDP that is involved, and it feels like its yours, but it's the entity that is giving you your identity and it has control over it.

Follow-up: There's no such thing as a SSI service?

TR: Yes, there is, but you can fire it.

PW: Gives the history of IIW, URI, etc. It's not simple saying big companies corrupted it. What we got was OpenID & UMA and a boon to move people in the right direction. SSI is not a redemption of user centric, but an evolution.

Question: what is a relationship or claim that an SSI can have that a SSI can not?

If you think of SSI as a container only you have the key too, you have a place where the DMV can give you a credential. It's giving everyone a container, and the issuers of the world have a place to give you something - to issue the digital credentials. Right now everyone has their proprietary way of doing things… e.g. Apple wallet.

Follow-up: The container is my SSI.

TR: Yes, but it's not about the container, it's about the relationships you can have because of the container.

Question: How does the DID fit in with your view of an SSI?
Impression is you can take the claims and move em elsewhere, but DIDs are not transportable…

RH: We want to have something to be interoperable, the work to enabling thing to build an ecosystem, it's an enabler to build this.

Shouldn't lose your DID when you move from Sovrin to something else. How do we make this possible. The DIDs allow you to rotate keys. I can make an update to the DID Doc with my new keys… so DID is the same, and you tell the world the new keys (after key rotation).

Andrew Hughes: It's not a thing, it's a philosophy. Talking about SSI as a thing in the world, is not possible, it's an approach, a philosophy, not an implementation of anything.

CIVIC and uPort are using the same DID method. We are all in an early stage with these wallets. But we have not done a successful move… yet.

TR: There's an argument, take a point in time today - it's not SSI today … but the designs are there and we're moving there and there are standards. "Don't punish a freshman for not graduating yet."

Johannes E: what is the failure mode?

TR: How do we make it sustainable?

Kyle: I think it's economics.

JE: When I hear you explain it, that's what I heard so many times. So I want to hear, and this is why it won't happen this time.

PW: I don't know I know all the failure modes. One is: platforms provide natural monopolies. One way you can see this, having a natural monopoly - there are service providers - some are better than others. But all of them are run by a single service provider? How to combat that? One way…. (disclaimer, not an announcement) is to instruct the economic incentives to disincent that kind of natural monopoly. There are thoughts about how to do that.

Martin: Question: about the relationship. Is provider specific? Who defines this relationship?

RH: We don't know the right schema … I assume it will emerge.

Question: back to 10k rides, how does this solve from platform to platform.

TR: just an opinion, a new service gives reputation to share that.

Fragmentation?
Reputation - rabbit hole. It gets complicated.

Adrian: Why it's not gonna slide (answer to JE)
THe value of aggregating data because things are connected. The technology cost goes down. (Moores Law).

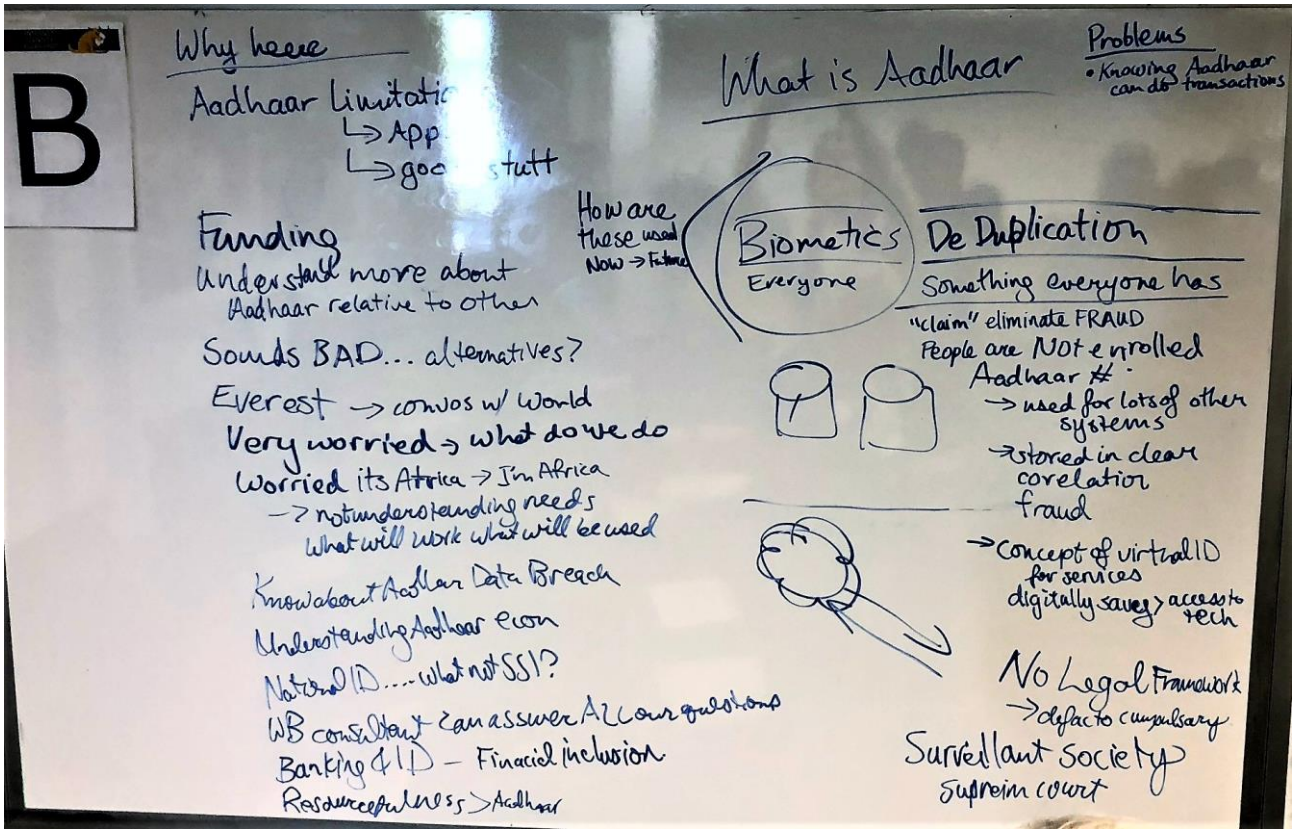
TR: the environment for regulation is high now… there is wind in our backs to make this happen and drive adoption through business channels.

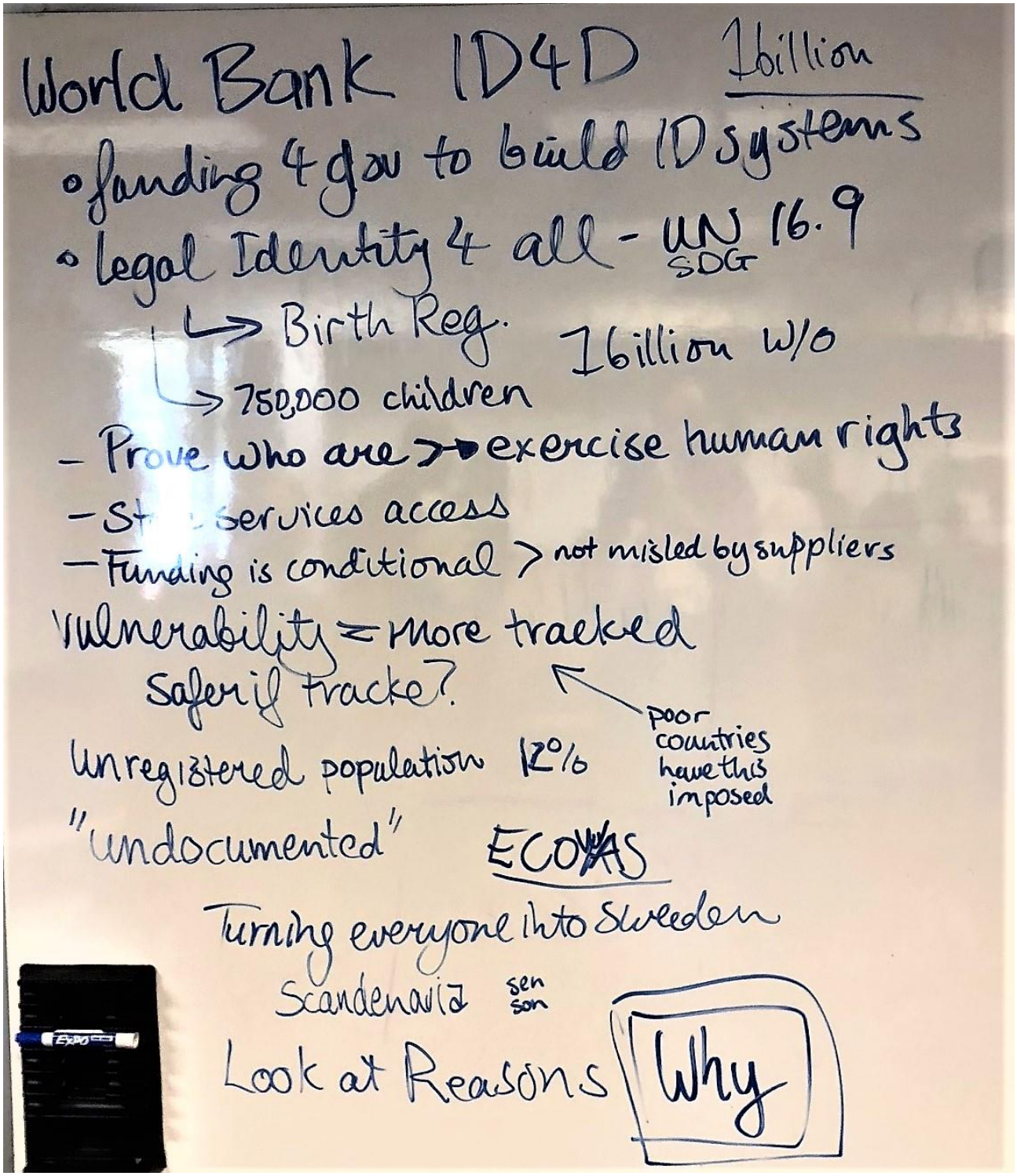
Comment: In Heathcare you have government mandate that you own your data. There is something that has to be dealt with the people holding your data. And they make it difficult to share your data…

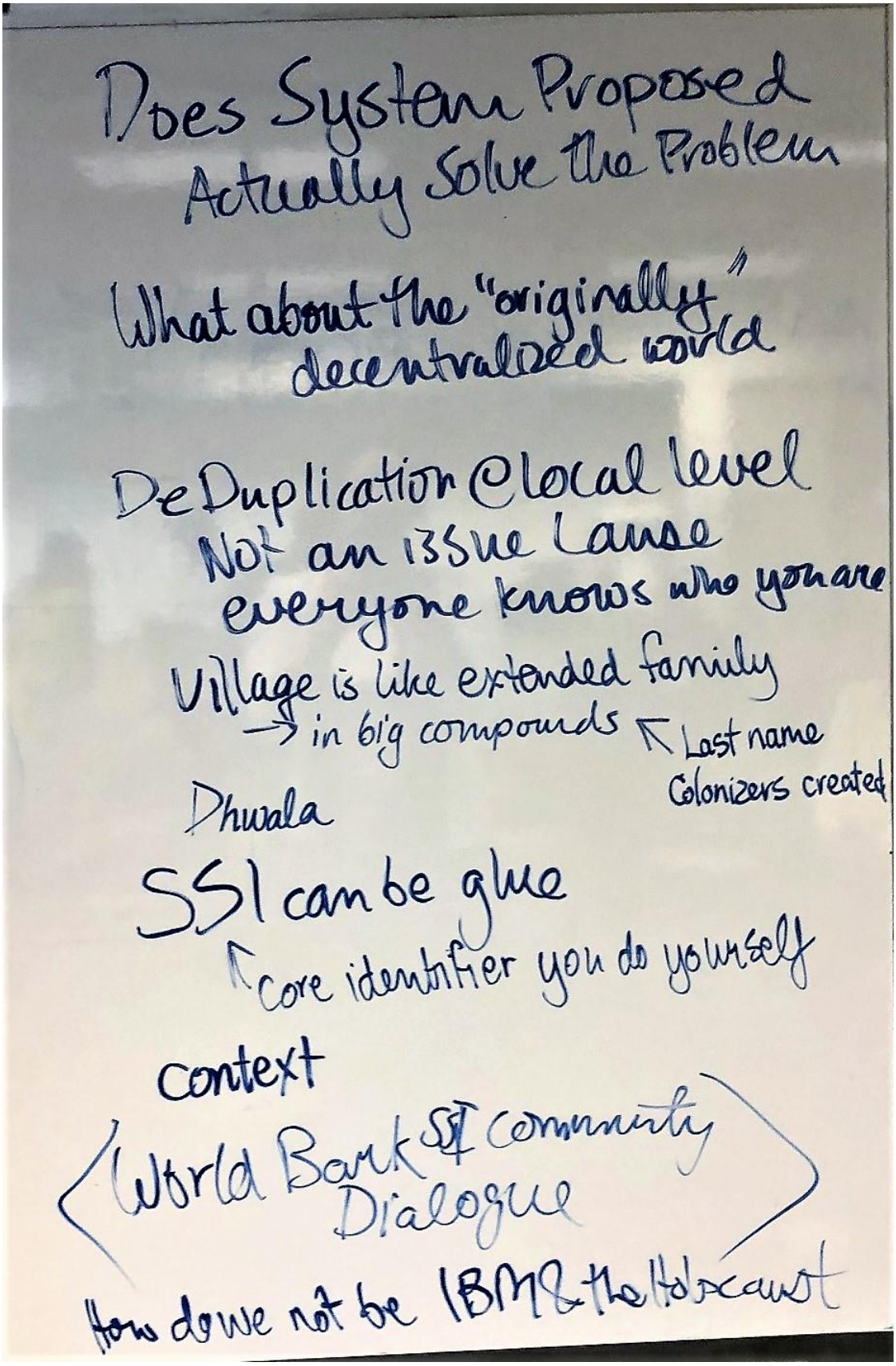
Identity & World Bank Funding. 1 Billion in Loans to African Countries for Aadhaar Like Systems – Could This Go To SSI Systems?

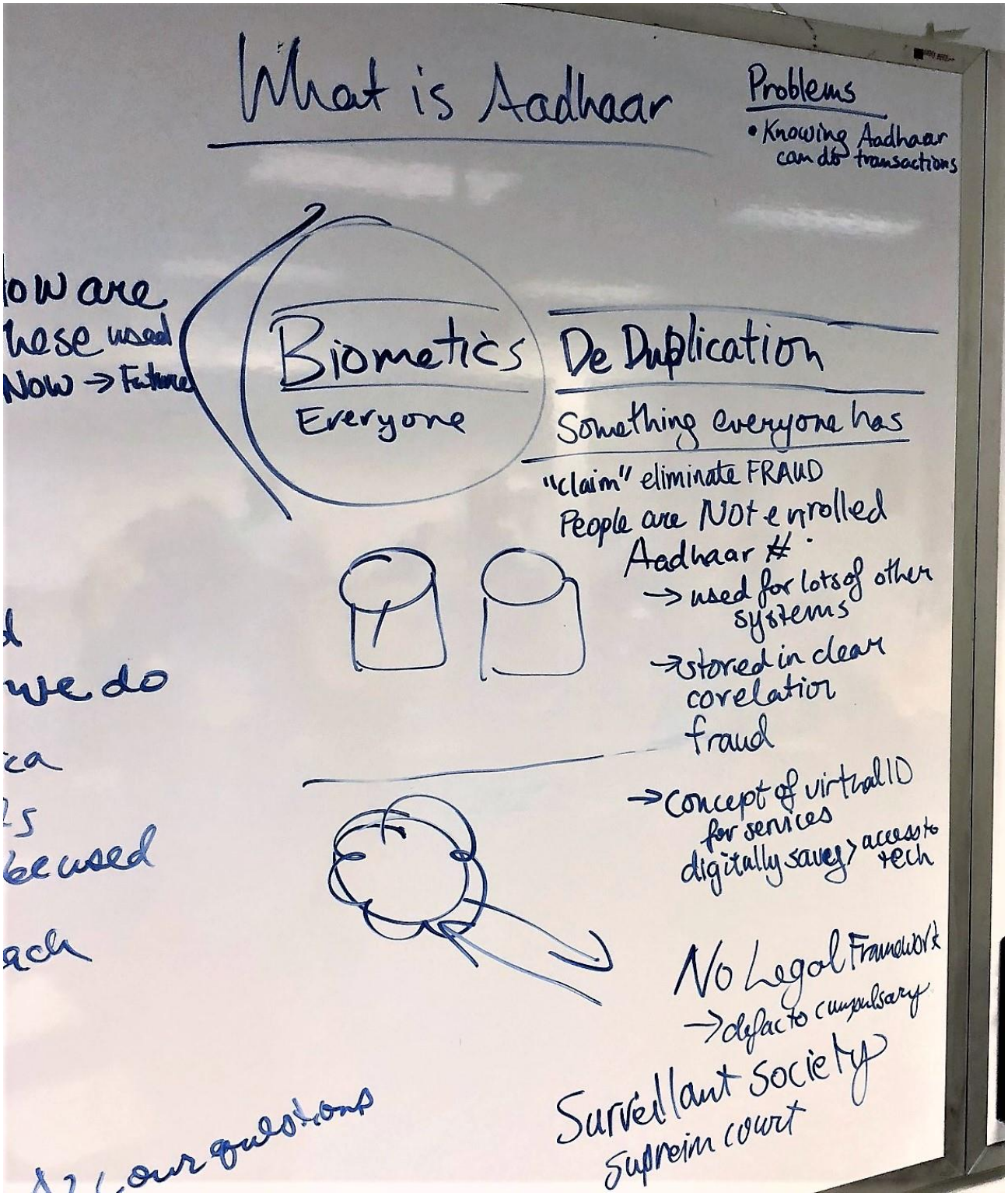
Day/Session: Wednesday 2B
Convener: Kaliya Young
Notes-taker(s): Kaliya Young

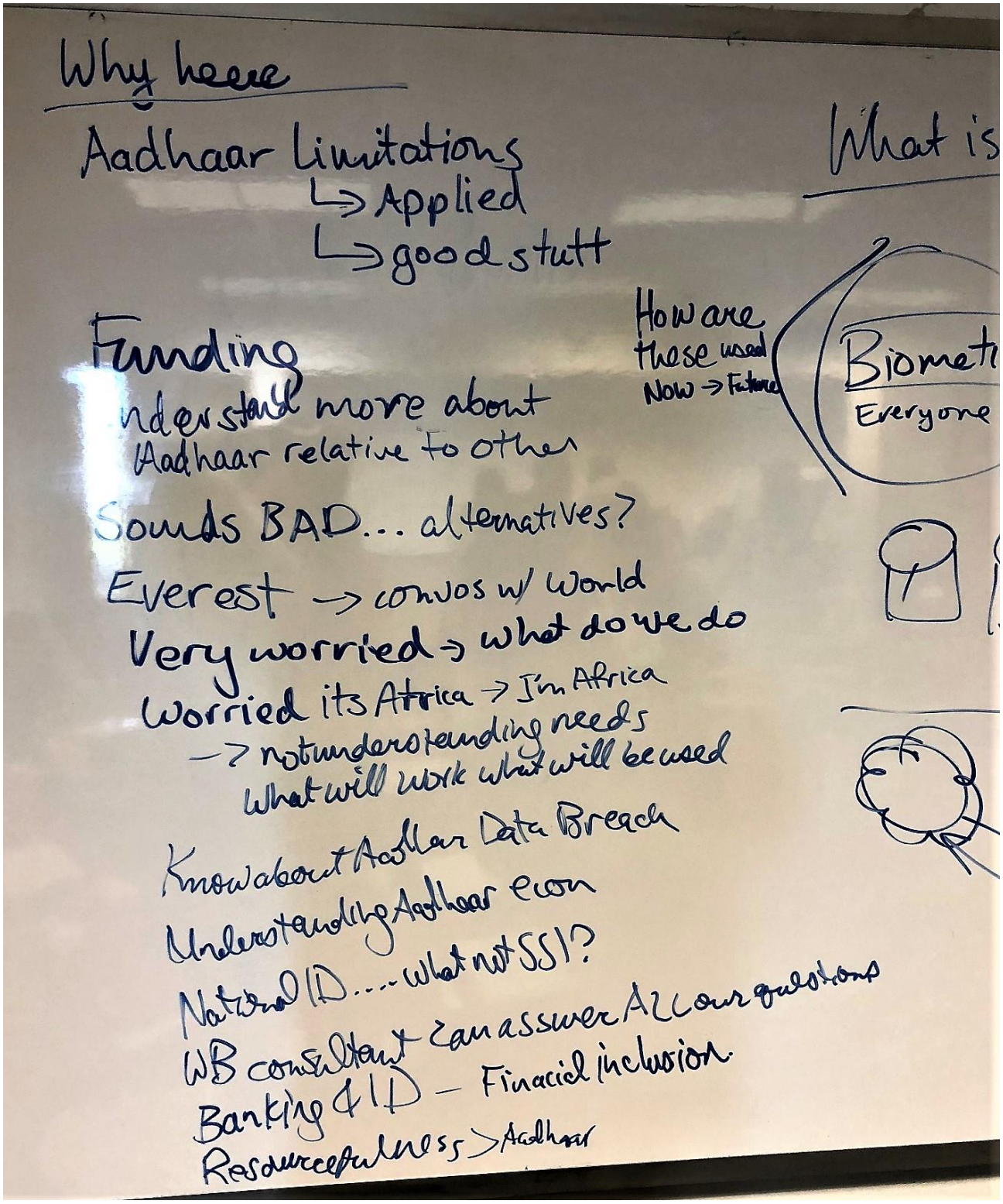
Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:




World Bank ID4D 1billion
• funding 4 gov to build ID systems
• legal Identity 4 all - UN SDG 16.9
↳ Birth Reg. 1billion w/o
↳ 750,000 children
- Prove who are → exercise human rights
- St services access
- Funding is conditional > not misled by suppliers
Vulnerability = more tracked
Safer if tracked?
poor countries have this imposed
Unregistered population 12%
"undocumented"
ECOWAS
Turning everyone into Sweden
Scandenavia sen son
Look at Reasons
Why


Does System Proposed
Actually Solve the Problem
What about the "originally"
decentralized world
DeDuplication @local level
Not an issue Cause
everyone knows who you are
Village is like extended family
→ in big compounds
↖ Last name
Colonizers created
Dhwala
SSI can be glue
↑ core identifier you do yourself
context
World Bank SSI community
Dialogue
How do we not be IBM & the Holocaust


What is Aadhaar
Problems
• Knowing Aadhaar can do transactions
Biometics
Everyone
De Duplication
Something everyone has
"claim" eliminate FRAUD
People are NOT enrolled
Aadhaar #.
→ used for lots of other systems
→ stored in clear corelation
fraud
→ Concept of virtual ID for services digitally saves> access to tech
No Legal Framework
→ defacto compulsary
Surveillant Society
Supreim court


Why heere
Aadhaar Limitations
↳ Applied
↳ good stuff
What is
Funding
nderstand more about
Aadhaar relative to other
How are these used Now → Future
Biometr
Everyone
Souds BAD... alternatives?
Everest → convos w/ World
Very worried → what do we do
Worried its Africa → I'm Africa
→ not understanding needs
What will work what will be used
Know about Aadhar Data Breach
Understanding Aadhaar econ
National ID.... what not SSI?
WB consultant can answer ALL our questions
Banking & ID – Financial inclusion
Resourcefulness > Aadhaar

Usability for Developers Applying Lessons from TLS to the Blockchain

Day/Session: Wednesday 2C
Convener: Kent Seamons
Notes-taker(s): Kent Seamons

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

Summary:

We reviewed recent research to simplify TLS application development and discussed how to apply this approach to simplify development in the blockchain space. The discussion expanded to cover usability for two-factor authentication. We also talked about often-neglected user populations that could benefit from more consideration for usability (elderly, etc.).

An Interactive Sovrin Demo II

Day/Session: Wednesday 2D
Convener: Michael Boyd
Notes-taker(s): Chris Matichuk

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

Link to 4 Videos…I did not shrink them. Watch in order.

https://drive.google.com/open?id=1-9FQRdC9KDuEK3ii7hmCfEgWtbBktd0B

PRIVACY CHAIN: A blockchain-based system for consent management for data supply chains.

Day/Session: Wednesday 2F
Convener: Arthur Coleman, Joe Hsy, Titus Capilnean
Notes-taker(s): Joe Hsy

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

Link to slide-deck, presented by Arthur Coleman:

https://drive.google.com/file/d/1Rdssq8Yxo8GwtZ063Q5UyZzX3TKgbXNu/view?usp=sharing

Notes from Joe Hsy:

- There was concern with putting PII information on the blockchain. Clarification is that the consent ID is put on the blockchain so no actual consumer ID is on the blockchain. Also, only information on what data and uses are consented to, but not the actual data.

- Discussed the possibility of putting DID on the consent. How to maintain privacy but still being able to authenticate as to who owns the consent and can modify or revote it. Seems doable, but more details will be required.

- There was a discussion on how many publishers are using the shared consent daisy-bit cookie. Oath is using it, but not clear how many other publishers are writing or using that cookie as many publishers are doing their own.

Fixing Enterprise IAM: Automation, Self-Service, Security, Rapid Adaption

Day/Session: Wed 2G
Convener: Jon Lehtinen
Notes-taker(s): Jon Lehtinen

Tags for the session - technology discussed/ideas considered:
Self-service, automation, containerization, devops, identity governance, single sign-on, OIDC, SAML, Virtual Directory Services, MFA, identity governance

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

As identity/security professionals AND individuals, it is in our interest to make sure enterprise environments are running modern, hardened identity stacks to not only prevent the breaches that damage the business, but also harm customers through the loss of their data. The issue is that the

enterprise is often loathe to spend the money necessary to modernize their IAM posture, or staff it to the level equal to the challenge. As such, we want to explore and discuss the strategies we can use to maximize the impact of our efforts in modernizing the enterprise IAM stack to protect the business and customers, while working within the monetary and staffing constraints imposed upon most IAM/security teams.

Self-Service & Automation as a force multiplier/cost savings measure
Infrastructure and Operations

Containerization, devops, and cloud-first design
Rapid iteration/upgrade of IAM systems through containerization

-Opportunity for CI/CD pipelines to refresh container images for automated redeployment when task/container fails

-Frequent environment rehydration sidesteps costs/staffing/time involved with maintaining long-lived servers

What services are candidates for cloud deployments?
SSO (particularly federation services)

-Participants felt this is fine for cloud/container deployments

-Allows good user experience for a global workforce

MFA

-Often offered as a cloud service presently. Offering to the business as a function of the SSO service reduces friction and eases integration/consumption of MFA by keeping the application integration aligned to SSO using protocols like OIDC & SAML.

