IIWXXIV

INTERNET IDENTITY WORKSHOP 24

Book of Proceedings

www.internetidentityworkshop.com

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

Notes in this book can also be found online at
http://iiw.idcommons.net/IIW_24_Notes

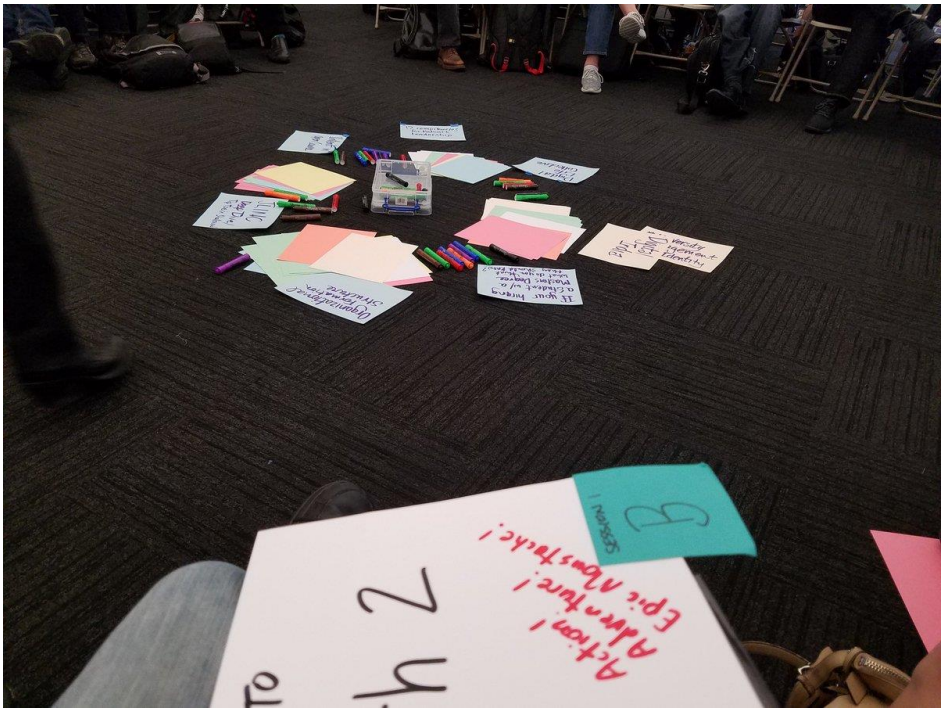


Photo credit #IIW @Justin
Getting started at #iiw ... We are agenda-fluid.

May 2, 3 & 4 2017
Computer History Museum ~ Mountain View, CA

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

Photo Credit @WayneVaughan
Getting started at the Internet Identity Workshop #IIW

Contents

Photo Credit @windley
Full House at #IIW Opening

About IIW

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

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

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

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

The event is now in its 13th year and is Co-produced by Kaliya Hamlin, Phil Windley and Heidi Nobantu Saul. IIWXXV (#25) will be October 17 - 19, 2017 in Mountain View, California at the Computer History Museum.

IIWXXIV Sponsors

Photo Credit @cirrusIdentity Great diversity of companies working on Identity Management and Sponsoring #iiw. Proud to be among them!

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

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

Upcoming IIW Events in Mountain View California

IIWXXV #25 Oct 17, 18 & 19, 2017

IIWXXVI #26 May 1, 2 & 3, 2018

What Inspires YOU to come to IIW?

At the opening of IIW XXIV we asked new and returning attendees to reflect on and record their main inspiration for attending. Here are the transcribed notes from those who shared their thoughts.

New Attendee Inspiration to be at IIW

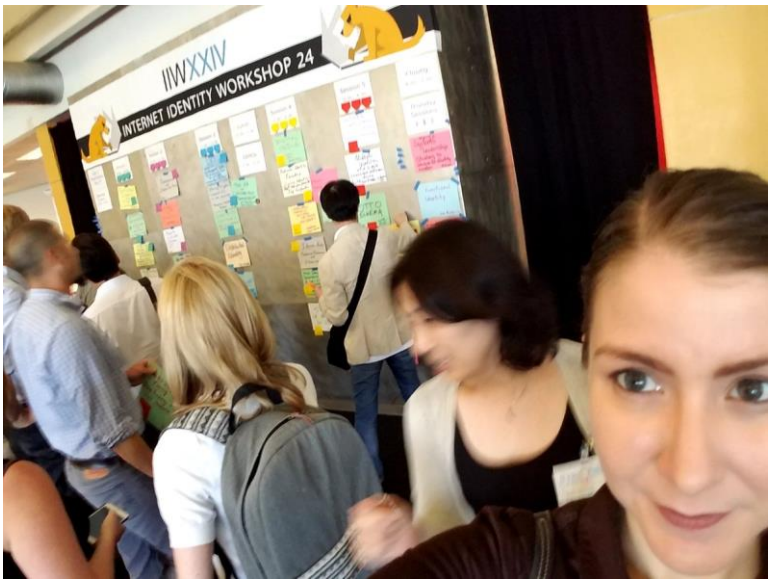
- I was inspired to come here by the advances made in usable cryptography (eg. blockchain, OIDC tokens, etc) and how these can converged to provide strongly-signed, encrypted identity that can be used by those with limited technical familiarity.
- Searching for the future of identity and identity management
- Inspiration to come, Doc Searls, Intuition and Identity Experience
- Understanding the latest technologies are around identity and authentication. Getting feedback on the authentication solution I've been building at Trusphere and understanding how it fits with identity technology.