-Step-up auth available to app teams via an end point or API

-Special integrations may still be offered (e.g. offline & ssh)

Privileged Access Management

-NOT recommended for cloud

-Hypervisor attacks could lead to theft of vault

Directory Services

-Attribute stores close to IDP for cloud deployments

-Credential validation could be isolated to its own VPC with explicit access only granted to the SSO system. All other applications could perform LDAP attribute lookups using an attribute store on a separate directory.

Identity Governance

-Was not discussed, though this is offered as a cloud-based/SaaS offering from some vendors.

Application integration to IAM services
SSO self-service

-Offer API for Oauth/OIDC client registration (such as dynamic client registration) for technically proficient internal customers/app teams

-Offer friendly GUI to that API for the non-technical internal customers who must enroll an app into SSO

-Documentation, customer engagement, open office hours, and templated solutions reduce the friction for delegating the work of app integration after issuing the "hook" to the IDP

-OIDC further reduces this friction as certified solutions for various languages/middleware facilitate the migration to OIDC from other access management solutions.

Push for OIDC over SAML

-OIDC is much simpler for self-service

-Dynamic Client Registration can be called after some sort of governance flow (like service now) that includes security, technical, and business approvers.

-SAML is HARD

-SaaS apps as each SaaS app has its own schema and requirements

-In previous org, the convener ultimately built a comprehensive self-service portal to accommodate several use cases based on customer feedback using a product management strategy, but that took time, and we functionally built a very friendly skin of the IDP administrative console by the time we were done. And even then it could not handle every SaaS use case.

-Internal apps can be forced to use a prescribed attribute package

-High hopes that FastFed will ameliorate this, but even after ratification FastFed will depend upon adoption by SaaS providers to improve this situation

IGA self-service

-This was hard. SCIM was supposed to help, but not as many SCIM ready apps as we thought there would be by now.

-Produce a frame work for self-enrollment for applications into authorization/entitlement enrollment/workflow review using Oauth tokens to delegate the auth prior to writing the connection in IGA

-Requires IGA-specific hooks to implement on a per-product basis, but would improve what is presently a tedious and time-consuming process.

Directory services

-Offer virtual directory views to applications which require LDAP through a self-service portal

-Requires individual integration with virtual directory product, no standards-based protocol to write the view

-Do you even want to offer LDAPS in such a fashion moving forward for your business? Remember your strategy. Increasing friction on old protocols and making newer protocols easier to consume can help drive the business in the direction needed to retire technical debt.

Fine-grained authorization service for applications?

-When offering self-service for SSO via OpenID/SAML, coarse grained use cases are addressed

-Very rough authZ decisions are made/enforced at the IDP at the time of authentication, e.g. terminated users cannot proceed.

-Is it desirable to offer a centralized, per-app, fine-grained authZ policy service?

-Discussion indicated that NO, enforcing coarse-grained AuthZ at the IDP was sufficient, and that fine-grained authZ could then be delegated and managed by the application owners as a function of their SSO integration.

-UMA2 endpoints could marry central policy management with self-service and per-app edge enforcement

-An app owner defines the policy (including per-path authZ policies using the UMA2 endpoints), and registers the UMA2 client using self-service. Now there is a record of fine-grained policies centrally, managed by the application owner (not IT security), and enforced at the application during logon through review of the UMA2 policy.

CYBORG Future of ID

Day/Session: Wednesday 2H
Convener: Sari Stenfors
Notes-taker(s): Steve Fulling

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

Two parts to this session: approximately 30 min. each:

1. Dream up the future we want for IDs for CyBorgs. What would work very well??
    a. Time limited and revocable identities.
    b. Natural identities based on how we as biological beings behave.
    c. If we embody the digital world, maybe the digital world takes us over as we pass out.
    d. Think of tribes, groups perhaps have identities, maybe like the "Borg"
    e. If we have AI agents, they act on our behalf.
    f. How do we use the Internet now? As a Cyborg we put on different personas. Multiple identities.
    g. Control each identity. Augmented reality.
    h. Ability to differentiate between a Cyborg and no-Cyborg
    i. Disappointed in how the human animal has been so overwhelmed on how to extend ourselves.
    j. Behave in the digital landscape the way we behave in the physical world.
    k. Many problems with biometrics. How about cybiometrics?
    l. Bridge interface between physical and digital world. Cybiowallet?
    m. Identities are identifiers and attributes. We are talking about identifiers.
    n. Biometrics are identifiers.
    o. Do identities begin and end? Identities continue but the identifiers do not keep living?
    p. Who / what are the components? What does it mean to be anonymous?
    q. What does it mean to be autonomous?
    r. What if you don't want to do the things society requires of you??
    s. How do we bring forth the same characteristics of our current environment?
    t. How do we have a verifiable record of what did an did not happen.
    u. How do you combine cyborg and real learning.
    v. Semi-autonomous agents? Are we online or are our agents online?
    w. We have group identity. Tribe identity.
    x. Identity is a social construct. We have identifiers and attributes.
    y. Identity can be associated with objects. Identify by objects.
    z. Manufacturing your identity. Who are you really?
    aa. Hivemind.

2. **How we are going to get there?**
    a. We are at a given place in time. How do we get to this cyborg future?
    b. What are the issues today?
    c. How do imagine our future?
    d. The figure is entirely different from what we could imagine today?
    e. How do we avoid the pain of operating by default?

f. What do we do to prep?
g. Legalize hallucinogenic?
h. We need imagination?
i. Rethink laws. What are rules?
j. Is it in our nature to be proactive?
k. We did create work unions, etc.
l. Nature is not civil nor is it fair.
m. There is a natural contention for resources.
n. We are frying our minds. Overclocking.
o. We are problem solvers.
p. For the first time in history do we have the option to change our future?
q. We have the ability to build in balance??
r. Do we have better tools today that we've not had previously??
s. Humans are noisy and predictable. We are simple.
t. We have coalitions of humans who want to do the right thing.
u. SSI / DID?

What is the most important thing we can do today??

a. Preservation of our identities.
b. Centralized powers and of force don't work well.
c. Decentralized governance, augmented with technology.
d. Grateful that people are thinking about his and working on this.
e. Preserving ID while designing privacy
f. Balancing with consent. Having control over your ID.
g. Read your history.
h. Read Accelerando
i. Use moral as compass.
j. Manage and remember our heart.

OAuth for Single-Page Apps (javascript apps): Best Practices Recommendations

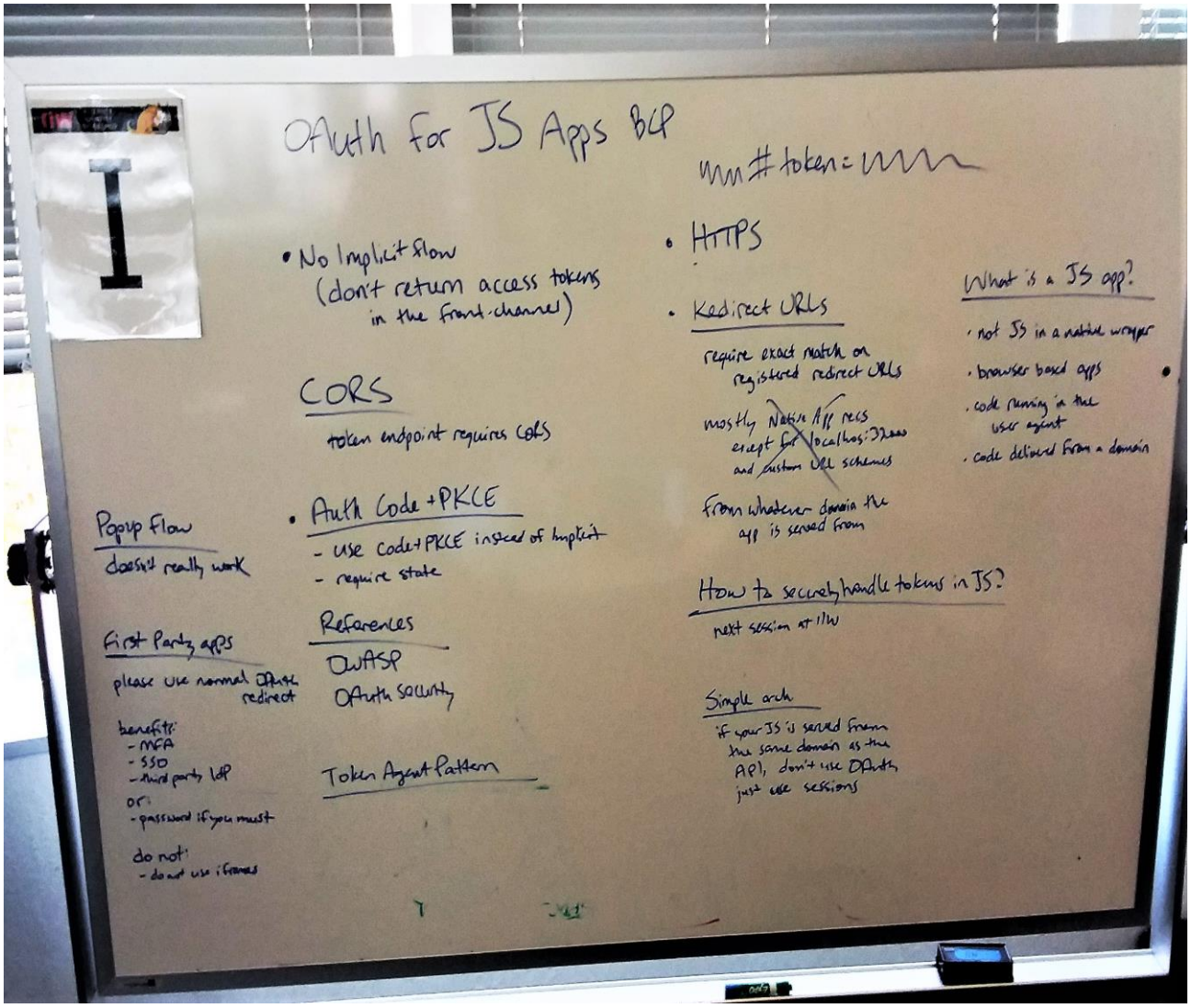
Day/Session: Wednesday 2I
Convener: Aaron Parecki
Notes-taker(s): Tom Brown

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

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

- Problems with Oauth implicit flow. We can do better
- BCP – best practices (get a number filled by a series of RFCs that can change over time. As close as IETF gets to a living document
- Not trying to break spec
- Nothing necessarily wrong with fragment but returning access token in front channel is susceptible to interception and replay attacks
- also, we have browser history api now so don't need fragment
- with JS, not client authentication
- Justin R.: no way to confirm access token is the one I requested
- AS has no assurance that code was sent to the right place
- Authorization code by itself is better than implicit. If you add PKCE, then you solve stolen code
- Justin R.: Many implementation don't do CORS because they haven't thought of it
- Torsten: Nonce not defined in OAuth 2 spec and went with PKCE
- Registering urls, not allowing wildcards needed for JS since no client authentication
- What is a JS app? (electron is a native app written in JS):
    - App running in a browser
    - Not JS in native wrapper
    - Code running in user agent delivered from a domain
- "token agent pattern" noted but seems out of scope
- In case of first party app, it sometimes doesn't make sense for user to leave the page (maybe there are no 3rd party apps)

- Anabelle: Popups are a pain
- If user doesn't leave page, there are losses: no single sign-on, you can't do FIDO, no 3rd party IdPs



Digital Link: Defining Digital Identity for 100's Millions of Every Day Things

Day/Session: Wednesday 2J
Convener: Paul Dietrich
Notes-taker(s): Gena Morgan

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

As businesses begin to deploy solutions leveraging the new standard, called GS1 Digital Link, brands and retailers can Web-enable barcodes and provide consumers with a direct link to brand-authorized product information and content including product images, expiration dates, nutritional data, warranty registration, troubleshooting instructions, discount offers, and more. Additionally, the GS1 Mobile Ready Hero Images guideline standardizes the combination of product images and information viewed on mobile devices.

Developed by an international working group of retailers, brand owners, solution providers, and technology experts, GS1 Digital Link is a digitally-enabled, globally-unique identifier resembling a Uniform Resource Locator (URL) or Web address. It leverages the ubiquity of the Web and data carriers, including barcodes or QR codes, to enable solutions that help consumers connect directly to brand-authorized product information instantly via product packaging.

Informative session on the above from the largest non profit standards organization for supply chains.

The group discussed the need for this standard for apps to be developed on authoritative data. We solicited input about resolvers as GS1 moves to phase 2 in standards development process - which will focus on replacer services.

Discussed the relationship between GS1 identifiers and DIDs and how they may work together for future "IoT" use cases.

Link to GS1 Web URI Structure Standard: https://www.gs1.org/standards/Digital-Link/1-0

Best Practices: Managing Access Tokens or How to Avoid Being the Next Victim after Facebook

Day/Session: Wednesday 3A
Convener: Bjorn Hjelm
Notes-taker(s): Bjorn Hjelm

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

Background slides: https://www.slideshare.net/BjornHjelm/iiw-27-wednesday-session-3

Summary

- Discussed the background and possible incorrect understanding of OAuth 2.0 in the implementation by Facebook.
- Agreement that there was a need for a common glossary for the terms in OAuth 2.0 to help developers. The interpretation of the terms or what the terms are referring to may also result in different interpretations (authorize v. entitlement, privileges as authority v. permission, etc.). One proposal was to ask IDPro (https://idpro.org/) to develop this glossary.
- Part of the issue was also business process related (for example, for Access Tokens revocation).
- Based on discussion of do's and don'ts when implementing OAuth 2.0, there was a proposal for creating a best practices implementation guide that could possible reside on OAuth.net.
- The general guideline was to be very restrictive with the privileges associated with an Access Token (per draft-ietf-oauth-security-topics) and to manage Access Tokens through the Refresh Token (that is only intended for use with an Authorization Servers).

Digital Life: State 1 – Survelliance, Captalism + Re-Engineering Humanity

Day/Session: Wednesday 3B
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:

- A high level thing. I do a thing in NYC called rectangle bingo. Everybody else in subway car is on their rectangle. Take a pano of the whole subway car.

- The point is these things changed us. We are not the same animals we were before. That's a very human thing.

- A whole lot of literature coming out now.

- Re-Engineering Humanity, Brett Frischmann and Evan Selinger – ends on note of optimism, references Customer Commons

- The Age of Surveillance Capitalism – The Fight for a Human Future at the New Frontier of Power – Shoshana Zuboff. Currently in German. English version out in January 2019.

- Lab Rats – How Silicon Valley Made Work Miserable for the Rest of Us – Dan Lyons – best title of the three

- Shoshana, Zuboff's Laws. 1. Whatever can be digitized. 2. Whatever can be informated. 3. Every digital application that can be used for surveillance and control will be used for surveillance and control.

- Marshall McLuhan, Understanding Media, The Extensions of Man. He meant technology when he said media. Humans are unique among animals in that we extend ourselves through our technology. We invented privacy tech (clothes) 50K years ago, haven't done it online yet. We shape our tools and they shape us. Every new medium works us over completely.

- He & his son Eric (who just died this spring), came up with the laws of media. Every new medium/tech does four things. Enhance, retrieve, obsolesce, reverse. Every new tech has negative outcomes especially as they get to ubiquity. It reversed into complete weird isolation. A way of understanding what media did to us.

- What happened to blogging. No publication would hire me. I wasn't in the business as a writer of hawking whatever company was buying ads, or vendor sports. By 2003, I had up to 50K readers per day. In 2006, Twitter & FB came along, my readers went down to dozens a day. Now 24K followers on Twitter. But a parking space makes that many impressions.

- What did social media do. Obsolesced all of journalism, retrieves gossip in a gigantic way. Enhances conviviality. Reverses tribalism. Everybody can now be a journalist.

- Blue Feed, Red Feed. Done by the Wall Street Journal. Take any topic, they have a fake character on FB that starts out slightly liberal or conservative, these are the news feeds they get. Not on the same planet.

- Go back to a stone tool. It had a lot to do with the human diaspora.

- The four causes of a table (from Aristotle).
  1. Efficient (a carpenter made it)
  2. Material (it's made of wood)
  3. Final (we need a surface to work and eat on)
  4. Formal (its form is a table)

- The form of a table is its own cause. What as a formal cause did print, speech, TV do. Each of those has a kind of major effect we're not especially aware of. McLuhan saw computers & satellite communications coming. About TV he said it's largely about fantasy and storytelling. Even journalism. The format of journalism is the story. An assignment editor will say what's the story. Stories aren't necessarily what's happening in the world. The formal cause of the bombs is probably digital life. Find out how to make it online. The Center for Digital Life who knows more about McLuhan, their claim is what digital life is about is memory. We use it to remember things. We rely on this to know stuff. One of my favorite moments, wrote about in my book The Intention Economy, Jeffrey asked him to look stuff up even when driving. I think we're living in world where we're remembering things in a whole different way we did before. My mind is not made up about this.

- TV antenna with birds on it. Over the air TV is a pro forma thing. Nobody is looking at that much anymore. More people watching YouTube than are watching cable TV at this point. Netflix has more watching than all of cable TV. McLuhan says the media gets obsolesced not the content. Radio obsolesced by podcasting.

- The collateral damage of adtech is massive. Tracking-based advertising. Wants eyeballs. More content to see more eyeballs, that's what it funds. GDPR is meant to obsolesce adtech, as is AB375 in California. But they already have negative effects.

- GDPR, I think it enhances consciousness about privacy, reverses into all these cookie notices. Obsolences little adtech, enhances big adtech.

- Not sure we will ever solve this. Joyce has a wonderful metaphor. Digital, the internet has no gravity. It's not a place. Not a place. Also no distance there. Not compatible with privacy. So you throw memory into that. A weird new mix in this non-space we created to occupy. Even the history of what we did here, SAML, federation, now we're at self-sovereign. We are the human entities present with each other, how do we control or assert the polyhedron of identities. Everyone who issues me an identity calls me David. Others call me Doc. How do manage all that? That's what SSI is all about. Doing that in a way that brings together identity-providing entities is the primary challenge. What are the outcomes of that? It's really early.

- How many people block ads at this point. PageFair's 2017 Adblock report: at least 11% of the world's population is now blocking ads on at least 615 million devices. GlobalWebIndex: 37% of all

mobile users, worldwide, were blocking ads by January of 2016, and another 42% would like to. With more than 4.77 billion mobile phone users in the world by 2017 (GlobalWebIndex) at least 1.7 billion people were blocking ads already: a sum exceeding the population of the Western Hemisphere. This doesn't fit the story format anymore.

- Google, FB, sell their consumers to advertisers. Amazon getting into advertising could be a problem. Prime is crack.

- Joyce: The prediction racket. What Surveillance Capitalism is really about, if you want to buy real estate, always buy in the past. That's what all this SC is doing, honing the opportunity to predict our futures. Critical to stop these aspects of it. Now these big companies can predict the future. We want to determine our own future. You'll feel like your agency is feeling I want this. We did a panel in New York last week on advertising. Doc was billed as a heretic. We used to worry about totalitarian governments. Now we worry about totalitarian marketing.

- Q: My quote when I do keynotes is Orwell was an optimist. The big thing for me, in 2010, we switched from a causation-based society to a correlation-based society, by inference. I don't think members of the society understand yet. AIs sit next to judges predicting the repeat offense possibilities of an offender.

- Q: There's a surveillance society.

- Q: Social credit scoring.

- Q: Chicago data science research center, bail risk technology in courtrooms. If you measure AI against a Cook County judge, a monkey could do better. To promote idea AI is better.

- Q: MS found we can turn AIs into rating Nazis in 48 hours.

- Q: Kathy O'Neill's book, Weapons of Math Destruction.

- Doc: Thing in Oregon with high-level business analytics people, how to lie with statistics.

- Q: Referencing books, The Known Citizen, it is early days, point repeated in book. Tech can do some stuff.

- Q: We all need to become polymaths, look through tech, econ, regulatory, cultural/moral, political. Often we default to the tech piece.

- Q: How to leverage the "big company" concern?

- Doc: Won't help to break them up. Tim's idea came up once on Monday and was dismissed on technical grounds. Big PR. I love Tim but stay in the clouds.

- Joyce: You can't repeat the big bang.

- Doc: He simplified something.

- Mike: We understand what's going on, but most people have no clue. Recruiting people to the cushion is the tricky bit. How do we make all the heartbeats realize all this is possible, there are massive data profiles, they need to pay attention. D&D, remember if you had a familiar, that was so cool. Why don't we start a company that sells digital familiars?

- Doc: Talk to Joyce. This whole memory thing.

- Mike: Auditing, checking my digital profile.

- Q: If we read all the privacy policies, would take 75 days and cost the U.S. economy $781 billion.

- Q: They're not going to break up Palantir.

- Sal: If signals out there are crap, it's still crap for the AI too.

- Joyce: I had this dream 5 years ago, if I had a thing that could crawl my own email, surface for me, I want to be able to dice and slice my own information so it can give me intelligence. The business plus on that is so much business to create a thing to work on my stuff.

- Q: I was talking about my digital profile outside my domain.

- Doc: Both of them are memory functions. Educating is too hard. The history of tech is not the history of finding a need & filling it. It's invention is the mother of necessity.

- Jeff: I hope education isn't a lost cause.

- Q: It's low-return investment.

- Jeff: We teach people if you walk into the street without looking you won't last long. The word free in people's heads is no dollars or cents, but there is a cost. Don't sign up for every thing. Free is part of human nature. Top 10 flashlight apps, all were malware. So much noise in your life, you won't be able to hear yourself scream.

- Kai: Let's put SSI in the middle and imagine what goes wrong. Potential to reduce the noise. Not to provide high quality data to the wrong actors.

- Doc: Idea is to enhance independence. Be a fully respected individual. Obsolesces every large identity provider. Reverses to utter chaos in the marketplace. I don't know. Clay Shirky said every good technology has bad uses. A sure sign of a good tech is you can imagine bad uses for it. 99% of email is spam but we can't live without it.

- Q: How can you decimate yourself on the digital landscape. If SSI gets coopted, think of the revolution that could occur. Can you prevent people destroying the value in their SSI?

- Q: Shortly after The Intention Economy came out, I came to Doc, if Google split into blue and green teams, one half did intent casting. Other, if we have enough information about you, we'll figure out what you want before you even know it. We need things like intent casting to drive out this stuff.

- Doc: If I had to reissue that book now, I'd change the names of the companies, most of which are now dead. Customer Commons helps us set the terms.

- Q: It will start out with privacy being a luxury good.

- Q: Good Wired interview last month, Tristan Harris and Yuvall Harrari who runs Humane Tech. Touched on this idea of a personal AI sidekick to help you make good decisions. Predict your own future, probabilities, counteract negative algorithms such as the ones that make you watch YouTube longer

Identity in the Academy

Day/Session: Wednesday 3C
Convener: Phil Windley
Notes-taker(s): (1) Nick Roy, (2) Matthew Hailstone

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

(1) Notes Submitted by Nick Roy:

One thing we could talk about is some of the plans for using verifiable credentials inside/outside BYU

BYU trying to create a system-wide profile - a web app, CAS at different levels in the system
System agent, BYU agent are agents in the ledger in the SSI system

BYU issue transcript to the ledger, student gives consent to share the transcript with the other schools in the system

Hard: How do we bootstrap a student with a credential?
Navigate to BYU webapp, go to CAS, redirects back to the browser, goes back to the webapp, webapp calls CAS to get attributes through SAML. Those attributes provide who the student is in the form of session data.

Can ask the student for consent to participate in the student profile, if they say yes, redirect them over to the profile web app. The CAS instances are federated, now can communicate the student information to the system. Can link credentials and ask the student if they want to share information with the system profile app. Then go to the system agent to start a process to create a wallet. The system agent can talk to the BYU agent and establish a pairwise DID relationship that is unique. Issue a credential to the student in the system profile app. Can assert info to the student, issue verifiable credential. Then BYU can issue things into the identity using a cryptographic proof.

What do the SAML attributes look like? In the legacy system you have a credential table.
In the credential table, you can do crosswalks to other identities/credentials.

<I talked about research identity here>

SAML attributes would say here is how you can contact the BYU agent

Another SAML attribute would have that DID that comes over to express the identity

Legacy authN system on top of SSI DID

If Microsoft or some other system wants to participate, we don't want them to have to stand up CAS.

Don't know who the person is at a system level until they authenticate at their institution.
Early prototype

I talked about proxies, ORCID and attributes in SAML federation. Could use a person's digital wallet to bootstrap their scholarly identity, research identity, identity in the proxy, etc. Allow them to relink their account using their digital wallet.

Creating a fine-grained taxonomy of competencies to allow you to map course equivalency for things like prerequesites. Use a zero-knowledge proof to test if someone has gained the needed competency.

Working on how to create the schemas in a rich format. Until then, they can bootstrap this within the university system using the entire blob of shared person info.

Working on an edu API with Michael Berman from IMS Global.

University can write a public DID and claim definition to issue credentials for, say, the alumni part of the lifecycle.

Real benefit is not authentication, it's carrying information about the person - badging, etc.

Going to a wallet-based system, you don't have to make tons of API calls, and you get loose coupling back.

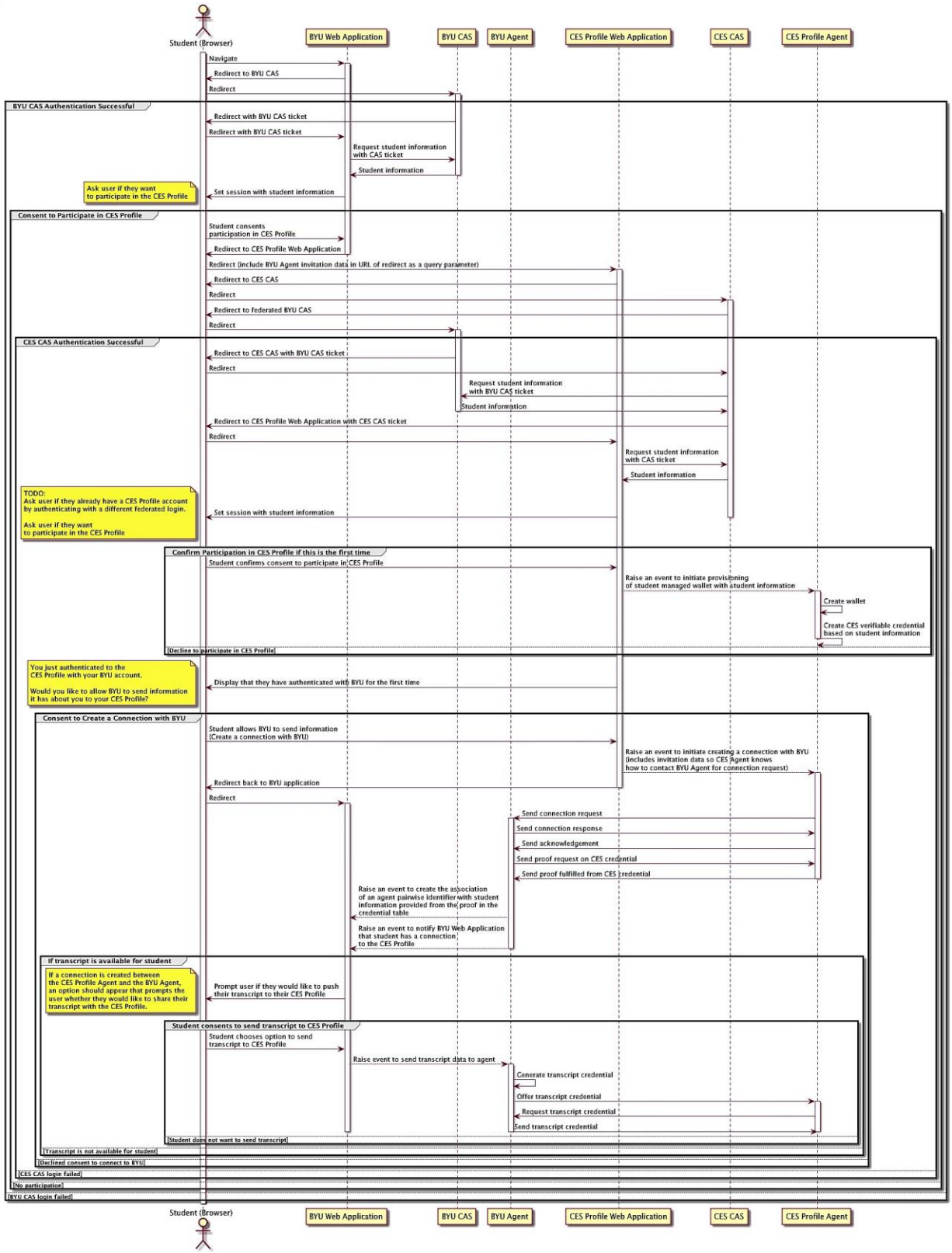
BYU presented at consensus NY using the CLR specification to present a digital diploma, using a mobile app.

Because Microsoft owns LinkedIn, they wanted someone to be able to go to LinkedIn to prove they have a degree.

Since then, they have created that link, so you can now do that in LinkedIn.

CONTINUE TO NEXT PAGE….

(2) Graphic of the sequence diagram discussed, submitted by Matthew Hailstone:



Continuous Access (Long-Lived Session Update Sync Across Clients)

Day/Session: Wed 3D
Convener: Atul Tulshbagwale
Notes-taker(s): Romain Lenglet

Tags for the session - technology discussed/ideas considered:
publish/subscribe, VPN, OCSP

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

- Long-lived sessions are currently not handled well
  - User, device, or app properties / security posture may change within a session
  - Authn-based access control decisions need re-evaluation within a session
  - Back-channel is not always possible for logout
- Example properties / security postures
  - User/device location
  - User/device status, e.g. employee termination
- Distinct entities
  - AS: Authority Service
  - RP: Relying Party, e.g. an enterprise SaaS app such as Dropbox.com
  - Device / App
- Initial protocol proposal
  - Authority Service streams context updates to Relying Party
  - Relying Party sends remediation response to Device based on updates
- E.g. of context information for a session
  - User location
  - Policy applied to the user/client
- The main question is: where is the policy evaluated?
- This looks like the old-fashioned model of having a centralized session database accessed directly by web apps
  - I.e. the Authority Service is streaming the information used by the Relying Party to make policy decisions
  - Instead of streaming the policy decisions themselves
- Atul clarified that the policy evaluation will typically not be done in the web app itself, but in a proxy in front of it
  - The proxy receives context updates from AS and evaluates policy changes
- One advantage is scale
  - The computation of remediation triggers is distributed to every proxy
  - This is a publish/subscribe architecture, which can be heavily cached on the RP side
- The contents of the context / policy updates, and maybe even the protocol, is specific to every specific Relying Party
  - The stream of updates from AS to RP is a streaming query which queries for the only attributes the RP needs for that particular session
- it seems we don't need a specific remediation process between RP and Device
  - It would be sufficient for the RP to decide to reset the close the session and force the Device to re-establish a session through the IdP, etc.

- The new session will have updated access rights
- This applies to non-web-app use cases as well
  - E.g. when the RP is a VPN server
  - The AS streams policy updates to the VPN server over OCSP
- We should pursue a 2-track approach, and see how they can converge
  - SaaS app use case
    - We can standardize the protocol and context model
    - But we need to find the incentive for SaaS apps to adopt it
  - Non-SaaS use cases, e.g. VPN or WiFi router
    - It is not realistic to expect vendors to adopt a new standard
    - We would need to use existing protocols, like OCSP

Decentralized Ecosystem Governance – with Blockchain

Day/Session: Wednesday 3G
Convener: Titus Capilnean
Notes-taker(s): Heather Vescent

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

Link to my google docs notes: https://docs.google.com/document/d/1CUU-YnGNe-5FCHeFApCeo-oZiDQqNIZ0jrdHj2bBkGM/edit?usp=sharing

Whitepapers: https://www.identity.com/
https://tokensale.civic.com/CivicTokenSaleWhitePaper.pdf
https://www.civic.com/wp-content/uploads/2018/05/Token-Behavior-Model-May-16-2018.pdf

Github: https://github.com/identity-com/

Q: Is Identity.com for profit or is it non profit?
A: TBD it is now part of Civic, but exploring opportunities to spin it off.

Users don't pay, requestors pay per use.
What's the situation where you don't believe the validator?

Question: How far are you into the working implementation?

Built the first layer of identity - abstraction layer - on github. We are working on the toolkits and governance. These things are in a whitepaper. The governance is just in the whitepaper. All on identity.com.

Validators have to have a stake.

M.E.S.H. (Managed Ecosytem Superdistrubted Hashes)

Day/Session: Wednesday 3H
Convener: Alexandra Mikityuk, John Calian, Dirk Thatmann, Alexander Manecke
Notes-taker(s): John Calian

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

Hosted by Deutsche Telekom Labs:

- Alexandra Mikityuk
- John Calian
- Dirk Thatmann
- Alexander Manecke

Six (6) attendees

Demo'd the MESH system, known as 'Hashståx'

This system allows any software developer to instantly start using the features of numerous blockchain/DLT networks, including payments, storage, identity and smart contracts

Of the features of blockchain that are important for Telco, its Identity that is most important. Billions of devices (IoT) will be joining networks in the coming years, and machine identity is the critical piece for network security

Additionally, human identity is a path all enterprises concern themselves with

Q/A
Are the APIs network specific?
No, they are unified for all networks, like the storage API can call IOTA

Is it open source?
Will be

When open source?
Dont know. Maybe end of 2019?

Basically this system creates bundles of pre made nodes for blockchains?
yes

Why have an abstraction layer like this? Do you really see system needing more than one blockchain?
Yes, because system design might require both permissioned and permissionless access

What about key storage?
We work on it

How do we solve the ecosystem issues? DID protocol? Wallet Protocol?
All of these are needed to be standardized
Separate session needed

Q&A with Sovrin Foundation Executive Director

Day/Session: Wednesday 3I
Convener: Heather Dahl
Notes-taker(s): Heather Dahl

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

Overview of the Sovrin Foundation:

- Established September 29, 2016
- Technology: Sovrin Network, Hyperledger Indy (supplier of code)
- 501(c)(4): In order for an identity to truly be decentralized, it must remain forever under the identity owner's control & never be subject to whims, weaknesses, or future prospects of any centralized entity
- Provisional Network Launched: 2016
- 50+ Stewards
- 19 Sovrin Community Boards, Councils, Working Groups
    - Dr. Phil Windley, Chair, Board of Trustees
    - CEO: Heather Dahl
    - CTO: Nathan George
    - CFO: Roy Avondett
    - CMO: Helen Garneau
    - Steward Operations: Steve Fulling
    - Employees: 20
    - Based: Provo, UT

What are the Foundation's goals?

- One Year:
    - Financial Independence
    - Technical & Ecosystem Independence & Diversity
    - Create Supportive Sovrin Communities
    - Build Sustainable Operations to Support Network's Growth

What has the Foundation been up to?

<u>2018 Achievements:</u>
Overall Foundation

- Collaboration agreement between Foundation & Evernym
- Developing Foundation playbook for strategy, goals, KPI's, metrics & transparency
- New Provo office
- 5-year budget projections
- Hired staff
- Established economic advisory council & task force
- Best practices HR training for full & part time staff
- I4A mission, strategy, & team

Stewards

- 50+ Stewards
- Restructured SQC
- All Stewards Calls
- Steward onsite event
- Expanded Steward relationship team
- Updated Steward agreement
- TFv2
- Dedicated Foundation counsel
- Steward portal

Marketing

- Visual branding
- Community and external newsletters
- Sovrin case studies
- Sovrin video series
- New website (November)
- Monthly Steward marketing call-in (December)
- Brand book & Sovrin usage guidelines
- Sovrin events & sponsorship support
- PR & social media support with new Steward approvals

CTO

- Technology acceptance process 1.6 network
- Expanded team to support technical requests
- Increased Sovrin community agent repository
- Supporting open source development
- Sovrin code testing

What can I anticipate from the Foundation?

Looking Forward

- October 2018: Live Network
- November 2018: New Website & White Paper
- December 2018: Trust Framework v.2 & Steward Agreement Signed
- TBD 2019: Launch Sovrin Alliance
- February 2019: Blockchain Africa Sovrin Featured Speakers
- April 2019: Sovrin Summit Conference
- May 2019: Inaugural Sovrin Alliance Worshop Series
- July 2019: Sovrin Developer Bootcamp
- August 2019: My Data
- September 2019: Hyperledger Member Summit
- October 2019: Internet Identity Workshop

Forget About Identity & Authentication (Discuss New Approaches)

Day/Session: Wednesday 3J
Convener: Andrew Hughes & Robert Mitwiki
Notes-taker(s): Alec Laws

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

IDEA: identity is pointless in technical sense -> it doesn't exist

Identity does exist in the world, but we're not talking about identity
- talking about: authentication, credentials ...
  - identity is label for collection of all of these services

in real world, no one know what 'identity' mean (as we discuss)

two things we actually do
1. authorization -> what a subject can do
2. identify the identity -> enough to look up authorization

method to identity someone, doesn't rely on any specific technique/technology
- proof of presence

Is there a way to track someone based on their patterns within an environment?
- use technology to measure

brings up identity vs identification

identity -> typically based on credential presentation
identification -> don't actually need the credentials

to escape tracking in digital world
ex mobile device tracking patterns
- patterns stay the same even if you change devices

identification without attributes, based on patterns

crowd Q. is this surveillance-based identity
-> coopt targeted marketing as identification system
- observables

creating an identity through measurement

assumption that someone documents identity, put in a registry -> everything flows from there
another entity accepts the issued 'identity'

assume there is no such 'issued credential'
- we identify without paper/plastic credentials -> how to translate into a technical system

observed vs assigned attributes

observation to build attributes vs presentation of assigned attributes

cQ. local checking vs remote checking? different use case?
- lofty goal -> it's universal
- what is the nature of identification, how can we make this electronic
- is this device fingerprinting? this is identification

verification and proofing techniques, gathering evidence (sometimes from id docs)
- dyn and risk based authz services, and really identification services

idproofing: linking physical identity to a person

there is no common measurement framework to express id proofing and behavioral sensing's are in the same domain
- allows supplementation of identity documents
- companies already do this to assess fraud

can we build this common framework to link behavioral and attribute-based identity?

Why is this the right direction? (shift from identity to identification)
- we have many different credentials -> can be lost/destroyed
- people would lose id docs

What is a good threat model for this? How can it be gamed? ie spoofing of location. Once people have motivation to attack... balance between effort and benefit

authentication is tied to 'time', in reality things are strongly ordered -> very hard to tamper

challenge w idproofing -> standard writing is b/w way. either identified or not. not really how it is. Is this continuous?
move from high -> low uncertainty

cQ. what we are calling identification would be called a risk score. identification to system vs many systems
supplement identity vs identification

cQ. for this to happen and connect risk scores, we need confidence in identity to relate to the behavior.
- start with a static proof of id and supplement with other techniques

cQ. how are scores made, and how can they be combined?
- standardization? error bars? number of sources, quality of data

what is the definition of a working system?

never a boolean, always a degree of confidence or assurance. probability based
risk model + threat analysis + other source to mitigate/change risk and make it measurable
acr shows what the 'person' did to authenticate

what can we standardize about these processes?
Take existing stuff and make into a patterns
key thing is time/timeline -> assume time always moves forward

registrar says 'I must identify you to issue a credential'
-> you show previous evidence with correlated data
-> shared events in the past, ie reregistration of license. vehicle permits
-> artifact memorializes the interaction

ie 'when you get murdered, make sure you sync your Fitbit' Fitbit tracks liveness, timelines didn't match and threw out an alibi

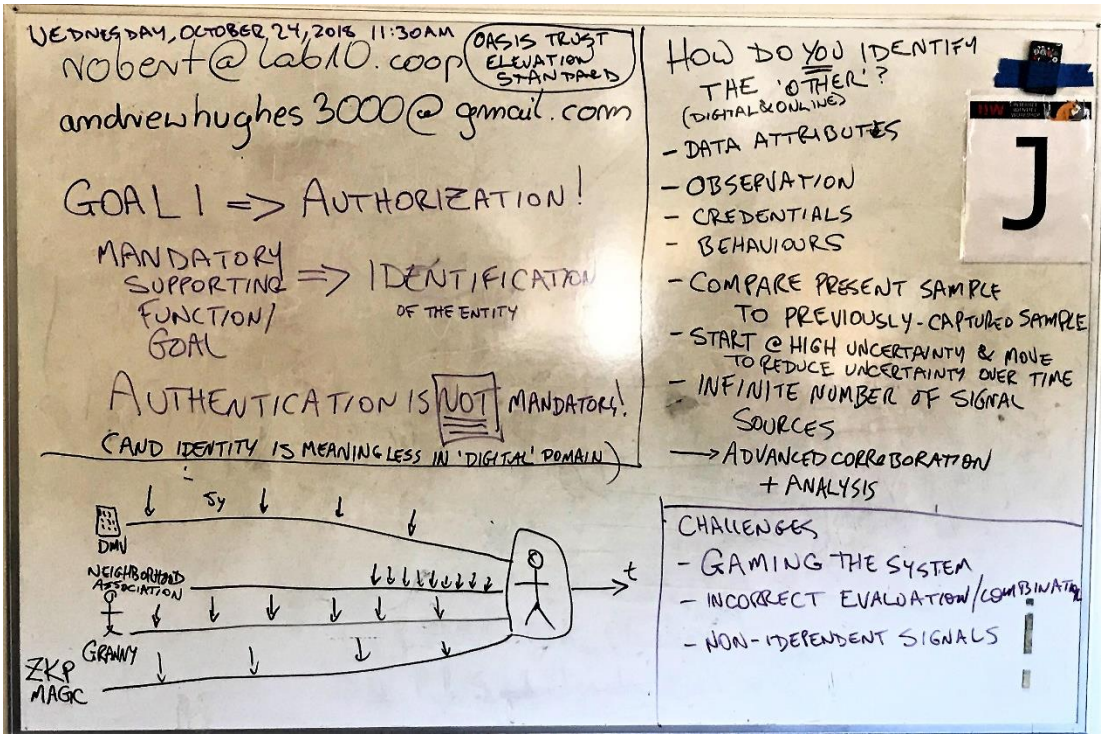
can we collapse the timelines between interactions with different entities?

score and assertion measurements mechanizes so that the can be compared

how to prove you climbed a mountain? take a photo? gps? you leave an artifact at the top, the next person can verify that it's there.
-> impractically of faking
-> the artifacts that you drop on the timeline show provenance of your 'identity'

website. I encounter website for first time, no access controls (anon access). they have identified you at protocol layer (at least). They don't care about authenticity of claim (ip addr), they never authenticate but they identify.
bank site. attempt to get $1. they both identify (username) and authenticate (with a proof)

how does this sync with privacy? access to data you need to perform this process
- private authentication assertions (zero knowledge proof) to address correlation
- ML model uncertainty vs proofs based on mathematics
- (non)independent data points -> especially when combining models
- secret algorithms 'black boxes'



OIDC DID-Auth Profile

Day/Session: Wednesday 3K
Convener: Oliver Terbu
Notes-taker(s): Oliver Terbu

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

The goal was to find a way to use OIDC request and response messages to support SSI wallets without having the need to have a central OpenID Connect Provider. Another approach would be to get redirected to your OP and do the authentication step using a SSI Wallet. In this case, you would have to rely on a central OP which in this case is not desired.

Some takeaways:
- DID Auth was more understood as being a concept rather than being one particular protocol.
- Defining a OIDC DID Auth profile was considered to be a good idea.

OIDC profile:
- This will be used to convey the DID Auth request and response messages using OIDC
- Using OIDC makes it possible to leverage existing libraries and supporting OIDC clients by introducing minor changes.
- How to solve discovery? —> Self-issued OP
- Distributed claims could help to support Verifiable Credentials from different Issuers
- Using the nonce as a challenge in DID Auth was considered as a good idea
- Using a JWT header from the id token to kick-off DID Resolution -> jwks URL could be a DID
- iss field will be encode the iss inside the id token

Furthermore, an IETF profile for JWT with native support for DID was also considered. Allow iss, aud, and sub to be a DID.

Overall, the session was very productive and I'm glad so many people participated in the session.

Self Sovereign Technology Demo and Ask Me Anything (AMA)

Day/Session: Wednesday 4A
Convener: Doc Searls
Notes-taker(s): Doc Searls & Adrian Gropper

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

Recapped the demo.

- 3 components (3 GitHub repos)
- UMA AS (authorization servers)
- NOSH (new open source health)
- Trustee directory, a record locator and encounter time service.
- First two are self-sovereign to an individual and can attach themselves to one or more of the directories. The directories are self-sovereign in that each sets their bundle of policies such as how patients are discovered or monetized. There's no central platform.
- Plus a uport component, doing digital signatures and authorization. Staying as close as possible to the DID spec. Open to Sovrin when it comes along as well and other DID / VC methods when they become available.
- Uport is a credential wallet and in that role it accepts credentials as well. It is also a method by which the wallet and the DID links to Ethereum for accountability of the credentialed users.
- The HIE of One Directory is one specific example. Provides a way for a patient to be discovered. View on screen is of patients, each with their HIE of One Trustee.
- Under trustee Authorization Server for Adrian, this is the doctor logging in to the patient's server. He or she scans a QR code with uPort Moble App. The doctor as an SS entity logs in to the patient's HIE. Dr. sees the patient's EHR (electronic health record). If the patient doesn't have his own domain a directory can provide a subdomain. Directories can also act as proxies with limited access to the patient's personal data.
- From the patient's view, it's the same NOSH EHR screen but with a consent table button. The consent table is the embodiment of UMA, Oauth and OpenID Connect., with many choices provided by the different standards.
- There are four sections, or consent categories: Resource Sever, Invited User, Certifier and Directory, with a legend at the bottom.
- The patient can control permissions: all, read only, Allergies and Meds, Care Team List, and Custom Policy (under invited users).

- Under certifier, it's Read Only, Clinician, Family and Custom Role.
- This is all about delegation and capabilities to avoid the temptation to share identities.
- This is not a patient engagement thing. It's a view of the plumbing behind what the patient engages, which is the Navigator or some other trusted intermediary.
- What Adrian is looking for...
- How do we drive UMA rather than Oauth? UMA allows delegation so you're not stuck with sharing logins and passwords, ways of not scaling. But we are having trouble, for political and business reasons, getting institutions to come along.
- Financing. It's very hard to say something is self-sovereign if there's a walled garden. Such as Apple has. Who will pay for it? There will be a thing for the home to back up the server In the cloud. How do you finance and scale something like that? Can't sell equity. Might look like a utility token.
- Hard to sell insurance companies. They live and die by proprietary data.
- Could be a coop.
- This is most appealing to patients spending a lot of money out of pocket. No shortage of those.
- If you can solve the problems of reputation, matchmaking and support, you don't need the Uber or AirBnB of this, or something like it.
- The costs of systems controlled by large entities are immense.
- Question: "Sounds like Henrietta Lacks 2.0."
- "If you're sick with cancer and costing the system, it's not unreasonable to assume that it will cost $0.5 million to get best available care." "The way secrecy works in the business of medicine has to change."
- "What happens if the homeless guy loses his QR code?" "That's why you have the directory. The Navigator will have that."
- This is about having a bulletproof way to do delegation and recovery...
- SSI for the professionals will offer many ways to disintermediate their hospitals as “platforms”.
- Surveillance capitalism, the current system, takes no risk.
- There may have to be an UMA 3 to do multi-party delegation - in response to what AK wants in chained delegation / revocation.

- Locations for repos: hieofone.org.
- M: the UK situation is similar. Both have many Epics hired by the NHS.
- The issue is behavioral change. But the value of data is understood, and people want to hold it more closely.
- The $500k cost per individual situation is not unique to the U.S.
- India has no health record infrastructure. They have Aadhaar, and India Stack. What should we design against that?
- On one call to India: one from hospital interests, one from regional interests (euro model), one from Google, and Adrian saying "all you need to do is regulate the API to avoid centralized governance.
- “Health information exchange of one” was published as part of a draft policy by the Indian Government. But there are multiple ministries to navigate the coming implementation.
- UK *is* moving to open standards and open source. But the political influence of the bigs still stand.
- But regulatory capture persists. And Adrian is alone.
- Hope is simple: time is on our side. the value of aggregated data goes up exponentially while the technology cost of doing this goes down, and will include AI over time. Eventually economics drives this. In other words, this is waiting in the future for the economic case for it to become obvious and inevitable
- Much of this isn't written up for all audiences, because all of the audiences are separate.
- We've had decades of institutional incumbency that we're up against.
- Until the learned intermediaries, the profession of doctors, realize that they don't want to shift the governance of medicine to centralized institutions and corporate vendor AI, and that they need a balance of regulated vendors and licensed intermediaries, then they finally work the way an accountant or a lawyer might act as an agent of the client.
- We need the learned intermediary, the doctor, to be the fiduciary.
- 100% of those who want to make this happen in the first wave are shrinks because they want a direct relationship with the patient and don’t yet use / trust institutional EHRs.

Sovrin Ask Me Anything (Part 2)

Day/Session: Wednesday 4B
Convener: Phil Windley & Jim Fenton
Notes-taker(s): (1) Phil Windley & (2) Jim Fenton

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

(3) Notes from Phil Windley:

We continued to work our way through the white paper with Jim asking questions and Phil answering with the help of others. Jim's questions sparked other questions from participants.

The discussion continued to focus on areas like:

1. The need for decentralized identifier discovery in an adversarial environment

2. The details of Sovrin credential exchange

3. The architecture of Sovrin

(4) Notes from Jim Fenton:
Here's a short summary (includes part 2 from Wednesday).

This session was an open discussion of questions and answers about the Sovrin white paper, available at:
https://sovrin.org/wp-content/uploads/2018/03/Sovrin-Protocol-and-Token-White-Paper.pdf

Questions were seeded by Jim Fenton, who recently read the white paper, and most answers were supplied by Phil Windley. Other questions and clarifications were supplied by others in the session.

The questions included (page references are to the above PDF):

- (page 6 bottom) Given that there is an existing trust relationship, why doesn't the verifier already have the issuer's public key?
- (page 7 bottom) The issue with PKI seems to be with the CAs. Why not just have the issuer sign the assertion with their key?
- (page 9 middle) The link for Validated transactions points to a bitcoin document. Validation is undoubtedly different for Sovrin; what does it consist of?
- (page 9 bottom) Why is immutability of records important?
- (page 9 bottom) What is "self service"? Isn't this done by stewards, not users?
- (page 10 top) "No registration authority": Isn't the blockchain, in effect, a registration authority?
- (page 11 top) Who signs the public key assertion on the Sovrin blockchain? You need to trust that signature, too.
- (page 13, top) Why not use one of these , like DNS?
- (page 13, middle) "never be taken away" Why is this a threat?
- (page 17) How does one get claims for new DIDs? Do you need to give all DIDs to each claim provider?

- (page 22) Comment: quantum computing will cause problems for Sovrin public keys as well.
- (page 23, bottom) Does the past failure of ZKP to catch on stem from lack of infrastructure, or from desire by relying parties to get as much information as possible?
- (page 26, top) Access to Sovrin is not necessarily password-free.
- (page 28, bottom) Compliance costs for businesses are often low: direct financial losses akin to shoplifting for financial institutions, and arguably low penalties for breaches of personal information. As a result, there was little interest in deploying earlier federated technologies. Are the incentives high enough for deployment of a very new technology?

Data Transfer Project: Universal Data Portability for All (Overview, Demo, How To)

Day/Session: Wednesday 4C
Convener: Jessie "Chuy" Chavez
Notes-taker(s): Scott Mace

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

Enabling Universal Data Portability https://datatransferproject.dev/

Google, Facebook, Twitter, Microsoft have contributed.

- What portability looks like today. Ideal portability solution. Data Transfer Project Overview. Data Transfer Project Architecture. DTP & screenshots. What's next

- Mini-version launched 8-10 years ago.

- Download your data. Launched as a one-stop hub. We're already at 80 products, especially with GDPR. Good framework in place to make sure we capture everything. An article after Cambridge Analytica that an Irish blogger wrote, 200,000 retweets. Pointed directly at Takeout.

- Surprises, I didn't know Google had my voice searches. Next wave is to make it more user friendly. We have Privacy Advisor, launched today inside Search.

- Challenges today. Mobile overtook desktop. Now what do you do? iCal good to download, upload elsewhere. Other formats not as easy yet.

- Data also deletable.

- N squared scaling problem.
- What if we had a common set of data models.