Inspirations from Returning IIW Community Members

- Self-Sovereign Identity x2
- Exchange of credentials and attestations between silos using a distributed trust model.
- The rubber is hitting the road! Real implementations for real user are generating new and interesting questions
- Connecting ALL the nodes
- UMA move from authentication to authorization
- What are the costs vs. consent "balance of trade"?
- I'd like to get feedback on pre-auth entity trust (POET)
- To help think through identity in health care
    - What are the costs of mis-managed identities?
    - What are the ways to manage identity and create online?
    - What are the pros/cons?
    - What are the known problems with those techniques?
    - How do you instigate individuals to manage-proactively their identity?
- Meet really smart people with the same goals
- OTTO Federation management for OpenID Connect, SAML and extensions for other protocol and required promo. GDPR and US companies complying
- As a person building on decentralized networks like blockchains, I have found myself needing to find ways of representing identity in an environment with no central authority and I'm wrestling with those implications
- User Consent
- GDPR, Consent Receipt, EU Regulations, Safe-Harbor Act, 1994-Cookies
- I see progress - very slow - AWA from both "user" and "centric" but toward what? sovereignty

- Most Inspiring: blockchain based decentralized identity
- Next step in the evolving definition of ideals of enlightenment (self-sovereignty)
- Wise contracts - machine readable and better human readable (common as air)
- Better angels of our nature. Three years head down keeps the lights on and trying to stabilize. Time to catch up. Angels + agents - inspired by the promise of not being handcuffed by FERPA
- Personal API Phil - clue train manifesto and intention economy
- Data Privacy
- True Self-Sovereign Identity Inspires me. Key management will be one of the hardest things to solve in a truly self-Sovereign world.
- I believe that distributed self-sovereign identity can enable agents with the power to raise people to first-class citizens in an API world.
- Distributed Peer-to-Peer Technologies
- Want to catch up on distributed identity - hear what others are doing in the space
- Renewed interest in PKI and Web of Trust style systems
- The recognition and interest from established industry leaders that didn't exist in the past
- Users being in control of their digital destiny
- Having on non centric strategy when "creating" and identity and be the owner of this identity and manage privacy/confidentiality
- I'm inspired by the possibilities around allowing user to "login" to devices that they never would have thought to before, and have those devices then off customized experiences to the user.
- Widespread user of Mastodons
- Awareness that Digital Identity is merely one tool to help people and society manage Identity
- Identity and trust are key to what is next in innovation. Creating a global identity construct that opens opportunity for all is what inspires me about IIW
- The increase in self-assertion and individual capability to make statements about their identity and control how it is consumed.
- Looking to network with identity professionals to learn from them. Goal: in time contribute (give back) to the identity community
- Most Inspiring User Owned Identity taking back control
- Live ID proofing and user enabled access without giving up any additional PII. Beyond KBA, Biometrics and security.

IIW 24 Session Topics / Agenda Creation



Sarah Squire @SarahKSquire May 3
The beautiful chaos that is the internet identity workshop #iiw

Tuesday May 2

Session 1

1A/ Self Sovereign Identity Container
1B/ Introduction to OAuth2
1D/ Decentralized Names and ID's Working Group – DID101
1E/ IDPro
1G/ Joram v1.0 bit.ly/joram100
1H/ OIDF Modrna WG UpDate
1J/ 12 Competencies for Network Leadership
1K/ Digital Inclusion

Session 2
2A/ Digital India
2B/ Introduction to OpenID Connect
2D/ Decentralized Names and ID's (continued)
2F/ JLINC Overview Demo Discussion
2G/ Delegated Account Recovery – Kill the "forgot password" email
2H/ Build Badass Identity Team
2I/ Consent-Informed Attribute Release for SAML/OIDC at Scale