- Open to all companies

- Scalable
- Enables innovation
- Reciprocal
- No one company can own it.
- DTP is open source, 1300 commits. Make it super easy. We're adding schema.org model overlays. Also microdata formats coming in. All on Github.
- Focus on customer data.
- People moving from Google+ to Google Groups, Slack channels, a different problem because the data is owned by many.
- Architecture slide. Mail exporter. Mail & photo exporter. Photo exporter. Internal representation of Mail Exchange Format, Photo Exchange Format. OAuth 1 and OAuth 2.
- Mail is well defined. Photo is well defined. Except little motion thing in Google. A fidelity problem, how to represent things that are unique to each product space.
- Exporter: Mail importer, Photo Importer.
- Idea is each of these exists once.
- We call those adapters, generic name. The magic happens in the adapter.
- Apple has nested albums. Apple doesn't have to change its API.
- We provide the plug-ins. Applied what was learned over the years with Takeout.
- Hosting environment:
    - Docker image containing demo frontend and back end userver. Running on local machine.

Steps:

1. Download our demo image from DockerHub
2. Obtain and download keys for the APIs you wish to support
3. Run it!

- First FB contribution: FB photos.
- Instructions are online. You do have to have Docker.
- Demo 2 – Prototype: Data Transfer Project at Google.
- We have Google Dashboard, high-level summary of all the data you have at Google across all the products, i.e. location history is on. Drop down how to download data. Can transfer the data. Slides

showing migration. Transfer to Flickr. OAuth screen to Google, followed by OAuth screen at Flickr. Trying to use OAuth scopes as best they can.

- Take token, issue reads / uploads of files. Can do it now.
- Future plans
- Productionizing existing code (O'Reilly Site Reliability Engineering book)
- Additional partners
- Additional verticals
- Consumer-facing functionality.
- Big announcement was in July.
- Agricultural findata project out of Purdue, really cool project. So farmers can have a unified dashboard from disparate systems
- Strava to Fitbit, Google Fit, Garmin
- What does it look like on the consumer side? How users actually handle the transfer.
- Am I deleting at the same time, close their account? A lot of confusion
- A privacy / UX challenge & tradeoff between those concerns
- Getting involved
- Build adapters!
- Log bugs / requests
- Make it your own
- Local French businesses sharing power / utility data
- Would love to see importers into identity hubs
- The more users empowered to move their data around [the better]
- Displayed Github repository
- Constant flow of commits

- Right now most of the developers are from Microsoft or Facebook
- Cool fact, most of our developers are women
- Web site with our white paper, pages of the stuff government officials and regulators want to see
- Get into everything about minimizing data.
- i.e. if Facebook does social media export, should it drag along your friends and their comments? Posts, not the name of the person who did it? Next-generation concerns. GDPR advises not necessarily to include data from person not doing the transfer
- Not everyone allows the token to be revoked. We only want it for the length of time it takes to transfer your data. Bad actors could keep tokens. Kind of a failure of OAuth.
- Some tokens are actually too broad. We don't want to change profiles.
- Q: Is what you're running in the service the same as what's in the repo?
- Yes. Aside from Google authentication code.
- Q: Will it appear on Google's site?
- We will vet it, but if it's useful, it will appear on the Google site.
- Q: Export of authenticated data?
- We haven't done it yet, but it came up in Mydata a lot. Data could be an asset for insurance reasons. Verifying data is a really important. We were wondering if we could add that as a layer to this. You would also have to insure that each product is verifiable.
- Video, presented in 2017 in Datentag in Berlin, first conference on data portability.
- We have a talk from Ali & Greg. Geoffrey Delcroix. Really interesting stuff on data portability. Microsoft came on board.
- Google My Account, a lot of stuff. Today we launched privacy advisor. Can be annoying if you're looking for driving directions. There are tradeoffs.
- Privacy Advisor is contextual. You'll see it in Search.
- In Takeout we're launching Schedule Takeout.
- We keep hoping standalone viewers will come out.

Blockchain Top Level Domains (TLDs): Identity, Key Management

Day/Session: Wednesday 4D
Convener: Greg Slepak
Notes-taker(s): Heather Vescent

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

Link to Heather's google doc & notes:
https://docs.google.com/document/d/1qNx-MWzoc9PpMrYGH9jNFJnYTkzhKLH6Kw3W1bfzPZw/edit?usp=sharing

What's a TLD - top level domain. e.e.g .com .org

What's not a top level domain: apple.com (just a normal domain)

Security problems: someone eavesdropping on the conversation.
A digital communication problems since the beginning of digital communications.

Certificate Authorities - entities you've never met. Root authorities.
You're trusting the weakest link in this list.

A certificate authority can add someone to the list - called Intermediate authorities.
There are more than 1000-1600 combination of these two groups.

What is the fundamental difference btwn blockchains and this system?

Blockchain - collection of independent entity for consensus - aka voting. VOting on what transactions to include in a chain of blocks.

.bit was the first TLD
Truth is the longest chain.
Consensus based on proof of work.
There are other consensus models.

Trusting a collective vs trusting the weakest link of security certificates (weakest link security).
Trusting a collective is stronger.

Smart objects are not secure because… communication is not secure.
How is software running on IOT / smart objects verified? It's not.
To verify the software you need digital signature & key management.

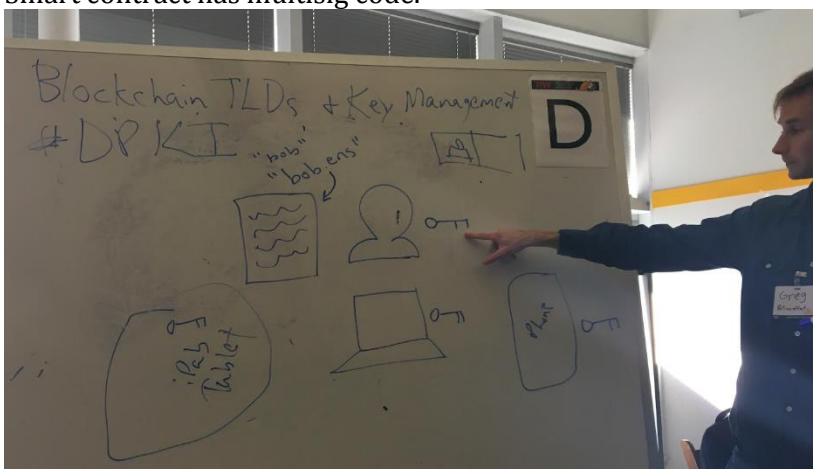
Key management with certificate authority is weak
But key management with blockchain, is more secure.

DPKI - decentralized public key infrastructure
Weboftrust.info
Smart contracts
A piece of computer code/program registered on the blockchain.

Bob Bob.ens (etherium name space)
Key management

Register bob.ens and point the blockchain.
This smartcontract has a public key, managed by bob.
Iphone has a key
Ipad has a key
Laptop has a key

Three devices to sign software.
Smart contract has multisig code.



Removes iphone
Replaces it with a Fairphone / Libram 5
Create a new key

Shamir secret - sharding the key. https://en.wikipedia.org/wiki/Shamir%27s_Secret_Sharing
How are these keys held?
Preference: trusted computing modules…
AES256 - symmetric cipher.

Question: why did namecoin not work?
A: it's not that it didn't work, it works, the project doesn't have much backing and there are competitors that are running much farther. Etherium makes smart contracts much easier.

Consumer IoT: A Perspective Of Retailers, Brands, and Manufacturers

Day/Session: Wednesday 4E
Convener: Paul Dietrich
Notes-taker(s): Gena Morgan

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

Provided an overview of effort including the worlds largest brands and retailers to define business drivers and requirements for enabling a seamless consumer experience.
Enabling richer experiences between brands, retailers and their consumers with their "dumb" products through their smart devices.

Intro to our effort —
Sanjay at MIT on our board
Define consumer internet of things
seamless consumer experience
Commerce is changing
Devices are doing our shopping
What does this mean for our members and our standards

The process -

Key stakeholders from GS1 member companies
Recruit a larger community. Folks came from IOT strategy or from future initiative type programs.
retailers
brands
manufactures
healthcare
solution providers
data carriers
CIoT
frameworks
identity providers

Series of face to face meetings and calls to refine and converge
What business drivers are behind the efffort
What are the requirements for these business drivers
how do these map to a solution architecture
What components require standardization
What component are available in the commiunity already

Business drivers

Product information
Product state
Provenance
Dynamic Delivery
Replenishment
Customization

Compliance
Consumer engagement

Next steps include piloting some of the business driver use cases leveraging GS1 Digital Link standard and solutions.

Ask if GS1 to explore standardization of digital receipts.
https://www.gs1.org/sites/default/files/docs/internet-of-things/GS1_IoT_Handout.pdf

Part Deux! Permitify – dFlow in Action

Day/Session: Wednesday 4F
Convener: John Jordan & Stephen Curran
Notes-taker(s): Stephen Curran

Tags for the session – technology discussed/ideas considered:
#von, #sovrin, #ssi, #government, #verfiablecredentials

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

The session was a follow on to "A Catalyst For Trusted Digital Ecosystems (Part 1?)" (Tuesday, Session 3A). We began with an overview of the motivation and concepts behind TheOrgBook - a directory of **public** Verifiable Credentials about organizations or individuals, and the related (usually Government) Services that issue authoritative credentials (registrations, licences and permits) to both TheOrgBook and to the SSI-enabled subjects of the Verifiable Credentials. The slide deck for the presentation is here, and those interested can view a webinar of an earlier version of this presentation.

Next up was a summary of the technical components of TheOrgBookecosystems (perhaps to be called "Hyperledger Indy Catalyst" in the future) that we have in production today as the BC instance of TheOrgBook. That includes:

- TheOrgBook - a Sovrin Agent that has a community wallet holding (currently) over 1.4M Credentials, including one or more for every incorporated (and "Doing Business As") entity in British Columbia. TheOrgBook also has a processing engine for credentials to create a web- and API-accessible searchable directory of organizations based on Name and Credentials held. TheOrgBook is also capable of allowing search on locations of the entities.
- VON-X - a Sovrin Agent designed to make it easy for existing Credential-issuing Services to issue digital Verifiable Credentials - currently just to TheOrgBook, but in the near future to subject organizations directly.

TheOrgBook has been built on Hyperledger Indy software and is anchored in the Sovrin Provisional Network (DIDs, schema, etc.).

We also talked about (and answered a number of questions about) the enterprise-ready elements of the solution, including the horizontal scaling (capable of processing 3,000 credentials/minute), enterprise storage (Postgres database), and supporting tools for development using Docker and deployment using Red Hat's OpenShift Kubernetes platform.

From there, we demonstrated Permitify, an early version of a "dFlow" - a Decentralized Workflow application built on top of TheOrgBook ecosystem. Our workflow challenge is helping (particularly) new and small businesses navigate the myriad of jurisdictions, permits and licences necessary to open a new enterprise - a restaurant, shop or service provider. The problem is usually just left to the business to learn as they go from the various Issuers, although some manually curated directories are available (such as Bizpal in Canada). Neither solution is ideal - the latter because of the workflow variations and ever-changing requirements. The idea behind Permitify is that each Credential issuing organization declares, through their SSI proof requests, the prerequisite permits and/or licences needed to apply for the permit/licence they issue. By iteratively (recursively) and dynamically finding the prerequisites for each credential, the business owner's Agent can provide a roadmap to the goal. Further, by checking their Digital Wallet for those credentials, the Agent can determine exactly where they are on that journey - what verifiable credentials they have and what ones are left to get. The decentralized component of the solution is that each Issuer need only state what they require before accepting applications, vs. the entire, ever changing, workflow for each scenario. The Agent collects the decentralized information and presents it to the Business Owner.

Questions or comments should be directed to: John Jordan, Stephen Curran

The HumanOS as an Identity Generator (Implications on the Digital Domain)

Day/Session: Wednesday 4G
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:

When a person creates a profile to, say, meet someone via social dating, imagine the following situation...
One person's profile (persona, aka identity) is created after experiencing being cheated, loss of their job, and is feeling lost and needy. Recent experience of broken trust and doubt of self may be quite foundational influences of profile questions.

Another person profile (persona, aka identity) is created after experiencing getting a raise, buying a new home and getting great results from the doc regarding their annual checkup. Recent experience of appreciation, personal growth and wellness may be quite foundational influences of profile questions. How different are the influences affecting those two different profiles? What is it those two different profiles are reaching for in a relationship search? The first is a somewhat dark and tortured moment. The second is a moment in the clouds, lofted by joyfulness.
This is an example of how our Real World impacts choices regarding the identity we establish on the digital landscape. Our Human Operating System (HumanOS) has different outputs and requests, relative to state of mind, of the individual at the time of choosing how to relate to the digital landscape. With that said, we would expect two very different wants.

Ready for the reveal? The profiles were created by the same person five months apart. This is how our HumanOS impacts the "identity" we choose to express in the digital world. Circumstance drives sense of wellness and want. If the person discussed above is rather "steady state" regarding their emotions, we may see a near exact profile in either case. If they are volatile, prone to histrionics, or manic you probably would not recognize the profiles as originating from the same person. They may even be so different you wouldn't believe they are the same person in two spaces of life circumstance. Our human nature and the aspects of personality, behavior and reaction can vacillate. Influences on our demeanor can be extremely changeable. Translation and how we project ourselves onto the digital landscape can, by choice, be not only variable but designed to meet an intention of some will rather than a reflection of a moment. The translation may be false and misleading if we are in a dishonest way. Translation may be designed to conflate who we are somehow if we believe gain of some sort is the reward for the self.

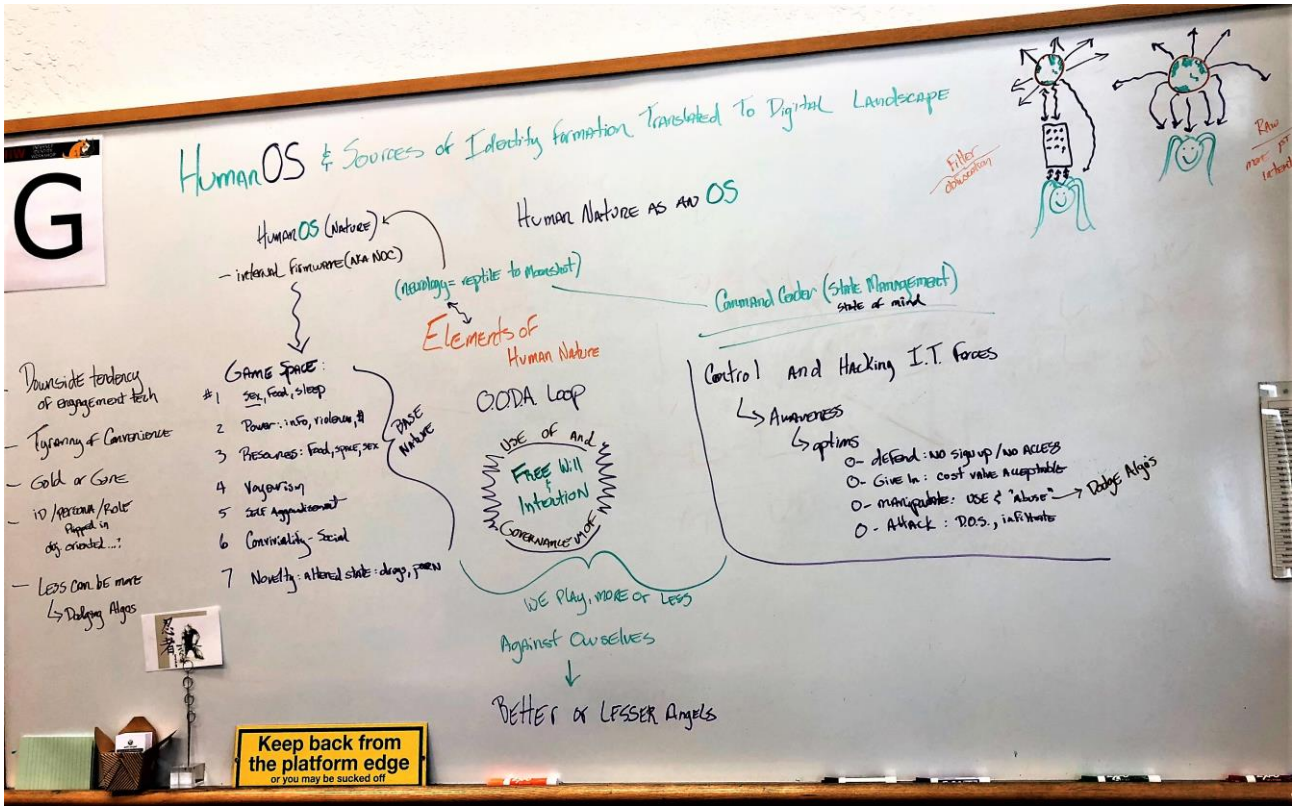
Here is the crux of this issue. Being Human. We are susceptible to change and influence. Our nature has soft spots. Wanting to fit in. Wanting power. Wanting sex – a prime mover. Wanting to look to others.

The software systems and influences on our nature challenges us and often baits us to engage. Is the engagement nourishing for us or a profit for a system and people or persons behind it? Humans are well known to engage lightly on positive topics and more deeply on topics which anger us. A good story may be told to a couple people whereas an annoying or angering topic will be spread to a dozen people.

If the pay model of a system is engagement based on algorithms that drive stories and topics towards the user, would it not be somewhat evident that negative and annoying topics are herded to people

and thought communities. The algorithms probe to surface human nature which should fuel and create greatest payoff for the system. Great for the systems and the folks converting that impact into their dollars. Meanwhile those same systems impact us by blazing a trail towards "the lesser angels of our nature."

Awareness of these frameworks combined with protection of our state of mind (Digital Aikido!), and clarity in terms of the goal of these systems, give the Human animal its best shot at maintaining and gaining our intention, all the while being subject to these forces.



Identity Proofing w/Open ID

Day/Session: Wednesday 4H
Convener: Torsten Lodderstedt
Notes-taker(s): (1) Torsten Lodderstedt & (2) Nick Roy

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

(1) Link to Torsten's slides: https://de.slideshare.net/TorstenLodderstedt/identity-proofing-with-openid-connect

(2) Nick Roy's Notes:
Identity proofing with OpenID Connect - Torsten Lodderstedt, yes.com
Verifying data that an IdP provides
Prove identity data to relying parties because the RPs have regulated use cases
There is no way to communicate that today in SAML or OIDC
Invented their own way to do this
Use cases
- Opening a banking account (anti-money laundering)
- Applying for a loan (AML)
- Mobile subscription (Anti-terrorism)
- ID for access to health data
- Qualified electronic signature (eIDAS/etc)

Needed for
user claim values
confidence level per claim or set of claims
data about the verification process and identity sources (e.g. document number)

Supports mixture of verified and unverified claims (self-declared and issuer verified)
Used with: User info, ID token, access token introspection
Needs to be a way to request specific claims to be verified (selective disclosure)

What verification means is defined by assurance frameworks, but need a syntax to transport the data
This is very similar to authentication context and vectors of trust, but they are not granular enough

Side note: Token introspection is a problem for Google/Microsoft because of scaling/throttling

Example
RP wants to verify user identity according to eIDAS assurance level substantial
Need Name, Birth Date, Place of Birth, Nationality
User was verified using national ID card by the bank, according to anti-money-laundering law
Bank has know your customer data associated with online banking account

How they did it:
Add a verified_person_data claim in a specific namespace (yes.com)
Verification gives all the verificatoins evidence, associated with a claims object
Externalize all the data collected to verify the data. Banks collect data according to anti-money-laundering law, but that data can be mapped into eIDAS verification requirements.
Method of proofing is included in the verification context because some forms of proofing are excluded

for certain use cases.
What ties the verification data to the claims? Nesting within the JSON. Claims are nested within the verification data.

Must be possible to dynamically request the claims
Extended the set of claims for OIDC because they needed some claims that don't exist yet

Requesting verified person data
Extend the claims parameter - can specify at the user info endpoint that you want to see a type of claim, and you want to make it essential.
The RP can specify which claims it wants from the OP
Mike Jones says the right way to do this is to make the verified_person_data type be an attribute of the claim you are requesting from the user info endpoint. One of the syntaxes is outside the claims portion and one is inside the claims portion in Torsten's model, which Mike says is incorrect.
But, also need to set parameters on the verification type - example: expected value of the max age of the verification date. Can't do that at the top level, or you'd have to specify that for each and every claim.

Step-ups scenario
Want a success/failure scenario - if failure, ask for a different set of claims. Does this support that kind of dynamic challenge-response?
Not doing protocol, just doing syntax.

Use cases exist, and there is money behind it.
Could see multiple signals coming from multiple directions - example the CIVIC demo. They are doing this from a different direction, using blockchain. They insert in the process of issuing something, where they can involve the verifier, and cache the result of the verification on your device, and place a hash of the information on the blockchain. Whenever you need verification, you just verify the claim on their device with the hash, so info never leaves the device.

Are there opportunities for collaboration?
Agree on the schema/syntax for this kind of assertion
This doesn't require c18n, whereas verifiable claims require RDF/JSON-LD and that has been rejected by developers with their feet. We shouldn't try to do that again.
Want the data, and evidence of the data, feed that into a risk engine.

How are the clients consuming the verifiable claims? Are they looking for specific strings of the proofing type, etc?
It's not being widely used yet - there is at least one client looking for specific values of proofing type.

Electronic audit trail for digital signatures - in case of dispute or audit.
The schema is a hard problem that needs a generalized solution.
RP knows what they want, but the question is how do they tell the OP what they want, and how does the OP communicate back to the RP what it can provide?

Some of the claims have a fixed list of values - starting point for creating a registry.

What happens when verification policy changes?
Need the ability to add new verification methods to the implementations/taxonomy

Should we be talking about standardized levels of methods to do abstraction? That maps back to stuff like NIST SP800-63, but that failed. Need to be able to express desired properties of a verification.

This feels like overcommunicating, the NIST method undercommunicates. We have to play with what works and what doesn't.

The issuer needs to sign the document so that you have verifiability that the issuer's claim isn't tampered with by the OP.

torsten@lodderstedt.net

Would want the verifier to sign things directly using the distributed and verifiable claims system in OpenID Connect.

How to Build Context-Aware Systems to Avoid Context Breaches in a World of Intelligent Agents, IOT, and AI.

Day/Session: Wednesday 4I
Convener: Jeffrey Friedberg
Notes-taker(s): Jeffrey Friedberg

Tags for the session

- Contextual Integrity
- Context-Aware Systems
- Context Breach
- Intelligent Agents
- IOT
- AI

Technology discussed/ideas considered:

- Controlling Identity Attributes
- Concept of "Contextual Integrity"
- Examples of "Context Breaches"
- Unique problems with Intelligent Agents and IOT
- How to enable contextual integrity in systems

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

Slide deck content with additional notes follows:

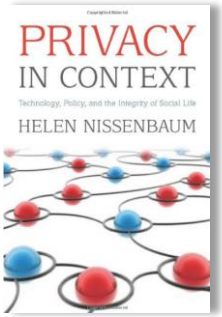
Controlling identity attributes

- Many attributes describe us
- Humans expect to be able to control who knows what

- Sometimes easy (wear a shirt to hide tattoos)
- Very hard in today's cloud-based world
- Using separate IDs (decentralized or otherwise) is not enough
- Smart data scientists linking across Device IDs, IP address, other data …
- By design, goal of many systems is to build a unified view of you
    - One big lump of identity attributes

Contextual Integrity

- A key concept introduced by Helen Nissenbaum could help



- Privacy is defined as:
    - ***Appropriate flows of data based on context and expected norms***
- Example:
    - Doctor / Party
        - You visit doctor who is also a friend
        - Doctor treats a sore in a sensitive spot
        - You invite the doctor to a party
        - At a party, when you are standing with others, you do not expect the doctor to ask about the sore
    - Salary
        - In the US you typically do not share what you are paid
        - Other places, may be a norm (e.g., must report to IRS)

Context Breaches

- Definition***:***
    - ***Data appropriate for one context is used in other that causes a range of harms***
- Examples:
    - Itch cream
        - You are home and need to find some itch cream for your sore
        - You log in with your personal ID and search for itch cream
        - Next day you need to give a presentation to your boss's boss
        - You log in with your organizational ID and need to surf the web
        - What are the chances you will see itch cream ads down the side of the browser?

- Target
    - Company was able to deduce from purchases a young woman was pregnant
    - Young woman did not know she was pregnant
    - Congratulations were sent with discounts to account holder – her father!
    - Big surprise with big social/family consequences

- Message leak
    - My colleagues were giving a big presentation to my boss's boss
    - My manager was unhappy with the pace
    - He sent a nasty instant message to get on with it
    - On the big screen, a toast popped up with the message for all too see!
    - System was not context aware. Could have easily checked a presentation was active and the message was not to the same list of people as was invited to the meeting!

- Cell Phone Wipe
    - I'm allowed to get my corporate email on my personal cell phone.
    - My young son picked up my phone that was locked with a PIN. Thought it was safe for him to play with it. 2 minutes later, he handed it back and phone was completely wiped. Lost 3 months of family pictures.
    - Company was worried I might lose my phone, a bad guy might find it, try to guess my PIN, and steal corporate secrets. They put a policy on the phone that would wipe all contents after 5 attempts to enter my PIN.
    - The issue isn't my company wanting to protect their assets. The issue is the deletion feature was not context-aware. i.e. It's OK to delete pictures of whiteboards at work. It's not OK to delete pictures of my kids at home.
    - With pictures getting tagged with time of day and GPS location, and with facial recognition, the system could have distinguished my personal photos from ones in scope for deletion.
    - Side note: to protect against a child deleting all photos on a locked phone, all the company had to do was to set the maximum attempts to 10 instead of 5. On the iPhone, after the 5th try an increasing time delay is added and a child would quickly get bored and give up.

- Range of harms for a content breach
    - From temporary embarrassment to life changing impact (e.g., leaking your sexual preference in some parts of the world could get you killed).
- Need to consider context in design!
    - Most systems aren't tracking context yet or using it to gate data operations and flows!
    - Should add "Context Breaches" to the threat model and test for it as part of the software development lifecycle!

Unique Challenges

- Intelligent agents
  - Can be more effective if they know more
  - Higher levels of trust needed
  - Need to get context right!
- IOT
  - Limited opportunity for consent
    - At a high-end store where I live, as you walk in, behind the fern, there is sign that says my location is being tracked (via my cell phone's IEMI #) so they check my dwell time in front of different products and use that to market to me.
  - Must pass on context to avoid harm

Open Discussion

- How do we enable contextual integrity in systems?
  - What goes in plumbing? In the UI?
- Which context attributes to capture?
  - What to capture first? Work/School/Home?
- How to model expected normative behavior?
  - Needs to be culturally localized
- What tools can we leverage?
  - AI, D* Identity, Privacy Chain, …

Identity, Ethics, and Digital Inclusion – the IEEE DITA Program

Day/Session: Wednesday 4J
Convener: Greg Adamson
Notes-taker(s): Greg Adamson

Tags for the session - technology discussed/ideas considered:
#digital inclusion, #digital ethics, #cyberspace access

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

The IEEE program DITA (Digital Inclusion through Trust and Agency) is looking at issues that limit access to the on-line world. These could be expected, such as cost and availability, or complex and social, such as on-line harassment in virtual reality gaming. Points of interest raised in discussion:

- Risks in digital controls for property rights;
- Ownership of data collected from vulnerable communities;
- Inclusion in business models for developing countries;

Achieving mutual respect through consensus in on-line communities.

Civic AMA: Product & Partners

Day/Session: Wednesday 4K
Convener: Zachary Bush
Notes-taker(s): Titus Capilnean

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

Civic's Secure Identity Platform (SIP) uses a verified identity for multi-factor authentication on web and mobile apps without the need for usernames or passwords. Through the decentralized architecture with the blockchain and biometrics on the mobile device, our platform provides multi-factor authentication without a username, password, third-party authenticator, or physical hardware token.

Zack demonstrated Civic Connect. The app-to-app libraries for Android and iOS enable partners to trigger an identity verification process natively from within their app with the "Connect with Civic" button. Users authorize the verified credential request and can then continue with the app they intend to use.

More information: https://www.civic.com/blog/introducing-civicconnect/
Demo: https://www.youtube.com/watch?v=Bu5dPa3egGY
Questions revolved around the architecture, the way the app communicates with the server and the Identity Requester - more technical information can be found here: https://docs.civic.com/

Subjective vs Objective Identity

Day/Session: Wednesday 4L
Convener: Duane Johnson
Notes-taker(s): Duane Johnson

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

We started off talking about the slide that Duane prepared, dividing identity into "subjective" and "objective" sides.

We proposed various alternatives, thinking of it as a "spectrum of trust" and "relative trust" that is relative to either the issuer's perspective or the verifier's perspective.

We noted that a "claim" implies subjectivity (as opposed to a "fact").

We also talked about Kaliya's master's thesis at identitywoman.net. The conversation then shifted towards uPort implementation details because of the proportion of participants from uPort or interested in uPort.

Link to Slide:
https://www.dropbox.com/s/1q6hbxejchr3g27/2018-10-21%20Subjective%20vs%20Objective%20Identity.pdf?dl=0

Seed Quest & Didery (3-D Game Mnemonic DID Key Store)

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

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

Link to slide deck for this session:
https://github.com/SmithSamuelM/Papers/blob/master/presentations/SeedQuest_Didery_IIW20181023.pdf

The Identity.com Ecosystem – Introduction & AMA

Day/Session: Wednesday 5D
Convener: Martin Riedel
Notes-taker(s): Martin Riedel

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

Link to session notes from Martin Riedel:
https://docs.google.com/document/d/1WZQrUrrAMik8ZRGdPIBp48VWeveOgjez5F3hdLquge8/edit?usp=sharing

Manifold: Give Your Things an Identifier

Day/Session: Wednesday 5E
Convener: Bruce Conrad
Notes-taker(s): Bruce Conrad

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

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

Manifold (see manifold.picolabs.io) is the user experience for picos (see picolabs.io)

We think of picos as virtual computers in the cloud (or wherever they are hosted) which are very inexpensive to launch. Every thing that we care to model corresponds to a pico. Ideally, the pico would be created even before the thing was manufactured, and would follow the thing through its lifespan, and even continue to exist after the physical thing was no more.

Picos have an identify and provide communication channels to other picos and outside entities. Each channel is identified by a DID and so messages can be encrypted and/or signed.

We talked in more detail about a couple of examples: an automobile, a supply chain, and land records.

Overlays 101

Day/Session: Wednesday 5G
Convener: Paul Knowles
Notes-taker(s): (1) Paul Knowles & (2) Robert Mitwicki

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

(1) **Link to Paul's slide deck for Overlays sessions:** https://drive.google.com/file/d/10RK6lEzpTbLzugfvlcWcB9mZghBOPQTC/view

(2) **From Robert - in addition to existing notes we compose github repo where we put our demo:** https://github.com/mitfik/overlays-demo

Making Oauth Work on the Open Web (Share & Tear)

Day/Session: Wednesday 5H
Convener: Aaron Parecki
Notes-taker(s): (1) Aaron Parecki & (2) Tom Brown

Tags for the session – technology discussed/ideas considered: #oauth

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

(1) Links to Aaron's slides and files from session:

web link: https://speakerdeck.com/aaronpk/making-oauth-work-on-the-open-web
PDF: https://slides.aaronparecki.com/2018/making-oauth-work-on-the-open-web.pdf

Here are the links mentioned within the slides:

https://indieauth.net/

https://aaronparecki.com/2018/07/07/7/oauth-for-the-open-web

https://www.w3.org/TR/indieauth/

https://hacks.mozilla.org/2018/10/dweb-identity-for-the-decentralized-web-with-indieauth/

(2) Tom Brown's Notes:
Session is related to article: https://aaronparecki.com/2018/07/07/7/oauth-for-the-open-web

Discussion:
OAuth for the open web does not require client preregistration nor locked down user accounts. Instead, there is IdP discovery and bring your own identity.

OpenID Connect does not solve these original problems of OpenID

There can be any number of authz servers so it is impractial for devs to do client registration for all. For instance, Mastodon adoption has this problem because devs can't easily register on every instance.

UserIDs need to have a shared global namespace.

There is no overlap between Google and Microsoft user namespace, for instance.

Limit the problem space:
Client ids and user ids are full urls (provides path for discovery)

OpenID usability problem was with the way the url was presented to user, not the url itself.

The browser now autofills url and an email address can resolve to a url. Start with something that can turn into a url.

IndieAuth is just an extension to OAuth 2

Focus on the client:
client_id in the redirection url is the url of the appropriate

App info is published at the url that is the client_id. It seems choosing one of these three possibilities would be ideal:
1. parse HTML for microformats (downside is that server needs a microformats parser)
2. manifest.json
3. .well-known
(an example client is https://quill.p3k.io/)

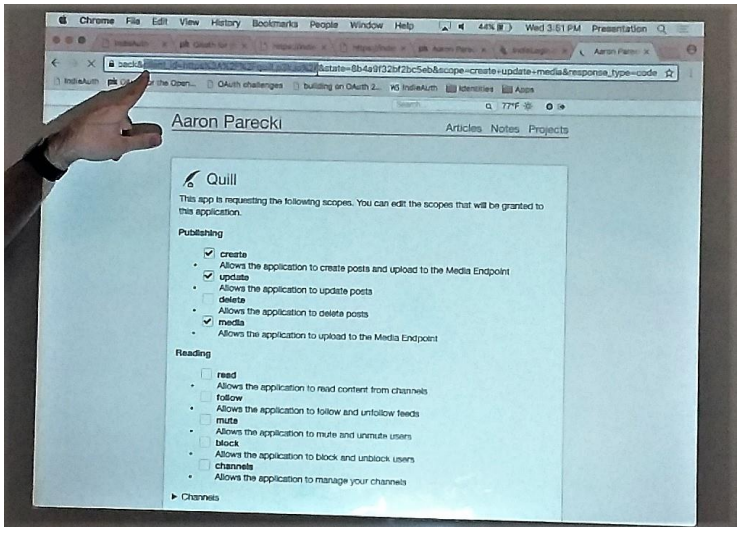
Let's consider beyond the Indieweb and include the open web which does not seem to include enterprise.

Justin R. references Kitties are Fluffy!

Book ref: Why We Fail https://rosenfeldmedia.com/books/why-we-fail/

a traditional IdP often doesn't want to allow arbitrary clients that haven't registered first

SPs often want more than a subject
https://indieweb.org/authorization-endpoint



Data Store Interop? How Do We Bridge Private Islands of Users?

Day/Session: Wednesday 5I
Convener: Lisa LeVasseur
Notes-taker(s): Liam Broza, Lisa LeVasseur

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

How do we bridge islands of users? Technology islands [micro-ecosystems] created by Identity Systems, Digital Wallet/Data Store providers, etc.

Observed Pain Points with current state of Personal Data Ecosystem industry:

1. App development is hard—which technology choices do I make, as an App developer/service provider to consumers? Which data store "sandbox" do I choose—I can't build for all.
    a. Unfavorable economics of app development.
2. As a consumer, I want to be able to go into Best Buy and buy hardware that complies with "I'm in charge of my data, data usage and contract"; I want to be able to select apps that comply with "I'm in charge of my data, data usage and contract". I want to be in charge my relationship with my service provider.
    a. I don't have enough choices for tech that isn't operating as surveillance capitalists.
    b. I want a grok-able "nutritional content" label for technology and tech providers.
3. There is a proliferation of "plumbing" / infrastructure, but not interoperable:
    a. Identity systems,
    b. Personal Data Stores / Digital Wallets,
    c. Consent management/permission management solutions.

Need interoperability around:
- The way things decentralize,
- The way things authorize, and
- The way things get stored.

* and the way things get shared.

Are there sufficient standards for this?
- Indy Agent - https://github.com/hyperledger/indy-agent
- Daniel Buchman – DIF?
- Zero IDF?
- <one more I didn't catch>

Need to separate data model from the Auth model.

Need an IDL for data; so then we can index & query and write services on top.

how to mind map concepts, project & people.

Human factors considerations: peoples' existing [bad?] habits vis a vis apps and technology.'

Business model considerations: Big dogs not particularly incentivized to change their business models.

- > won't happen until users have choices other than the big dog ecosystems.
- Need a new ecosystem

Some talk about open hardware development, getting also at trusted devices/platforms, and the economics that open HW will enable.

Need a solution that addresses both technology enablers and business models.

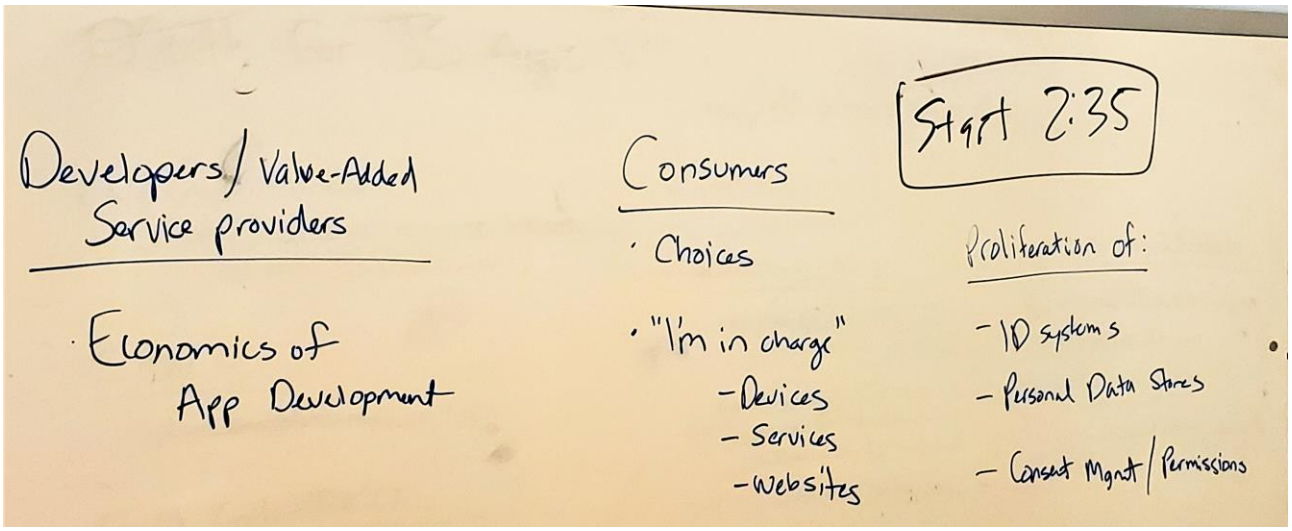
Discussion around industry consortia that create industries by:

- Clarifying and or writing specifications,
- Certifying solutions (in this case HW, apps, services, websites)
- Consumer facing brand, promotion, education, and fostering adoption

Is there interest in such an industry consortia?

- Yes

Whiteboard from this session:

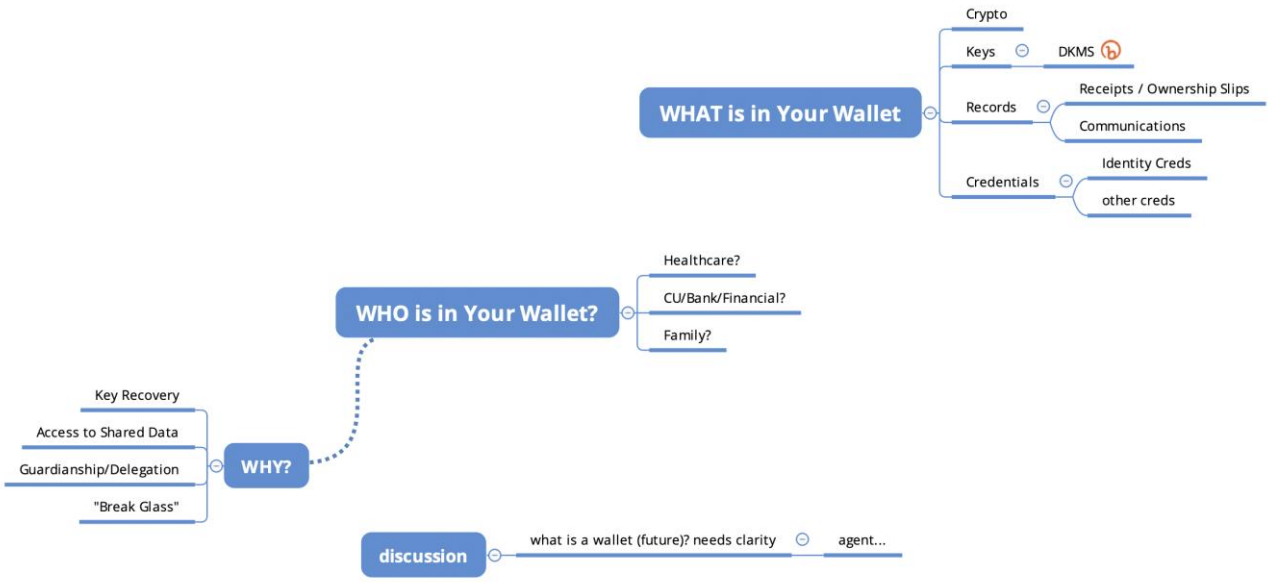


What's In Your Wallet? & Who's In Your Wallet?

Day/Session: Wednesday 5J
Convener: Darrell O'Donnell & Drummond Reed
Notes-taker(s): (1) Darrell O'Donnell, (2) Heather Vescent, (3) Alex Laws

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

(1) Darrell O'Donnell's DKMS Link (full write-up/presentation) http://bit.ly/dkmsv3



(2) HEATHER VESCENT'S LINK TO GOOGLE DOC + NOTES BELOW:
https://docs.google.com/document/d/1siiTA04zNUqe5hQasmkd9OhUYSdtyFSUVU8xu0J_OVQ/edit?usp=sharing

What are in your wallet

- Crypt
- Keys
- Records
- Credentials

Who are in your wallet

Do not want to talk about crypto wallets.

What's in your wallet that you really need.
What does my digital wallet do for me (as a developer) or for my mom (no cell phone)?
Is there a delegation role for me to take care of it for her.

What kind of credentials?
Digital Driver's License

Service card (BC) the card + attributes

What is a vault vs a wallet?
I want to be able to get at it.
Records of communications.

Who have I been interacting with via a wallet.

The terms wallets and agents.
Wallet is a storage - in the sovrin world.

We used to carry phone numbers in our wallet, pictures of our kids.
As a developer, it's an SDK.

There's different levels to what a wallet is.
See it more like its an app

What happens when Apple makes a wallet sdk that meets all out needs?
My app has wallet capabilities.

Are we securing the data in the secure elements?

Who is in your wallet - with you?
Re: medical records.
Break the glass situations for medical.
Cloud of 3rd parties…
Bank, financial advisor, can you have their software agent,
Loyalty program membership
Or part of a credit union.

The wallet becomes a capable thing.
You want certain agents to see certain parts.

Scheduled drivers license - prove over 21.
Does my wallet protect me - they are asking for your police version of the dr license.
Guardianship

Can you do that for me in a business environment.

What's the role of a bank or FB friends.

-- Drummond gave update/history of DKMS, DHS S&T

(3) NOTE TAKER: ALEC LAWS

Definition of Agent/Wallet

What does it mean to issue or use a wallet?

What & Who is in your wallet? Stuff...

What's in your wallet? crypto/keys/records/credentials
Who's in your wallet? Healthcare/ Bank/CU/Family

ignore the crypto side

crowd Q. what is the audience for this dicussion? devs? 'normal' people? my mom?
- all of the above, more about what the defn is

** WHAT
- keys: important, stored securely (TEE) OR on a server
- credentials:
  - identity document ex BC service card
  - corp registration
- records
  - what utility does it have?
  - fidelity of a receipt -> line items with diff classifications
  - ownership/warranty
  - communications records
  - this is getting bloated

vault vs wallet?
- don't want to carry everything around

cQ. a wallet is an app. an agent is in the cloud? many vs some people
- in sovrin wallet is secure storage

there is some ambiguity, but _I_ don't care

definition of wallet is a moving target
- ex no long keep phone number in wallet, photos of kids etc
  - they have been moved to

wallet is akin to real wallet, keeps stuff I need

**WHO is in the wallet
- ehr and a telco
  - break the glass (in emergency) based on other credentials (ie doctor)
  - NOT key recovery
- bank knows where I spend money, loyalty rewards cards

specific people can see specific parts of the wallet
ex digital driver ... proof of age ...
guardianship, who can sign FOR you

key recovery
- will you remember where you put the backup in 10weeks, years
- Facebook friends.. don't really trust that

2 levels of the wallet
- ssi, ux questions, how to actually manage this (ie key corvery), how it works behind the scenes

DKMS (hyperledger indy)
- dids -> blockchain -> privacy problem
- BC only for identifiers
- dids only useful if YOU control keys -> DKMS

how to solve key recovery, interoperability, portability

android vs apple wallet users
apple 50% use
android 5%

DHS problem, standard for interoperability between DKMS wallets?
- recommend that it becomes a standard (OASIS has some work, KMPI key management interop interface, enterprise level)
- prevent vendor lock in
DHS wants to complete 'baseline' functionality, in HL indy, by Q1 2019
- they will fund review of indy code base, then to OASIS

edge/cloud agent/wallet
- agent acts on a wallet, wallet is storage, agent is actor
- agent is either at edge (under user control) or cloud (not on HW controlled by user)
  - cloud can by HSM (hW sec module)
  - this is a policy decision

analog to email (clients/servers)

edge agents must be able to connect directly
- ex pulled over by LEO without cell signal
- DKMS covers protocols for agents to communicate
  - not structure of wallet
  - but interfaction between agents

edge to cloud agent can have strong auth (agent/agent comms)
- recovery from other device sin network (ir family)

cQ. does key manger mean private key management, or pk exchange/rotation
- BOTH
- in sovrin did is part of base58(pubkey)

cq. dmks covers way more that centralize key manage
- yes

nist 800-135(?) design of crypt key management systems
  - meta spec for designing kms
  - what applies to dkms (80% overlay, 15% sorta, 5% irrelevants)

cQ. how social recovery works?
- see dkms report (indy-sdk)
- agents automate the process except the most social step
  - id verification should be out of band (between the trustee and key owner)

- encrypted wallet backup to cloud
- add trustees as you make connections
  - nothing for user to do, but select who do they trust

cQ. wallet sync between owners edge agents
- yes/no
- design NEVER shares private keys across wallets, only did's

cQ. do you share link secret?
- YES
- used for zkp
- BLS has no correlations

- derived keysa are a special use case, ie group key for multidevice comms

cQ. is cloud agent mandatory?
- NO
- edge agents aren't' required either
- some parts are more challenges
  - message routing without cloud agent
  - ie pub/sub router
- edge agent can comm directly with did layer (BC)

Who's in your wallet? your connections
did-did channels (pairwise pseudonymous) can be used for ANYTHING

cQ. data edge agent wants to store NOT in the wallet?
- that's a vault, secure store that's not in wallet
- vault is cold storage of wallet data?? not what you want right now
- vault stores credentials?
- vault encrypted by keys in the wallet

DKMS Spec: https://github.com/hyperledger/indy-sdk/blob/master/doc/design/005-dkms/DKMS%20Design%20and%20Architecture%20V3.md
DKMS is an entire approach

Thursday October 25

OAuth 2.0 Security for Dummies

Day/Session: Thursday 1B
Convener: Torsten Lodderstedt
Notes-taker(s): Torsten Lodderstedt

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

Torsten presented the recommendations outlined in
https://tools.ietf.org/html/draft-ietf-oauth-security-topics-08

Link to his slides are available here: https://de.slideshare.net/TorstenLodderstedt/oauth-security-4-dummies-iiw27

Notes:

-- Redirect URI matching

Q: Does this document replace RFC 6819?
A: It will be an enhancement.

Q: We have many customers, who do not want to match the entire URL but only the hostname part. What would you tell them?
A: The exact redirect URI matching helps against open redirection. It is also about leaking URLs in refer headers
This was also behind the attack against ESPN.

When we say use a whitelisted URL then part of the guidance should also be to use the state parameter to convey information to get back to where they want to be.

Q: We have so many redirects and we cannot manage whitelists for all of them.
A: Maybe there is a need for text about how to solve the use case.
A: In SAML we have been using the cookie to determine where the user originally came from and to make sure that he / she get back to the starting page.

-- State parameter for XSRF prevention

Q: What do you mean by PKCE or nonce?
A: Nonce is from the OpenID Connect world and is not available in OAuth. PKCE wasn't intented for this purpose but it also provides the same protection capabilities. It is not exactly the same functionality.
A: From a spec point of view it would be better to just recommend PKCE since it applies to all OAuth deployment.

-- Mix-up prevention
(AS-specific redirect URIs: The client needs to remember what AS it talked to and when the redirect comes back it matches it against the stored value.)

Some groups use the state parameters to restore the proper state the client was previously. State is very flexible and useful. It is also used as a an XSRF. The use of the state value is referenced.

Hans mentioned that there is a draft about the state parameter encoded as a JWT:
https://tools.ietf.org/html/draft-bradley-oauth-jwt-encoded-state-08
It is currently expired.

-- Token Reply
Recommendation is to bind the access token to certain originators.

Q: In a lot of distributed system the refresh token exchange is handled by one system and the access token exchange is handled by a different system. I am retrieving contact info and email. The systems are independent services. I have a central token management service. The client is a collection of distributed system. How do TLS-based apply in such a world?

A: I don't think they would work. We don't have anything today that secures this model.

A: Drawing was created. <<figure goes in here>>

Suggestion to turn the token service into a proxy, which could make handling more difficult.
All requests would go through the proxy. There are, however, different scalability considerations.

Q: Could we use Token Exchange as an alternative?
A: Token exchange is yet another way to get more access tokens.
The question is also who is making the exchange.

Another architecture is being presented by Justin, which required more protocol exchanges but was more secure.
You need to understand your downstream dependency chain in the application.

<<Figure 2 goes in here>>

Justin wrote a draft about exchanging an access token against another access token in
https://tools.ietf.org/html/draft-richer-oauth-chain-00

Torsten mentioned that they implemented a similar service without having to understand the downstream dependency in the application but rather in the AS.

At the OAuth 2.0 level you need some "smartness" to implement these features.

Torsten says that the use of token binding with certificates is a recommendation and works fine in simple scenarios.

-- Access Token Privilege Restriction
Restrictions about resource server and action. It is not easy to implement but possible.

Any time I need an access token I need to get back to the AS to create an access token for a particular purpose.

If a mobile app wants to back to 15 different services then the mobile app needs to request lots of tokens (particularly when tokens have a short lifetime).

There is no way for the client to mint a derived tokens, with the limited scope. Torsten, you are suggesting to be Zero Knowledge Proofs.

Aaron asks what attacks are prevented by these restrictions. Privilege escalation attacks are prevented.
It would be important to point this threat out. Torsten says it is in there.

Q: Putting a URL in there is more restrictive; using a logical name is more practical
A: It is more difficult to have a logical location for practical purposes and for security matching.
A: Justin suggests to use both.

<<< Torsten wrote down notes about token leakage prevention. >>>

Q: Hasn't the audience been part of scope?
A: No, the scope parameter has been rather unspecified.

ME2B: Creating a Non-Surveillance Capitalism Market

Day/Session: Thursday 1F
Convener: Lisa LeVasseur
Notes-taker(s): Lisa LeVasseur

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

Me2B consortium proposal: https://www.slideshare.net/secret/2Vz2uCtUsZXcNt

Lots of support and recognition of need for such a forum to coalesce interoperability and certification in order to foster a thriving app/service market as well as creating a consumer brand. TBD where it will live. I will be facilitating the initiative, sending email and calling next meeting and steps.

DIDAuth + Obj.Cap.

Day/Session: Thursday 1G
Convener: Orie Steele & Alan Karp
Notes-taker(s): (1) Orie Steele & (2) Matthew Hailstone

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

Hosted by Alan H. Karp and Orie Steele, with notes by Orie Steele and Mathew Hailstone

https://alanhkarp.com/

(1) Notes from Orie Steele:

What is DIDAuth and how is it compatible with Object Capabilities?

We started by defining and describing object capabilities:

A Capability is a Transferable Unforgeable Permission. It can be implemented with unguessable URLS or signed objects.

A Java Program object reference is a capability, it allows for actions on the subject (the object instance).

A stronger implementation of object capabilities involves a digital certificate issued by a public key, for a resource with a set of supported methods:

Issuer: AlicePubKey
Resource: did:dad:0x123
Actions: Read,Write
Signature: 0x456

See attached image or tweet https://twitter.com/OR13b/status/1055540084106190848:

Public key creates a certificate that you give to a colleague that allows them to do work (capability)

Brown block is the delegation
Orange block is the use of that delegation

Object capabilities support Chained Attenuated Delegation.

President > General > Major > Private

Private does not have rights of president, and does not need to ask him or permission to act.

Its impossible to prevent delegation, so its critical that users or agents be thoughtful and be prepared to take responsibility for the actions of a delegate.

Its often preferable to be fine grained w.r.t. actions, so that revocation can also be fine grained.

We discussed the security model of a resource domain:

Identification

Authentication
Authorization
Access Decision

AuthN occurs at Grant NOT at the Use when using object capabilities.

DID AuthZ ~= Object Capabilities (could be!)

DIDAuthN supports mutual authentication in 2 ways:

Simple nonce + challenge signature flow between 2 DIDs (has privacy issues).

Authenticated Encryption (Diffie Helman / Group Key) produces a symmetric key for use.

Some discussion over the validity of NonReputability (there is no legal protection afforded, the term was created by cryptographers, and may not be helpful, but some people believe it is valuable).

2 Main issues arise when attempting to provide AuthZ for microservices:

Confused Deputy -> https://en.wikipedia.org/wiki/Confused_deputy_problem
Gross Violations of Least Privledge -> https://en.wikipedia.org/wiki/Principle_of_least_privilege

When Object Capabilities are leveraged these issues are addressable within a system for decentralized microservices. ACL or Authentication related approaches are problematic.

Sam Smith mentioned using CurveCP for DIDAuth.

https://curvecp.org/

https://github.com/SmithSamuelM/raet

Pelle from UPort mentioned waterken a system for object capabilities:

https://stackoverflow.com/questions/17297632/automatic-persistance-of-node-js-objects-in-database

Also uPort has an OpenID Connect related JWT implementation of Object Capabilities, that might be more compatible with legacy systems.

Alan mentioned https://w3c-ccg.github.io/ocap-ld/

Orie Steele closing thoughts:

I left desiring a concrete implementation of DIDAuth + Object Capabilities potentially built with

CurveCP, maintained under https://github.com/decentralized-identity/ and supported by the community.

We should support both a JWT and DID + JSON LD implementation for both modern P2P and legacy systems.

(2) Notes from Matthew Hailstone:

Object Capabilities / DID-Auth

What is a capability?

Take your keys and hand them to someone else in order to allow them to drive the car.

Enabling delegation of authorization to do something

URL with an unguessable string

Java program

Reference to another object is a type of capability

Public key creates a certificate that you give to a colleague that allows them to do work (capability)

Brown block is the delegation

Orange block is the use of that delegation

Attenuation

Chained attenuated delegation

Do AuthN and AuthZ at every request

4 steps to Access Control

- Identification
- Authentication
- Authorization
- Access Decision (at the resource at the time of the request)

Two things to protect

- Bearer token
- Revocation could be like a chain

Put the revocation on the blockchain and the distributed resource can check the blockchain

Not revoking the key, but revoking the delegation

DID-Auth

AuthN

DID uses a key to sign a nonce to another DID

(mutual authentication)

(authenticated encryption - sign cryption)

group key

diffy helman and key exchange

produces a symmetrical key

has the symmetrical key

hash the plain text

hash the cypher text

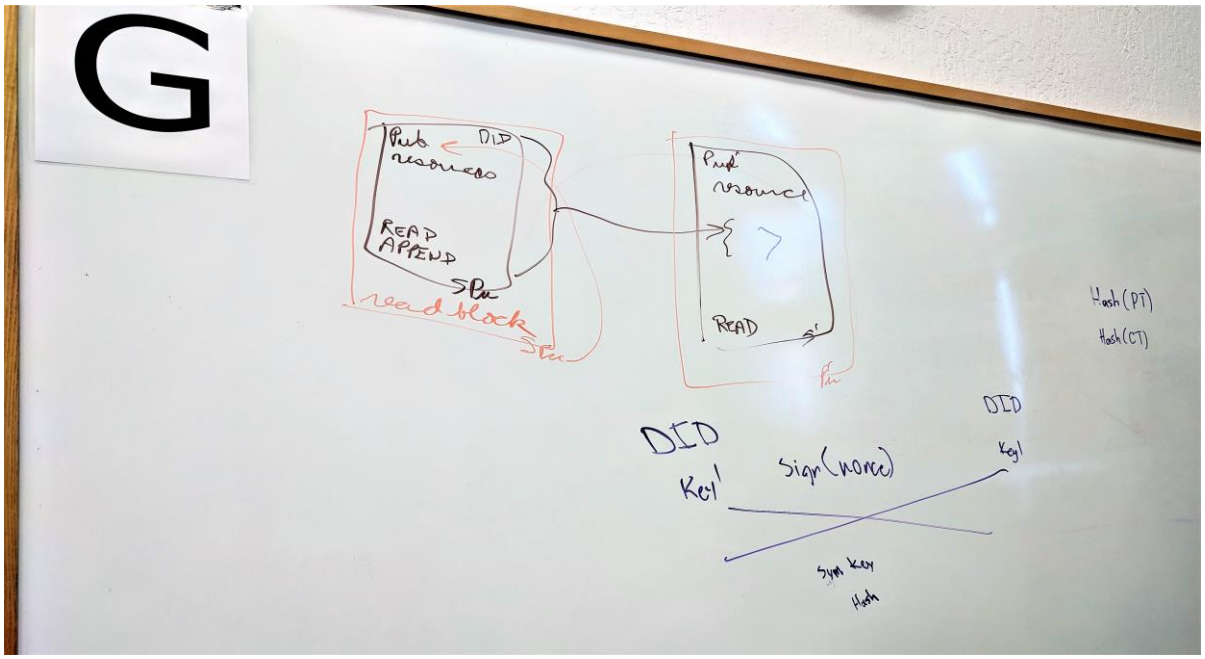
curve CP (daniel bernstein)

alanhkarp.com

SOA identity identification

zbac

water ken (ethereum)



Bliss & Emptiness – A Buddhist Approach to Identity

Day/Session: Thursday 1H
Convener: Heather Vescent
Notes-taker(s): Romain Lenglet

Tags for the session – Technology discussed/ideas considered: #Buddhism, #Philosophy, #Ego

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

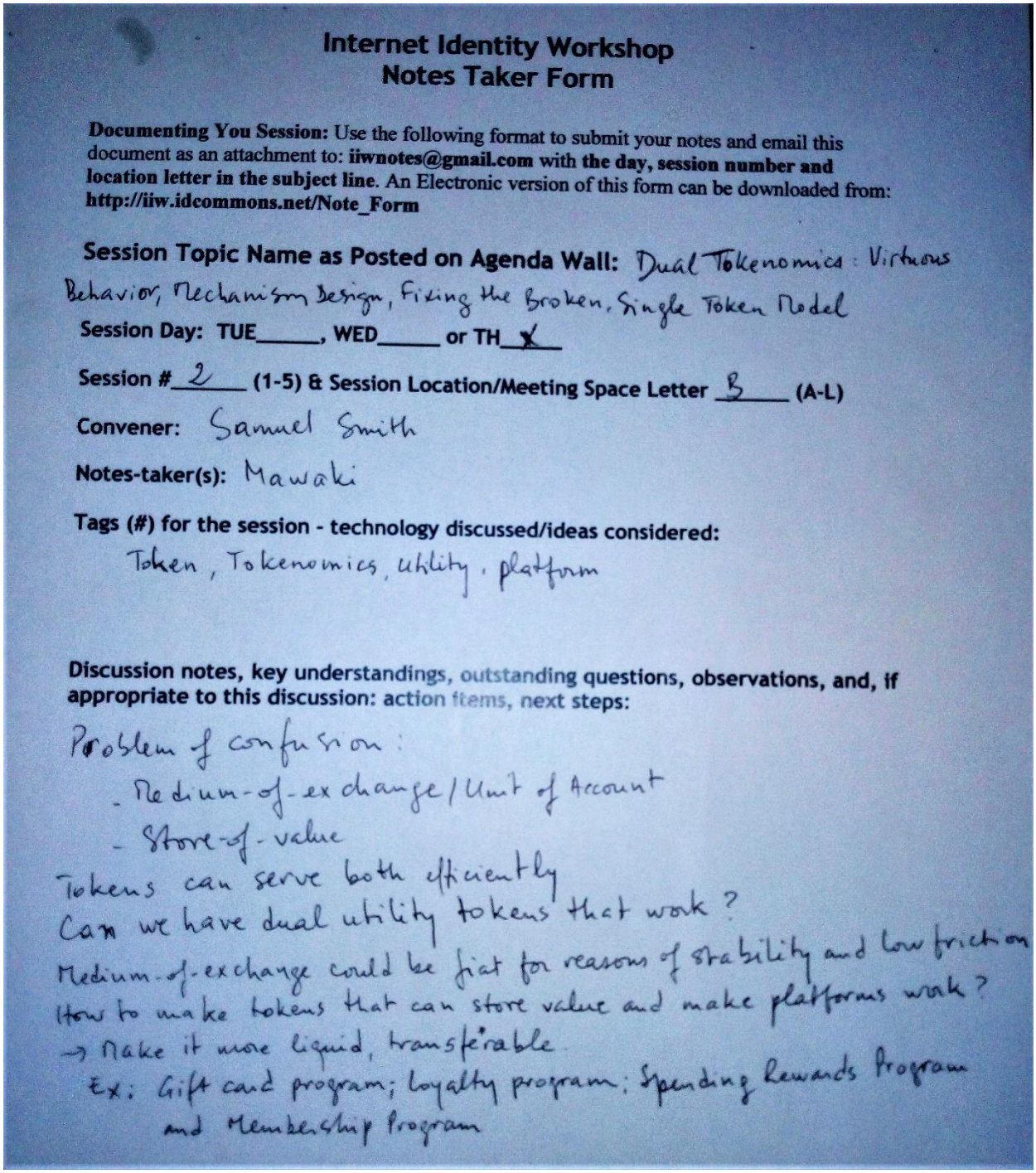
- How to deal with the large amount of drama and conflict in the world?
    - Reduce the sources of drama (people, etc.)
    - Heather interprets Buddhism as promoting emptiness
- Our identity changes over time, constantly
    - There is no consistent identity
    - We're becoming someone else, all the time
- In standards, we're not caring who you really are
- The question is: how can we help users be in a blissful state?
- The ego is an illusion
- But we are social animals
    - We need to interact and function in the world
    - So we adopt personas
    - This is a necessary and good thing
    - The key is to not *identity* with our personas
- One way to model this is
    - Personality -> Personas -> Roles -> ...
    - We typically each have lots of identities / personas / attributes
- One way to define our identity is in terms of our relationships
    - We are interdependent, inter-being
    - Ubuntu philosophy: I am because we are
    - "Collective identity"
    - Identity is a social and contextual construct
- The Australian definition of a person: someone who has a digital identity
    - That's a very extreme position, and it seems wrong
    - Bringing in a Buddhism point of view would help prevent going into such an extreme position
- Thai society seems to be losing its Buddhist tradition
    - They seem to be moving to Western culture
    - But there shouldn't be an opposition between Buddhist and Westerm cultures
- The risk of technology is that we may be trapped in hive minds / group think / echo chambers
    - We're driven by a need to belong, to be in a group
- Mindfulness is about being intentional in how we use our identity / personas
    - We are responsible for our own identities / personas
- Frustration with SSI
    - It's hard to manage the nuances of those many identities / personas
    - Technology should allow us to better manage our personas, and managing more personas
    - For instance, it could give us some insights / awareness about our own identity

    - Technology should help us with that, but it currently doesn't and may even prevent us

- Technology needs to better address the temporal aspect of identity
    - Better match our constant changes of identities over time
    - Concept of "identity flow"
- However, the overall conclusion is that technology has limits in how it solved identity
- We need better terms
    - Identity is too vague, and is used to refer to too many different things
    - Better terms would be: persona, identifier, ego, etc.
- No spider was harmed during this session

What's In It for Governments? (Potential Use Cases)

Day/Session: Thursday 1J
Convener: Mawaki Chango
Notes-taker(s): Mawaki Chango



Internet Identity Workshop
Notes Taker Form

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

Session Topic Name as Posted on Agenda Wall: Dual Tokenomics : Virtuous Behavior, Mechanism Design, Fixing the Broken, Single Token Model

Session Day: TUE_____, WED_____ or TH_X_

Session #_2_ (1-5) & Session Location/Meeting Space Letter _B_ (A-L)

Convener: Samuel Smith

Notes-taker(s): Mawaki

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

Token, Tokenomics, utility, platform

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

Problem of confusion:
- Medium-of-exchange / Unit of Account
- Store-of-value

Tokens can serve both efficiently
Can we have dual utility tokens that work?
Medium-of-exchange could be fiat for reasons of stability and low friction
How to make tokens that can store value and make platforms work?
→ Make it more liquid, transferable
Ex: Gift card program; loyalty program; Spending Rewards Program and Membership Program

Dual Tokenomics: Virtuous Behavior – Mechanism Design – Fixing the Broken Single Token Model

Day/Session: Thursday 2B
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:

Here is the Sam's link to the slide deck presented: DualTokenomics_IIW_20181025.pdf

MyAI – Gaining Insight Into Your Own Data

Day/Session: Thursday 2F
Convener: Sari Stenfors
Notes-taker(s): Travis Giggy

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

Facilitated by Sari: sari@aulead.com Emailed to: iiwnotes@gmail.com

What do we do with our data?

Starting with requests for topics:

Frequent flyer miles

- How can we shape a new loyalty? How do we re-make loyalty?
- Our own data has "use value" but little value in the marketplace.

A better relationship with United Airlines than now.
A better relationship with himself

- The basement of my life is so full I can't get downstairs

So much potential. What are the first steps we can be taking to give ourselves more insight to ourselves?

An idea to make a bathroom scale w/o a number readout. You have an AI that will give general advice about life. No angst about a number, just

"Jobs to be done list"

Travis: Organize your life and achieve your goals

How will he know that the AI will be controlled by him? How does he know that it has his best interests in mind?
Travis: Trust and companionship
Another way: do the computing at the edge on your own personal devices

Think of it as digital army.
Digital mirror. Lifelock on crack
Something that spins up bots and manages needs
Big companies have big data and analyze you. Why can't I do that for myself?

Sari wants to break up into groups
Instead, by suggestion, we are going to have all the people in the room who are working on something similar talk about their viewpoint for a couple of minutes each.

Sam Chase: Lifescope.io

- Builds mesh networks using webER in the browser, raspberry pi's
- Lifescope is a master API collector, grabs data bout you, collects it, you can learn about yourself. Trying to create the bedrock of a personal AI marketplace. Trying to create perfect context, allowing you to have streams into your life, more real-time AI.
- They have a wallet working
- Right now, OAuth, GraphQL, they are here for people to look at what they're doing, how to make it more secure, scalable, something that people want to use.

Rob Collins: TodayPlatform.com

- UI layer

Henry: Peercraft.com

- We have gone from local villages, the EU has an idea... if you want to shop for shoes, there are 100k-1M places to shop. If you go to Google and look at privacy policies, it would take 4 years to buy shoes. We need to speed that process up and extends our brain to be faster.
- We don't need AI, just ordinary logic

Travis: Akin.com

- A public benefit corp, measures success by the formula: Number of humans * Depth of relationship * Increase in well-being
- Creating a consortium of large enterprises who value their humans and want to understand the future of Personal AI

Wendell: Oath.com

- Yahoo, AOL
- Building tools for marketers
- AI = propensity marketing, used on large bodies of people to convince them to buy things

- He thinks of AI as "if you do this, you might want that"

Johannes: Indiecomputing.com

- Ships a personal server, has your personal data, goes in your house
- Wants to have an AI that runs right on it
- How does it come together in products that people can use, understand, buy?

Robert Mithicki: cling.online

- Create a substitute of your best friend. Something personal to you. Always with you, always in the places where you are, runs on your mobile, helps you out, discovers the surroundings. One use case is the simple thing of the networking. If the best friend knows the people in the room he knows who to introduce you to.

Sal: openconsent.com

- Have a privacy signal, akin to cargeigie mellon privacy beacon. Currently constrained by inputs, given AI they could make the signal more robust.

Lisa: wrethink.com

- Founded by Arlene Harris. Building family solutions, treating homes like small enterprises, they operate like a small enterprise, but without the technology. Automating the workflows in homes to help people live better lives and recognize the context of family. Built around personal goals. Users are in control of their data, their relationship.

Privo

- Created a device registry for kids. When you buy a mobile phone, when a phone connects to a network, the business can know that it's a kid.

Travis talks about architecture required to achieve an AI that could accomplish what we're talking about today.

Jobs to be done: what is needed to get it working? what do we want it to do?

- Sam: personal schemas. Wants to talk about data structure, not the things we could do with it
    - Given what we already have, sensors coming online, etc
    - Schema standardization first
    - Understand things that stress me out before they do
- Would rather have data models that don't rely on schemas. Ontologies
    - Smart toothbrushes or something?
- extend portability to extendability
    - end game: all work together, not one central place for data
- Worthwhile to break apart the roles we wish AI. A lot of it is pattern recognition, another is deeper data analysis.
    - End game: pick some low hanging fruit and eat it

- Johannes: first office manager he hired he had to travel, the next day she already figured out business insurance. She looked around, figured out what needed to be done, and did it
    - That is what he wants
- Need to figure out how to collect enough information. Not sure if info already being collected is enough to understand what he needs for his daily life.
    - AI will understand me in a ways that are predictive and not driven by him
- Need to find a way for ethical frameworks so analytic systems can recognize toward greater human well-being.
- Sari: works for IEEE ethical AI for human well-being. 3 year project, have done 1-year, have 300 different standards for human well-being. Doesn't even know how she would distill that.
- Wendell: Fiduciary crops up in these discussions. How a person or institution must act or behave. They don't generally extend to friendship, but do extend to well-being or in your benefit that you don't necessarily benefit, but need to do/know.
- Something that knows his ID's and when to renew them. Had to send a passport to a lawyer but it was expired. Someone who monitors spending. Has a kid on meds, doesn't trust anyone who is an MD, wants an AI who knows every human under my stewardship, flags for me if relationship between meds change. If it knows about him, can do stuff he doesn't have time for.
- Wants something to manage complexity. Settings/configure life to his personality would be useful. E.g., fix all the bad settings on his laptop. Docker for all his stuff
- Would very much like to see all analogies for who is wearing the collar. Where is the boundary of giveover where the AI puts collar on us and says "I know where to take you". Where is the governor or checkvalve there? Who is in charge? How do you express guardianship, inertia?
    - Would measure metrics of behavior. At start of relationship, more core human competencies you have, navigation. Over time, do you lose your ability to navigate?
    - re. Chinese tendency to give over decisions: it's a culture thing
    - Doc likes the metaphor of the collar, thinks agency is the way to frame it
        - End game: we're all dead. Perspective. But in the mean time he wants to help out. Doesn't think there is an end game, there is a constant process that is a tug of war and we're al victims. Thinks it is cool that there are potentially competing companies here that all want to work together
- Any tool we build should be simple enough that a user should feel some sense of control over it.
- Doesn't want to have AI. Wants to become. Doesn't want to lose himself. Why can't he do that stuff on his own? Doesn't want to outsource it. When does the digital avatar become more you than you are?
- The right mental model is Douglas Englebart (inventor of the mouse): Humans and machines have to evolve together. As I learn more, my machine can learn more.

Frequent flyer miles / Loyalty programs

- Wendell
    - Loyalty programs are a concrete thing you can do to help people. Many people love to collect stamps, miles, chips, the joy you hear from people who think they gamed

the system, people love that stuff. Behind it is modeling to figure out when it's going to work and what the outcomes of the population are going to be.

- When we talk about AI, you can often just insert the name "God" and get basically the same outcome. First we had honeywell thermostats, now we have Nest. When you have to do something concrete, it often looks banal, like a thermostat.

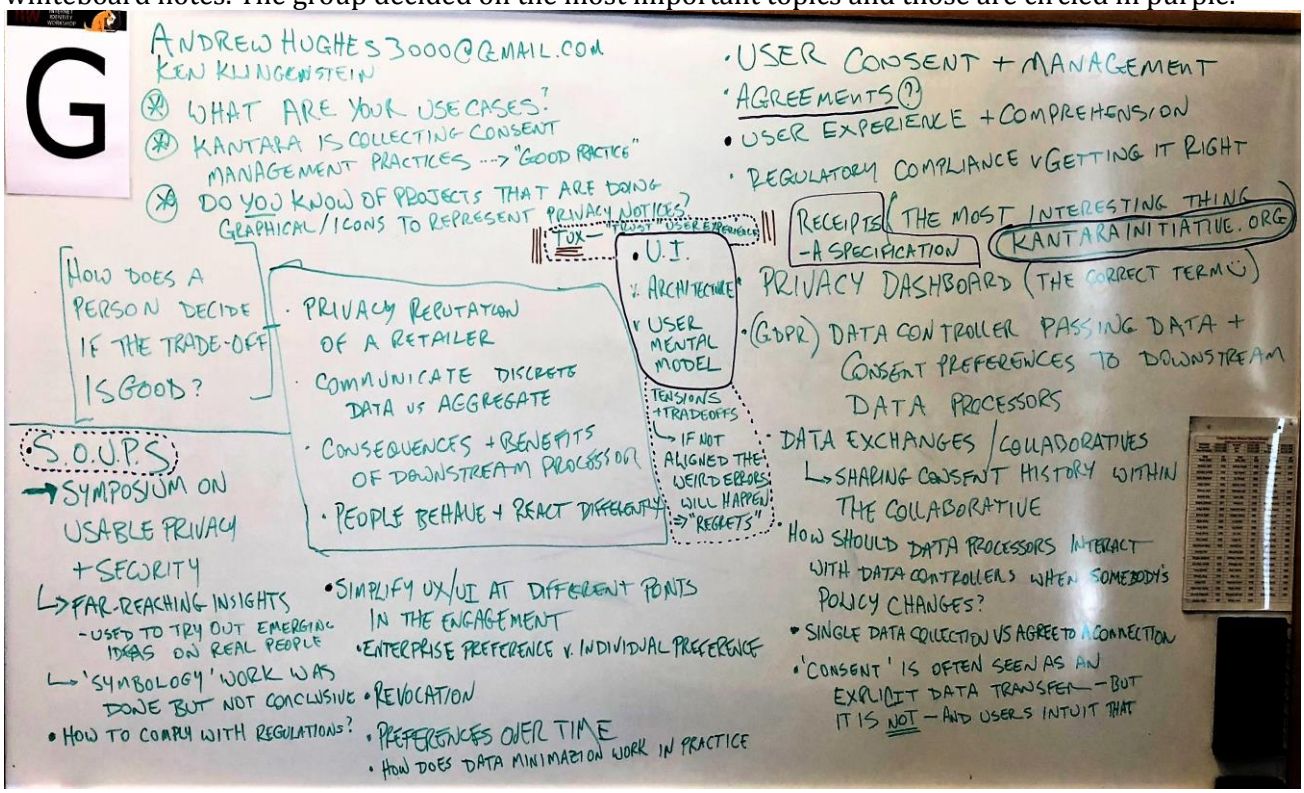
- Sam: Martech papers are unbelievable. Just switch out who it is for and we can apply a lot of the science elsewhere for good.

Consent Management – Receipts Practices Standards

Day/Session: Thursday 2G
Convener: Ken Klingenstein & Andrew Hughes
Notes-taker(s): (1) Andrew Hughes, (2) Jeffrey Friederg

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

We discussed the topic of consent - use cases, receipts, definitions, issues to consider. Here are the whiteboard notes. The group decided on the most important topics and those are circled in purple.



(2) From Jeffrey Friedberg:

Thank you for letting me introduce the concept of the Trust User Experience (aka TUX) in your session.

When users are placed in the "hot-seat" to make a privacy, security, or trust decision, they are presented a TUX. It is made of 3 things: the UI that is shown, the underlying architecture, and the

user's mental model. When any of these three are not aligned, the user will likely make a mistake – one they usually will not realize until later when the outcome of their choice is explained to them. And at that point, they usually have regret (something that can be measured).

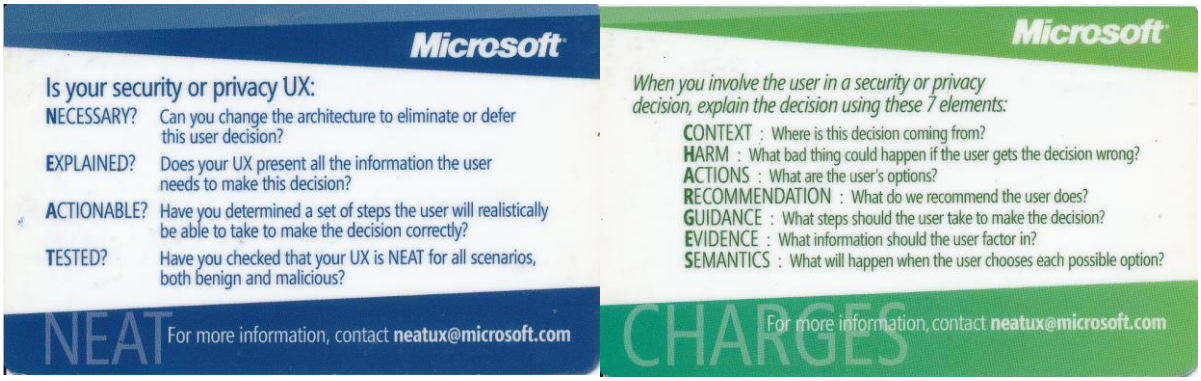
The TUX presented for consent is just one type of TUX. There are a number of different types of TUX including warnings (something bad could happen) and prods (a nudge to get you to do something). For consent the most common type is an "all or nothing" pattern. That said other patterns are possible, like a "haggle" TUX where the horse trade is negotiable.

Note, the T in TUX is for Trust not Trusted. The TUX is just that – something presented to the user related to a trust decision. Ideally the experience would be *trustworthy* (i.e. "trusted"), but we are unfortunately a long way off and many are deliberately deceptive or attempt to game the user into making a particular decision (per Cass Sunstein's "nudge" theory). At the end of day, designers of TUX are really "choice architects" and ideally, they should have a responsibility to be fair. Testing the TUX in a system should become part of the threat model and the normal software development lifecycle. TUX best practices, as they become known, should be taught to developers and UX designers.

Per you request, attaching some additional background on TUX and some suggested best practices:

- A 2009 Blog introducing TUX concepts and a call to action. I posted the content inline at the end of this document in the appendix for convenience.

- Wallet card of TUX Best practices. I believe the email address is no longer being monitored.



- Video of a Microsoft Research presentation I did in 2010 on the End to End to Trust initiative that includes a deep dive on TUX. Link here. My session starts at 41:07 and covers the goals of the initiative (to create a safer more trusted internet), the methodology, and some innovative roadmaps of what needs to be built. At 1:06:26, seven key families of building blocks are summarized including improvements to digital identity, the use of minimum disclosure claims, rules-based access to data, and TUX (1:07:38) which is a horizontal and needed for just about everything. The deep dive on TUX follows (for 20 minutes) and covers both good and bad TUX and some interesting research take-aways. And at 1:26:04. why informed consent doesn't work.

- Slide deck on End to End Trust from 2010. Link here. The deck covers similar content to the video above, but the slides are not compressed and useful as a companion to the video. The seven families of building blocks is posted on slide 23 and TUX is further explained with examples from slide 24 to 48.

Happy to engage others on TUX – the last two feet of end to end trust!

Jeffrey Friedberg

Appendix

Content below is from a blog I posted April 15, 2009

TUX: The Last Two Feet of End to End Trust

In his recent blog post, Scott Charney described a vision for End to End Trust. Core to the proposal is a trusted stack rooted in hardware. The "last two feet", the place where the user interfaces with the system, requires special consideration. It's where the user must make key trust decisions like: "Is this really my bank site? Should I install this software? Should I share my sensitive data?"

Unfortunately, the trust user experience (TUX) that is presented can be confusing to some users. For example, they may be perplexed by the written guidance or unfamiliar with the semantics of the security indicators. Many just click through these critical check points without fully understanding the implications.

How bad can it get?

Making a mistake here could expose the user to range of harms. At one extreme, installing rouge software could turn their system into a remotely controlled "bot" which can be used to send spam, enable identity theft, or worst-case help launch a cyber-terrorism attack. At the other extreme, choosing the wrong sharing model on social networking site could expose embarrassing photos to the wrong people, resulting in a damaged reputation and even job loss.

TUX vision and scope

Many consumers are uncomfortable having to make the trust decisions that are put in front of them. They would much rather just continue listening to music, buying products on the web, or chatting with friends. The trick is finding a way to increase their safety *without distracting them from enjoying their digital lifestyle.*

Poor TUX does not just affect consumers. It affects enterprises as well. It can lead to setting up the wrong configuration by an administrator. We have all seen the headlines: "Millions of records lost." The other issue businesses face is connecting with their customers. Users are told to be very suspicious of email and to not click on links. This forces some business to create walled gardens on the web just to have a conversation. The vision for businesses is to help them better connect with their customers and to honor the trust promises they made.

Whenever possible, it is best to address trust in the architecture to avoid needing to ask the user in the first place. No TUX is good TUX. However, when the user needs to get involved, the goal is "trust at a glance." It's unrealistic to think users will manually inspect a certificate or read every line of a privacy statement. We must find ways to increase the user's confidence they are making a good trust decision while reducing their need for doing all the leg work.

More than just UI

TUX is much more than just the user interface (UI) that is presented. It includes the underlying architecture of the system and the mental model the user has in their head. When designing and evaluating a TUX, *all three elements need to be considered.* Improving the UI will only take you so far.

In some cases, changes to the underlying architecture will need to be made. Likewise, it is important to assess whether the user is likely to form the appropriate mental model for the task and take steps to create better alignment.

Creating great TUX is hard

Users come in with different goals, expectations, and experience. There may also be cultural differences. When it comes to creating great TUX, "one size" unfortunately does not fit all. We need to understand what will really help a user when they are in the hot seat. In some cases, providing clearer guidance may help. In other cases, it's a design issue and new less complex controls need to be provided.

Some users would rather not deal with the risk analysis and would like to simply "call a friend" or "poll the audience". As in the real world, consulting outside advice from people, communities, and tools you trust can play a significant role in making better trust decisions (and can reduce anxiety). The ability to conveniently tap this information is often missing in the TUX that is presented. Establishing a common framework for providing reputation feeds could help users connect with advisors they trust.

One additional challenge to highlight is habituation. For various reasons, many users have given up trying to fully understand the risks and have gotten in the habit of just clicking "Next, Next, Next" (when was the last time you read an end user license agreement?). It's important to find ways to catch the user's attention and guide their behavior to safer outcome *when it's really needed*.

The path to better TUX

TUX is nascent discipline that draws from multiple domains (e.g., security, privacy, usability, accessibility, psychology, and anthropology to name a few). Across the industry and academia, a number of TUX-related efforts are in play. For example, in 2007 we assembled a TUX Advisory Board of passionate experts from across the company to help product teams with their critical TUX and to hone and validate best practices. On the education front, some schools now offer study in this field (e.g. Carnegie Mellon University has a Center for Usable Privacy and Security).

Join the discussion

As we and others investigate and mature this discipline, it's important to leverage the great work that has already been done and to find ways to collaborate. The End to End trust discussion is one such forum for engaging in that dialog.

Our ability to make good trust decisions starts with a trustworthy system. Per the End to End trust vision, we need to build in trust from the bottom up (i.e. a trusted stack) -- and it will take a global village to harden critical infrastructure components like the Internet. Identifying and deploying common metaphors for establishing trust relationships and making trust decisions will help reduce the learning curve for users and enhance the overall safety of consumers and enterprises.

What good is building great trust plumbing if we end up making silly mistakes in the last two feet?

Jeffrey Friedberg
Chief Trust Architect / Microsoft Corporation

How Should a Blockchain Social Network be Moving on Digital Identity Now?

Day/Session: Thursday 2I
Convener: Dave Room
Notes-taker(s): Dave Room

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

New social apps may want to use three ways to login now:

- email or handle
- auth through one of the big social networks or Google
- auth with UPort or Civic

Leading DID based solutions

- Uport
- Civic
- Sovrin

There was conversation about whether Civic is sufficiently decentralized.

There was conversation about how DIDs could carry group relationships so that groups of people can gain access to social networks based on the group affiliations associated with their DID.

Blockchain Myths & FAQ

Day/Session: Thursday 3C
Convener: Greg Slepak
Notes-taker(s): Greg Slepak

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

Background of presenter

- Greg Slepak
- Researcher, entrepreneur
- Read Satoshi's paper a year after it was published, became fascinated by blockchains
- Read Aaron Swartz's "Squaring Zooko's Triangle", became fascinated by Namecoin and decentralized, human-readable namespaces
- Worked on DNSChain, a DNS server that can do blockchain lookups for blockchain TLDs (top-level domains like .com, .org, .net)

Legitimate use-cases for blockchains

- Quick overview of how blockchains can greatly improve the security of the Internet
- Blockchains can change Internet's trust-model from "weakest link" trust model (X.509) to consensus-based trust through strong decentralized consensus algorithms like Proof-of-Work

Blockchain Myths

- "Bitcoin wastes energy"
    - No, it doesn't, it uses that energy to secure its blockchain
    - It does things that no other system can do, including PoS (proof-of-stake) systems
        - PoW can distribute coins without having to receive them from somewhere else
        - It can measure time in a trustless way and provide strong guarantees like "proof-of-publication"
        - Its security is cumulative
        - It cannot be "captured" in the same way that PoS consensus can be captured permanently by a cartel with enough stake
- "Bitcoin's energy use is bad for the environment"
    - Don't blame Bitcoin for humanity's choices when it comes to where it sources its energy from, this is not Bitcoin's fault
    - A few hundred square miles in the Sahara have enough solar energy to power the entire world
- "Blockchains can't scale"
    - Description of the problem and introduction to DCS Triangle and DCS Theorem
    - Scaling solutions that work around DCS Triangle like Lightning Network by combing a DC system with a DS system

FAQ - Answered audience questions

What Every Identity Professional Should Know: An Introduction to IDPro

Day/Session: Thursday 3F
Convener: Steve "Hutch" Hutchison
Notes-taker(s): Steve "Hutch" Hutchison

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

Presentation deck at -> http://identityhutch.com/docs/idpro-iiw27-hutch.pptx

What should every identity professional know?
You are not alone.

It sounds like a very fortune cookie phrase to throw out in a presentation. But the reason I say it is because if there's any common thread amongst the hundreds of members we've talked to, it's that almost everyone in the field has had to rely on themselves and their own initiative to learn this craft. For and identity professional in an enterprise environment, it's easy to feel alone.

The creation of IDPro was born out of a need to 1) provide support the existing identity professionals in the industry, 2) develop a book of knowledge to help build the next generation of identity professionals, and 3) provide opportunities for identity professionals everywhere to collaborate and contribute to the advancement of the industry.

To provide a roadmap, and to measure our success, we've adopted a number of efforts in five main program areas: Membership, Services, Operations, Industrial alliances, and the Book of Knowledge & Certifications.

Membership

- 16 months in and we have 500 members! This is particularly impressive to me as these people have all joined in the beginning when our service delivery is in its infancy. We take a lot of cues from the IAPP organization who said "the people who join at the beginning are the ones that not only realize there's a lot of work to be done, but it's the work that's actually important." So for those of you who have joined already, I thank you.
- Goal is to grow membership to 300 individual members with at least 5% from outside the US. On track with 270 as of today
- Goal of establishing an enterprise membership model for non-identity-related businesses

User Groups & Event Meetups

- We are currently tracking about 75 IAM user groups across the globe.
- Emphasize that these are IAM user group meetups and not IDPro chapter meetings. Our goal is not to come in and try to rebrand or take over any established group. What we would like to do is ask for 5-10 minutes during the meeting for an IDPro member to give a brief update of what's been going on as well as any new information about collaboration opportunities. In return for that, we will help to find speakers and materials for the meeting organizers to use.
- Currently piloting in Hartford, Charlotte, and Richmond.
- The local user group meeting is an incredibly important piece of the puzzle that accelerates progress in the industry. Not every one gets to go to conferences like this one but many more

people can attend a quarterly meetup in the local area. It is in those forums that lofty industry-wide discussions can be thrown up against real-life use cases from people in your area.
- Upcoming user group meet ups are listed on the IDPro.org website
- We have also had IDPro-specific meetups at RSA, EIC, and Identiverse
- Hutch has a biweekly cocktail party at his home in Richmond, VA every other Wednesday. You should attend.

Services
- Monthly Newsletter
    - Since November 2017
    - All issues are archived on IDPro.org website
- Slack
    - Daily realtime conversations
- Discussion Threads
    - Usage is lessening as Slack usage rises
- Events calendar
    - Curated listings for both user group meetups and upcoming identity-related conferences
- Speakers Bureau
    - Not just to provide speakers for events
    - Provide mentors and guidance for professionals who haven't spoken before, but would like to.
    - Would eventually like to provide scholarships for new speakers to travel to and attend conference

Operations
- Document and fully implement member on-boarding and off-boarding procedures
- Evaluate and select an association management service
- Evaluate adding dedicated staff to ease the operational burden on the Board
- Build sustainable financial operations capabilities including budget planning, ongoing accounts receivable/payables, tax preparation and filing

Industrial Alliances
- Completed
    - DIACC
    - FIDO Alliance
- In Progress
    - IAPP
    - Identity Defined Security Alliance
    - OpenID Foundation
    - Women in Identity

Body of Knowledge
- The BoK is expected to be the extremely important to the organization (and the industry). Therefore quality is highly valued.

- The BoK is expected to support a variety of constituencies, including practitioners (at various levels) as well as other professionals not entirely focused on identity - such as application developers, managers, and policy makers.
- The subject matters in the body of knowledge will include
    - techniques, methods, best practices that are applicable in general;
    - similar materials which are specific to industries and/or jurisdictions
- In some cases, there will be controversy about the materials, requiring a degree of finesse in presentation.
- The set of this knowledge is not static, in fact it is advancing rapidly - therefore the methods of development and publication must support rather frequent publication.
- While certification program is an eventual goal, it is more important to ship than to take the time to develop associated questions for certification
- Progress
    - Completed
        - Construct and perform a membership survey to guide BoK efforts
        - Define potential approaches to establishing a BoK, including high-level staffing and funding estimates
    - In Progress
        - Deliver plan with specific milestones, tasks and resource levels needed for selected approach
        - Acquire staff and volunteers as well as and organize work for the selected approach
    - Not started
        - Define potential approaches to establishing a certification program, including high-level staffing and funding estimates

Final thoughts

- ABC -> Always Be Collaborating
- Get Involved!
- Join us at https://idpro.org/join

The Orgbook: Watch Us Create A Concept Map!

Day/Session: Thursday 3G
Convener: John Jordan, Stephen Curran, & Andrew Hughes
Notes-taker(s): (1) Andrew Hughes (Concept Map), (2) Stephen Curran

Tags for the session - technology discussed/ideas considered:

#theorgbook, #government, #conceptmap, #verfiablecredentials

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

(1) Notes from Andrew Hughes:

Andrew created a new concept map as John and Stephen talked about The OrgBook –

The concept map can be found at: https://kumu.io/andrewhughes3000/theorgbook#first-map

(2) Notes from Stephen Curran:

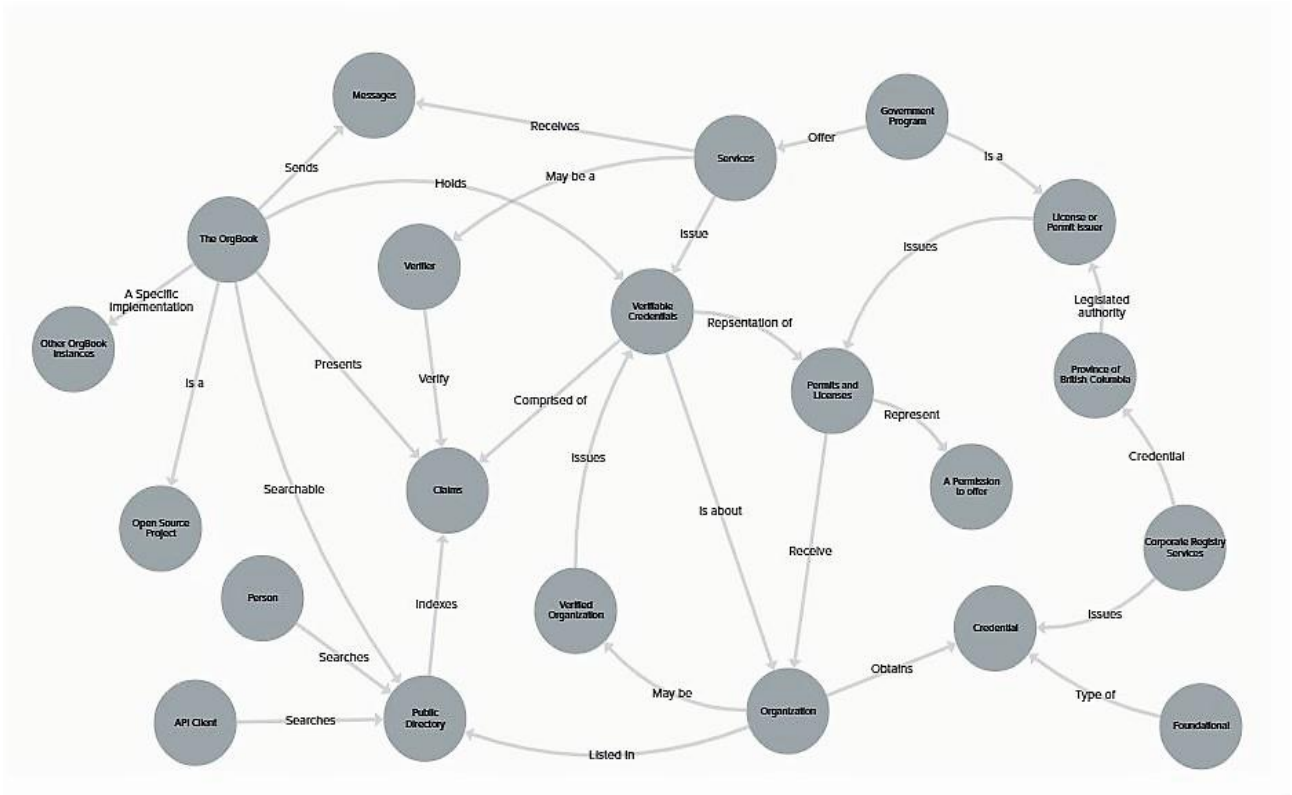
The session had three goals:

- To learn about Concept Maps - what they are and how they can be used
- To learn how to facilitate building a Concept Map
- To learn about the components of TheOrgBook - described in earlier IIW sessions: Tues 3A, Wed. 4F

We started from a blank canvas at https://kumu.io. Andrew Hughes provided background information about Concept Maps (see this site for more information), and some guidelines for carrying out the creation process (including, it seems, not to use the word "disambiguate"). The basic parts of a Concept Map are circles representing concepts and lines connecting the circles, representing relationships. A concept map is read by forming sentences using two circles and the line connecting them, ending with the circle pointed to be an arrow. Do not try to form extended sentences involving additional lines and circles.
Andrew has successfully helped the community create a couple of key concept maps using proposed W3C specifications about:

- Decentralized Identifiers (DIDs) - https://kumu.io/andrewhughes3000/rwot#decentralized-identifiers
- Verifiable Credentials - https://kumu.io/andrewhughes3000/rwot#credentials-concepts

Coming into the session, John and Stephen thought that the map would not be too big - maybe a handful of circles, and some line connections. During the session, we created this map (live and pictured below).



Ask A Millennial About Identity

Day/Session: Thursday 3K
Convener: Samantha Windley
Notes-taker(s): Samantha Windley

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

In this session we discussed different ways that millennials trade their data for service and what things they are willing and unwilling to give away when it comes to their online persona.

Social media platforms, such as instagram and Facebook, were brought up as a way to sign into things, and Sammi said that she uses her Facebook account as a "throw away" way to sign into different apps and services. Her phone number, on the other hand, is something that she is worried about using to sign up for apps and other services.

Millennials tend to keep their social identity separate from their identity they use for their bank account, etc. In consequence they are more willing to trade their social identities and information for services an app provides.

The question "what would it take for you to no longer trust a service?" — If the company does nothing to fix a hack and if the hack then compromised some of the person's personal identity, not just the social identity.

For millennials, time and information is no longer chronological— Instagram feeds, google searches, etc. are based on what the user has liked in the past, or what is most popular.

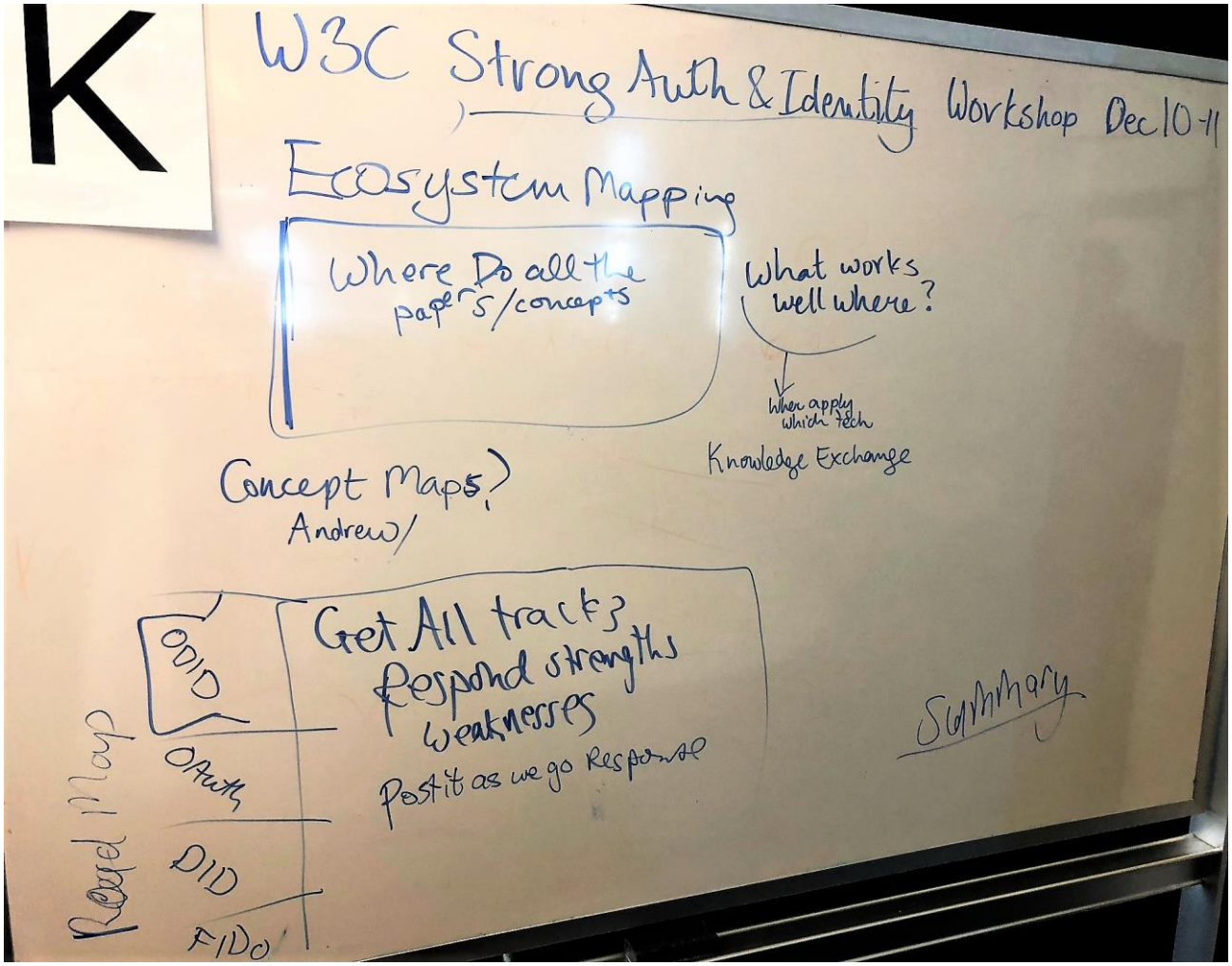
AI was discussed, and while Sammi viewed the email suggestions gmail gives you at the bottom of an email as creepy, the fact that instagram curates ads for her based on things that she has liked in the past didn't— more of a "Hey girl this is awesome, and I think you would like it!" AI approach vs. the "helpful assistant AI.

Social media fast— decided to change the content she was consuming to something uplifting and helpful instead of time wasting. Resulted in her being happier and empowered.

W3C Strong Auth & Identity Workshop Dec 10-11 - Ideas + Designs of Workshop

Day/Session: Thursday 3K
Convener: Kaliya Young
Notes-taker(s): Kaliya Young

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



Research & Education (R&E) Identity – Where Do We Go Next?

Day/Session: Thursday 4B
Convener: Nick Roy
Notes-taker(s): Nick Roy

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

Link to slides presented by Nick Roy:
https://docs.google.com/presentation/d/11RHFbaE60ngYwLOz0A_FwCs0zuUl5bLPwwMouEO8kUE/edit?usp=sharing

LifeScope Demo & AMA

Day/Session: Thursday 4C
Convener: Liam Broza
Notes-taker(s): Liam Broza

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

Our core focus was on showing how LifeScope and BitScoop solve core identity issues.

BitScoop allows for abstraction of auth models for APIs and general software development.

LifeScope simplifies identity with personal information wallets that deeply model an individual.

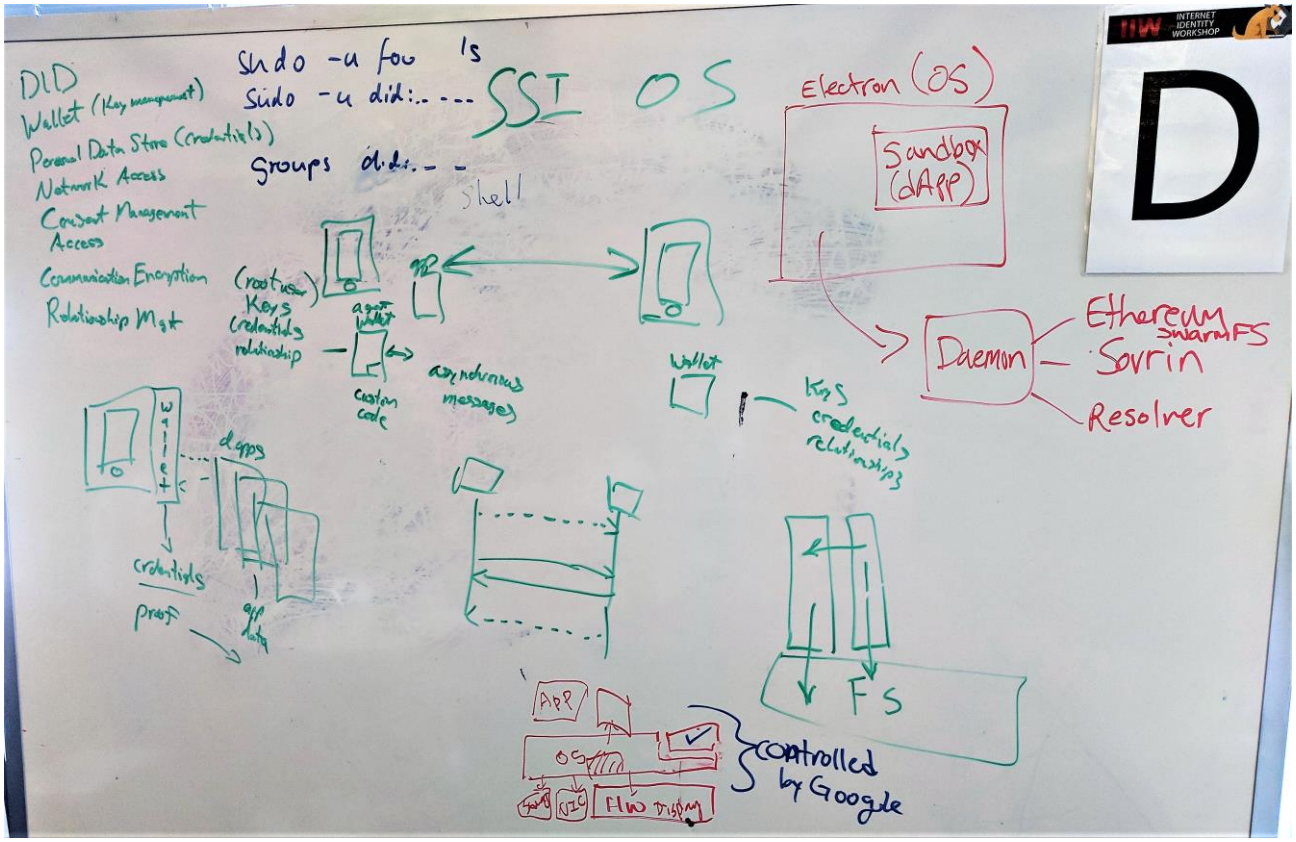
We talked about the advantages of these approaches compared to others and where we plan expand our capability.

Link to Liam's pdf files and notes for this session:
https://www.dropbox.com/sh/mcgvckstxaatnuf/AACYJ0LLR_86IOwtzlsFs2U0a?dl=0

Defining the SSI OS

Day/Session: Thursday 4D
Convener: Matthew Hailstone
Notes-taker(s): Matthew Hailston

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



The Great Dalmuti: What We Should Consider About Identity as Learned from a Card Game (+ Singing Time!)

Day/Session: Thursday 4F
Convener: Jacob Siebach
Notes-taker(s): Jacob Siebach (with video from Phil Windley)

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

We began by learning the rules to The Great Dalmuti, an enjoyable card game by Richard Garfield, before discussing the significance in identity.

The Great Dalmuti requires at least four players, who are each given a rank and seated in ranking order. All cards in the deck are dealt to players. The first person to successfully play all of their cards will gain the top-most rank for the next round, and the next person will be in the second position, and so forth. Thus, the titles and position of the players may change every round.

As far as Identity is concerned, the *identity* of each player does not change during the game, but their *position* and *title* do. This is much like a person elected to an office; after a time they may not be in that office anymore. The discussion resulted with the idea that the person should still retain their wallet and credentials for their personal affairs, but there should be a **fully separate and transferable agent**, with its own credentials for the job, which can be transferred from one representative to the next by some authority.

Singing time!!
Phil posted a link to the video that he took of this: https://vimeo.com/298206648

When Standards Don't Suffice

Day/Session: Thursday 4G
Convener: George Fletcher
Notes-taker(s): George Fletcher

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

George's link to the slide deck he used for this conversation:

https://www.slideshare.net/Identiverse/625-when-standards-dont-suffice-identiverse-2018-4-views-0-0-share

How Data Analytics Will Change Thanks to SSI

Day/Session: Thursday 5B
Convener: Matt Norton & Chris Matichuk
Notes-taker(s): Alec Laws

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

Huge part of the corp world, generating value for them
- analytics
- data science
- big data

What does this look like when consumers own their data?

context comfortables, people still use demographics. instead of 'how willing'/comfortable people are to share data?
- what notif
- what to share/send them

people more comfortable sharing data if they what value data provides to business

why would you sign in with FB but not instagram? why can some companies share data

Hypothesis: analytics transforms so that company is more transparent about value data providers & benefit the consumer at the moment (in context)

ocean protocol, silo'd data for analytics (not ssi compliance)
overlays, data capture schema generic across trusted framework. different overlay on scheme
- overlays are strong for SSI
- but ocean is ready to go

Q. they do same thing, or complementary?
- compl. needs convo between sovrin/ssi id and ocean

- a lot of PI companies, will give money/token for data
- does NOT like this, so like money that time thorght about risks makes it irrelevant
- avoid this discussion completely "it's a dumb idea"
- want to figure out value that costs person the least, but highest value to business
- a lot of agreement here

SSI is about giving power back to user
- data is held by company to deliver value
- if you hold yourself, you have the full view
take the data and make it make sense to the user
- understand (really) what they share, and what value they get

Q. what if i dont have access to data in enough quality to make a decision?
- can't build a model (statistically relevant)
- must reat as research project, different that what eula that was agreed too

- not using for eula purpose
- can't get data to build model and solve problem (in reasonable amount of time)

airline/airport/it
- can't imagine when data purpose isn't explicitly stated
- SSI difference, db/system is internal, collected, mined. but not shared with partners (hotel/car) providers
  - without being explicit about opt in to the user
  - no more profile db with all info

gpdr exists everywhere
- same as PII (in CA/US/etc)

what is the use case in the moment?

ocean/oerlays are tech solutions, what about FB data?
- shift in economic incentive
- ie decentralized FB
- why does the user signup (research trial)

"jobs to be done", hire company to accomplish a job
what am I hiring a data collector to do? just for one research model
- or are you a trust broker to downstream systems?
- do i trust you to share

Once data is collected/owned by user
- WIlling to give company data and let them help you discover services?

clinical trial ->FDA requires data to be held for 10 years
- locker mechanism before it's pushed out decentralized
- if data collected proper way, it may automatically pushed to public data store
overlay essential to do that

are we away from monetizing data as a bad thing?
gdpr didn not appear because we dont share data. we want to share data
- enables services, personal, usable in life
- therefore we acccept tos/eula etc

6000/50 person models
- statistics vs marketing

PII not all useful, labels/categories are
- want to know as many labels as possible

criteria search on hypothetical global data store
-> do you want to appear in the results?
-> yes -> pushed to result
-> no -> removed from the set
ie google pays for 3M result set
smaller costs less
maybe every 'observation' costs a fixed value

pay premium for more PII associated with labels
- ex when did you default on the loan
- pay more for PII associated

depends if consumer consents to how that data is used?
- if data is anonymized?
- you should never get name/address/PIIs

keep schema very basic, 'entry overlay' with prepopulated anon values
- everything else is free form
- PII auto encrypted, but associated with features
- if no overlay, same as PII

are we talking about buying data from orgs that collect data in SSI? that is ocean
- vs new model with SSI

SSI is about presenting credentials?
distributed trusted framework is good at identity, but broader thorugh trusted relationships
idea that id is base of credential, this is problem with id space
- identity is based on what we do (with some certifying authorities)
- real id is who all of these data points

part of service layers is decentralized compute
- same problems because other computers use your infor
- does this leak
-> homorphic encryption

clinical trials, you have relationship with study, pairwise with study
- you can't participate in multiple trials once you start
- but data starts by going into each trials 'locker'

lose transparency without reputation
- can tell who issued, but not how 'good/bad' they are
- tech gives proof data came from source, nothing to do with trust
this is the trust framework on top of digital tech

rwot, p2p degrees of trust
- missing from math modeal, subjectivity of model
- you capture trust at a time
- address is hard to prove due to conflicting data points
  - increase trust when by having something to lose (life/money/rep)
  - some actors are inherently altruistic(but it's a minority)
  - most poepl are neutral (good or bad)
  - what is correct incentive (is this what trust is?)
- adding math doesn't solve problem with stake

the relationship/rep of person you are interacting with is essential to how org uses/shars the data
- as an issuer you must prove worth
  - this is implicity (common sense), but hard to capture in tech
  - how to show that entity can be trusted

how can individual/community affect rep of entity?
- ex yelp
- solved by broker between parties?

value for data is the important piece. but doesn't need to be monetary

how does mutual contractual protection help?
- rep is important/subjective/complicated

in healthcare, they care about bottom line, drugs on shelves
- only hold data because of regulator (FDA)
- don't want the data at all
- but they have a central id system (pims)
  - change it there, not at big pharma

with SSI, decay of companies who make money by selling their data
- Credit bureau needs to go, or need to be redefined?
  - scraping info without consent is wrong
  - they enable commerce (loans, etc)
  - companies need to evolve

if data only used for credit score, that's fine
- but data has been exposed
- need better way, but not to go away

if we are for this, someone will be against it

SSI will change everything, don't think it will
- still need to give info to do business
- data shared removes anonymity

need to be able prove ownership of data to user? ex ccnumber/cvc/exp. not nessecarily

don't need tech perfection. lets be more pragmatic
- identity is about correlation, let user own it
- but must be usable
- correlation must be wanted and known by user
- possession vs knowledge based auth
  - possession + knowledge
  - must participate in transaction (authenticate)

more expensive correlation is, harder to establish rep
- need artifacts to base rep on

under SSI, data only doesn't prove anything. need credential + proof

cc, printed private key on public card
online, do you know email address?
SSI moves it back to a real secret

LifeScope Demo & AMA (Continued)

Day/Session: Thursday 5C
Convener: Liam Broza
Notes-taker(s): Liam Broza & Samantha Chase

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

(1) Notes from Liam:
Our core focus was on showing how LifeScope and BitScoop solve core identity issues.

BitScoop allows for abstraction of auth models for APIs and general software development.

LifeScope simplifies identity with personal information wallets that deeply model an individual.

We talked about the advantages of these approaches compared to others and where we plan expand our capability.

Link to Liam's pdf files and notes for this session:
https://www.dropbox.com/sh/mcgvckstxaatnuf/AACYJ0LLR_86IOwtzlsFs2U0a?dl=0

(2) Notes from Sam Chase:

Link to Sam's pdf files and notes for this part 2 session:
https://drive.google.com/file/d/1FcGNgXsl_98_pcFGCZBlhOvtx51y5hB0/view?usp=sharing

The session was defining the best practices PII wallet or personal data server. Objective was to bring together everyone in data wallet, personal server/personal AI space to create standards body and alliance/working group. All interested please email samantha@venn.agency

Vegan, Atheist, Crossfitter: Which Do You Mention First?

Day/Session: Thursday 5F
Convener: Justin Richer
Notes-taker(s): Aaron Parecki

Tags for the session – technology discussed/ideas considered: Identity, privacy, groups

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

In the real world, our memberships in groups come up in conversation even without prompting.

Jacob: (shouts letters and numbers)
aaronpk: replies with letters and numbers

Justin: I don't know what just happened there.

they both just shared their amateur radio call signs.

With our digital identity systems, we don't have a way to signal this membership.

Could we or should we? Do we want to?

There have been many attempts in the past about building explicit personas. When I go to your website I can see things. The real world doesn't work like that.

We walk in to a room with a primary persona we're projecting, but we can give signals hinting at memberships without explicitly giving it away.

Alan: Can DIDs solve this by slowly building up an identity?

No, because that's an explicit declaration, not hinting or sending subtle invisible signals. Those links are irrevocable.

Group privacy - I may be comfortable saying something about myself, but others may not want to share that they have that thing in common.

Problem with existing digital systems is for example you're in a facebook group or you're not. Everyone else can see you're in that group.

George: these tensions exist in real life. If there's a big group of people, I might know two of the people and be able to ask them questions without revealing to the larger group that I am a member.

Justin: A session from last IIW, when someone joins an online group, everyone else knows and now has to vet. Exercise: 5 people in the room, close your eyes. Everyone who has accepted money from the federal government raise your hand. Now put your hands down. Open your eyes. Now everyone who didn't raise your hand has to leave. Then when someone new walked into the room, had to do the exercise again.

Jeff: correlating data - two-factor authentication and stuff can hide data for a while. how do you keep privacy hidden?

Justin: the argument against my stance is sure you can do correlations but why make it easy?

George: is the need or expectation around personas generational? for me, I created a bunch of accounts and a separate email for photography stuff. created around a different persona. the vast majority of that is in its own space. I have one email for standards stuff.

Justin: George takes amazing photos. most people don't know that.

Alan: george did a slight reveal, and you completed outed him.

Justin: exactly. George said "I've got this photograph thing". That could mean any number of things. But truth is he takes these very beautiful photos, and I've added that bit of information. I am also a musician, I have 6 albums out, and a lot of people who I deal with on a day to day basis don't know

that. It doesn't tend to come up in my professional circumstances, and it's something I do try to keep separate. some of us are more blatant about sharing our musical inclinations. we can very easily in the course of human communication do things like belting out an opera to dropping hints about music.

Jacob: we keep saying how do we technologically do this? but it's a human thing. do we need a technical thing to solve this? if we have a way to communicate as humans we can do this online.

Justin: I am not a security nerd. The reason i'm in security is my background is in collaboration systems. The point of a collaboration system is to facilitate human communication. You can't do those kind of things effectively unless you keep security and privacy in mind. So does the technology matter? I would say yes but from the capability and functionality standpoint. We have this interesting hack that people do to explicitly separate these things. People use different email addresses. I have different websites for my music stuff and business stuff and (when it was online) my personal web page. Another example, reddit, an important feature is that it's almost instantaneous to create a new account. It has a tradition of throwaway accounts, people create an account to participate in a conversation pseudonymously. These are all hacks on top of systems. I have a main reddit account, which has a lot of reputation, but I don't use that to make controversial statements, or associate with groups I don't want to be seen as participating with.

Alan: back to the photography thing, this was an incremental reveal.

Justin: I know someone who has two different photography personas, one that takes graduation photos and one that does more risqué photos. He ultimately has his name on both, but there are no direct links between the two.

Justin: what i'm getting at, is could we or should we build systems that I can attach these hints to without explicitly attaching things to my account.

Justin: signaling group memberships. I was able to choose what I wear today when I got dressed. It's harder to do that online by curating your facebook profile before you go join a group.

?: Telegram has a mechanism like this. When you view someone's profile you see which groups you're in that you have in common with them.

Jeff: there are some number of aspects of people that are facts that they might be willing to put down in a profile

Justin: I think you'll find there are a lot of people who have some of these things that they may choose to protect instead.

How can someone signal that they are a member of a group to someone they are interacting with without explicitly reveal it?

Being able to drop a piece of jargon into an otherwise innocuous sentence. Relying on the other person to recognize that it may not be a thing they can acknowledge in public right away.

Something that is fine for you may be detrimental for someone else.

You're always taking a risk by trying to make a connection.

Justin: there is potentially some technology that could help people do this more safely. the tools we have for people to do this today are very coarse. make a new account and hope nobody can correlate them later.

George: the takeaway is we should have less online communication and more in person communication and the world would be a better place.

Justin: you're not wrong, but... The rules are different.

?: the telephone. there's a difference between the telephone and using skype. I don't expect the telephone will remember the conversation, whereas on skype, the chances of it being recorded on skype are a lot higher.

Defining SSI Layers

Thursday 5H
Convener: Oliver Terbu
Notes-taker(s): Oliver Terbu

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

Motivation
The intended goal of this document is to outline the different layers of compatibility that have been discovered which could break **interoperability** and eventually **portability** of self sovereign identities. One of the key concerns that has arisen is that in order to even discuss the differences, we need to first understand the layers of the architecture. It is not certain at this time that this is all layers or areas of concern that need to be addressed. More may be added in the future.

While these layers as being decoupled it is possible that layers may be coupled in order to achieve simplicity, scalability, or usage of other standards. Whatever the reasoning may be, it is possible that a SSI stack can be achieved while coupling these layers. An example of how this may occur is through JWEs. If JWEs were used, they would define the Encoding and Encryption layers by adapting the specification that is already outlined. Additionally, DID method specs could stretch over the DID resolution, DID operations, DID storage, and Anchor layers. This is acceptable assuming that it allows for **interoperability and portability** still.
Discussed proposal (at IIW)
A SSI layers definition was considered to be appropriate and beneficial. The goal was to work collaboratively with the SSI community on a layers definition - bottom-up approach.

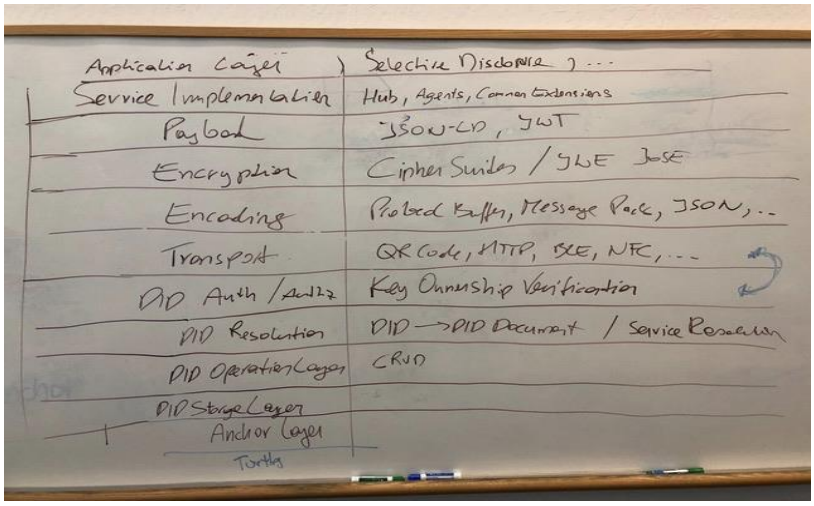
Having a layers definition in place, would allow all players in the SSI world to have more specific discussions, to collaborate more effectively, to work more independently and to leave more room for innovation at particular layers

It will also allow to compare different solutions more easily if it is visible which layers a solution covers.
The first draft was build at IIW in collaboration with members from many SSI communities (Microsoft, uPort, Sovrin, Evernym, HyperLedger Indy, Civic, Jolocom and more). The session was very productive and we came up with a first draft.

We identified 11 layers - see below. We expect these will evolve; we also need to better define the interfaces / optionalities, etc. over the next months.
Next steps: We intend to have further discussions on how to proceed with the SSI layers definition in DIF.

First next steps:
1) Communication / article for broader audience
2) The SSI community will identify which technologies they use on which layers - spreadsheet / slides for everyone to submit.

Please find attached a photo of the whiteboard as well as a nicer digitised version.



Layer Name	**Example**
Application	Selective disclosure, music app, rideshare service, extensions, etc
Implementations	DIF Hubs, Indy Agents, uPort app, etc
Payload structure	JSON-LD, JWT, COSE Web token, etc
Encoding	ProtoBuf, Cap'n Proto, Message Pack, JSON, CBOR, etc
Encryption	Ciphersuites , JWE, etc
DID Authn	Key ownership, verification
Transport	QR Code, HTTP, BLE, NFC, FTP, SMTP, etc
DID Resolution	DID -> DID Doc / Service and Key resolution
DID Operations	CRUD support for a DID Doc
DID Storage Layer	Optional, separate storage of DID metadata - e.g. IPFS
Anchor Layer	Bitcoin, Ethereum, Veres.One, Sovrin, etc.

Demo Hour

IIWXXVI #27 Community Sharing / DEMO LIST
Wednesday Oct. 24, 2018 from 1:30 – 2:30

Thanks to our Demo Hour Sponsor
Wireline

http://iiw.idcommons.net/IIW_27_Demo_Hour

1. **Danube Tech - DID Registration and Resolution:** Markus Sabadello
   URL: https://uniresolver.io/ Now that we have a basic understanding of what DIDs are for, let's take a closer look at how they can be registered and resolved.
2. **Article 26 Backpack™ /**The UC Davis Human Rights Tool for Universal Academic Mobility Keith Watenpaugh,
   URL: https://article26backpack.ucdavis.edu/ Backpack empowers refugees and displaced people to connect with highered and jobs safely, securely and effectively. More than an app, with Backpack's ecosystem refugees can store and share critical academic and employment information as they build narratives of achievement.
3. **Indieauth:** Aaron Parecki
   URL: indieauth.net IndieAuth is a decentralized identity protocol built on top of OAuth 2.0. IndieAuth brings back the original goal of OpenID where every website can be its own identity, and doesn't require apps to pre-register at each authorization server.
4. **Veridium, DID Authentication with Biometrics:** John Callahan
   URL: http://veridiumid.com/ A demonstration of Veridium's IEEE 2410 DID Auth integration using a QR-based challenge scanned by a mobile app. The app is a simple, Heroku-hosted, Ruby-on-Rails app that relies on a Universal Resolver service to resolve the user's DID.
5. **Peercraft / Open Discovery:** Henrik Biering
   URL: https://www.opendiscovery.biz/ OpenDiscovery is a KISS approach to realize scalable decentralized markets for products and services. OpenDiscovery nullifies the trading value of data to the benefit of security, privacy, trust, innovation, competition, and production planning. A simple POC will be demonstrated.
6. **yes® ID scheme (yes.com) :** Torsten Lodderstedt
   URL: http://www.yes.com (German only) yes® introduces a scheme that enables bank customers to use their online banking accounts for conducting various digital transactions, such as login, registration, identification, payment and signing, with Relying Parties. Use of bank-verified KYC data in conjunction with online banking multi-factor authentication allows to address use cases up to eIDAS trust level substantial.
7. **digi.me – current PC/Mac, iOS/Android version application:** Jim Pasquale
   URL: http://digi.me product & http://digi.me/video vision Experience 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, with external apps providing insight from financial data inside their library. Learn about giving data back with a new digi.me feature.
8. **Manifold:** Bruce Conrad
   URL: https://manifold.picolabs.io Manifold is designed to help owners keep track of their things, and information about their things. Each thing is represented by a card in the UI and backed by a pico which stores all of the information. Apps can be dropped into cards. Come see a demonstration and try it out with something of your own. The apps we have now are "Safe & Mine" and "Journal."

9. **HumanOS Level Digital Identity Management :** Jeff Orgel (jeffo@whatisyourrealit.com) Digital Identity is shaped by behavior/choice relationships with IT platforms/systems. Those affects will shape digital identity & presence. Will that digital identity reflect intention? A language, Real-IT, looks to manage & control how that relationship reflects into Reality?

10. **CitizenOne:** Lucas Tetreault
URL: https://www.vivvo.com/citizenone/ Using digital signatures (DID's) as a means to replace username/password entrances allowing the user to enroll themselves to services with digital interactions that broker verifiable claims and consent for in person and back channel verification workflows.

11. **Payfone:** Michelle Wheeler and Aidan Herbert
URL: http://www.payfone.com How can we use consumer choice to drive data privacy forward? Join Payfone for un-conference approach to demoing and designing a universally needed tool.

12. **Jolocom: Kai Wagner URL:** https://jolocom.io Kai will demo the Jolocom SmartWallet, an app based on the Jolocom self-sovereign identity protocol, implementing a range of open standards from DIDs, to Verifiable Credentials. In the Demo, he will show a self-sovereign single sign-on solution.

13. **Minerva User Friendly Digital Wallet:** Robert Mitwicki **URL:** https://lab10.coop Glimpse on new generation of user friendly digital wallet for your identity and assets. In the demo we would present how to use Minerva for single sign-on, second factor authentication and subscription payments in a mobile environment.

14. **UBOSbox:** Johannes Ernst **URL:** https://indiecomputing.com/products/ UBOSbox is a pre-configured home server that enables users to take their personal data home from on-line services such as Dropbox onto hardware they control. Announced recently in Berlin at the Nextcloud conference, it is now shipping.

15. **Videntity: Verify My Identity, an open source Open ID Connect Provider within Django Python:** Alan Viars
URL: https://github.com/transparenthealth/vmi Videntity has teamed with the Alliance for Better Health to create a standards-based information sharing platform. Some of the key features that will be implemented in the coming months include support for FIDO and Identity assurance escalation.

16. **OpenConsent and the OpenConsent Privacy and Security Network:** Sal D'Agostino, Co-Founder **URL:** https://openconsent.com The OpenConsent Privacy and Security Network is built with the vision that privacy and security needs to be usable for people and machines. They need to address the operational requirements of people and companies. We will show how the network, in its first phase, addresses this and in the process reduces risk and increases operational efficiency and the value of brand and personal information.

17. **Duo Mobile and Partner Program Opportunities:** Leya Leydiker
URL: https://duo.com At Duo, we combine security expertise with a user-centered philosophy to provide two-factor authentication, endpoint remediation and secure single sign-on tools for the modern era. Partner with us to connect and collaborate with Duo customers, resellers and developers.

18. **Identity.com Marketplace Transaction:** Martin Riedel
URL: https://Identity.com is an open-source decentralized identity ecosystem that enables access to cost-effective, secure identity verification solutions. We will showcase how Issuers can set prices for identity credentials items and how Subjects can hand out a verified credential that is issued through the marketplace.

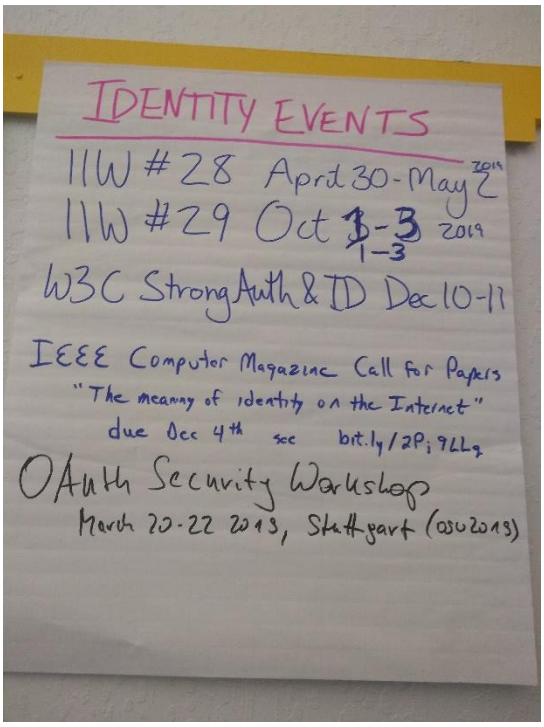
19. **HIE of One Trustee:** Adrian Gropper **URL:** http://hieofone.org Trustee by HIE of One is the first open source and standards-based self-sovereign personal agent. We combine UMA, uPort, and OpenID Connect to show how Verifable Credentials and Self-sovereign identity complement federated identity to create a true patient-centered health record.
20. **MUNINN next-gen intelligent network intrusion detection system (IDS):** Andreas Wehowsky
    URL: https://www.wehowsky.com Just as Muninn, one of Odin's ravens, watched Midgaard and informed Odin about critical events, MUNINN monitors your computer network and detect anomalies using cutting edge machine learning, alerting about cyber threats, espionage, and data breaches immediately.
21. **Secure Device Access: Hannes Tschofenig**
    URL: https://www.arm.com/products/iot/pelion-iot-platform Secure device access (SDA) enables device owners to give users who may belong to a different organization, such as service technicians, access to Internet of Things devices. Under the hood SDA uses the OAuth-ACE work.
22. **Province of British Columbia – Live Public Beta of TheOrgBook:** John Jordan, Stephen Curran
    URL: https://theorgbook.pathfinder.gov.bc.ca/ https://von.pathfinder.gov.bc.ca See the Province of British Columbia's first Hyperledger Indy production service called TheOrgBook. TheOrgBook is a cornerstone of the Verifiable Organizations Network (VON) which enables organizations to exchange data in trustworthy ways based on open standards and technology.
23. **Making App to App Identity Verification Seamless: JP Bedoya**
    URL: https://Civic.com Civic is a digital identity company, giving people the tools to control and protect their personal data. With our new app-to-app integration, any app that supports Civic Connect will be able to utilize Civic identity verification solutions, eliminating the need for a username/password while providing additional security.
24. **HiveMined demoing the new DMARC-enabled mobile endpoint app "Skeptify":** Mark Rees-Andersen
    URL: Danish only for now https://www.stopsvindel.nu Identity-based mobile security - Secure icons on every DMARC-secured inbound email and SMS, in the default email app (pat.pen). Full-screen inbound warnings against known fraudulent/spam callers. Security analysis of any text message, submitted via screenshot.

The IIWXXVII Demo List can also be found here http://iiw.idcommons.net/IIW_27_Demo_Hour

IIWXXVII #27 Photos

Check out Doc's FABULOUS photos of IIW 27 @dsearls

Day 1:
<https://www.flickr.com/photos/docsearls/albums/72157675199001098>
Day 2:
<https://www.flickr.com/photos/docsearls/albums/72157703398031255>
Day 3:
<https://www.flickr.com/photos/docsearls/albums/72157673408031037>



See you
April 30 -May 1 & 2 2017

for

IIWXXVIII

The 28th Internet Identity Workshop

REGISTER HERE
https://iiw28.eventbrite.com

www.InternetIdentityWorkshop.com