Session 3
3A/ Privacy Preservation and Controlling Correlation
3B/ 101 Introduction to User Managed Access (UMA) 2.0
3C/ IEEE 2410 Biometric Open Protocol Standard ("BOPS") EXPLAINED!
3D/ If You're Hiring a Student w/a Masters in IDM – What do you think they should know?
3F/ Your Terms that Sites Agree To (rather than the other way around)
3G/ OpenID Connect Account Parking Overview
3H/ Hybrid Personal Cloud – Applying devops open source tech to personal IoT
3J/ Identity Storage and Compute Working Group

Session 4
4A/ Intro to Fast Fed (new passport standard)
4B/ 101 MFA, 2FA, FIDO
4C/ Intent in Open Source
4D/ 10_Foot Platforms – Device Pairing
4E/ AI DAO's & ID
4F/ JLINO Deep Dive – Tip Toe in Shallow End
4G/ End-to-End Crypto SDK for Deve
4H/ Picos Everywhere
4J/ Identity Storage and Compute (contained)

Session 5
5A/ Token Binding – Proof-of-Possession for cookies, ID Tokens JWt's & OAuth Tokens
5B/ Blockchain 101
5C/ Why isn't IIW Wiki Secure?
5D/ HashO: IO Protocol – Web of Trust + Blockchain + Proof of Work + IPFS
5F/ Intro to Sovrin
5G/ Intuition, Identity, Internet
5H/ Beyond OAuth2: End-to-End Microservice Security

Wednesday May 3

Session 1
1A/ DID 101 – Decentralized Identifiers & how they are the key to interoperable self-sovereign ID
1C/ IEEEE/SA, Evernym, iRespond, SWIRLS – ADV The Human STD Hackathon (100K Refugee Framework)
1G/ Fair Dice Roll's in On-Line Game's using Blockchains
1I/ Application Identity and Trust in Healthcare and beyond

Session 2
2A/ How to Live with Shadow IT
2C/ Neural Science of Persuasion
2G/ Attestations and Identity Data Formats
2H/ ID PRO Body of Knowledge & Taxonomy
2J/ Intro to Verifiable Claims by W3C VCWG Members
2K/ Public vs Private Data – What can we share?

Session 3
3A/ DKMS = Decentralized Key Management System
3C/ What is it like to be part of a working group?
3G/ Storing Crypto Credentials
3H/ The UX of Secure Key Management Trust Frameworks
3I/ DID TLS
3J/ OTTO Schema
3K/Distributed Identity

Session 4
4A/ Digital India II (part 2)
4B/ Libsovrin Hacking – Zero Knowledge Proofs Selective Disclosure and Predicate Proofs
4C/ 5 Types of Privacy on DLT
4D/ End-User Identity Paradox "Curing Identity" – Don't lose your phone #

4F/ Using Sovrin for Decentralized Student Profiles – A Proof of Concept
4G/ Identity Hubs Technical Resolutions and Planning
4H/ Correlation Marketing Solicitation (not criminal) and Identity
4I/ Trust Frameworks!

Session 5
5A/ Levels of Assurance
5B/ DID Auth (Interoperable auth'n w/DID's)
5C/ "Blockchain Roadmap for Austria" Building self-sovereign identity into a country? & Reinventing National Identifier Systems using DIDs, DDOs & ZPSs, CL Proofs, etc…
5F/ Multiple Useres (IDs) of a Single Consumer Electronics Device (e.g. TV) How to make it happen
5G/ Making OAuth2 Secure
5H/ Certified Self-Sovereign Signature (An e-prescribing example)
5J/ How do People Manage Identities? Prelim findings from user research in India

Thursday May 4

Session 1
1A/ DID Service Discovery
1C/ "Verifier Impersonation Resistance"
1F/ Functional Identity
1G/ "It's a Pain In The Ass, But it's Well Supported" (FIdM)

Session 2
2C/ Privacy – Preserving Geo Location & Other "mystuff" Services
2F/ SovrinID Card – What should it do?
2G/ Pop-Up Enterprise
2H/ OTTO –Ifying – FAST-FED?

Session 3
3A/ Digital Life Collective Cooperative "The Web we want" – Getting to Actual Effects with Identity
3F/ Usability for Identity Management
3G/ PICO's in Practive
3J/Agents for I.O.T.

Session 4
4A/Reputation vs Identity – Definition Perspectives
4F/ Make XDI GREAT again!
4G/ Anonymous Claims Authentication
4H/ Sharing a Systems Leadership Strategy to Catalyze an Identity Ecosystem

Session 5
5A/NO RAGERETS
5F/Come Talk About All The Account Recovery Systems
5G/OAuth JAR Working Session
5H/ Will Nationalism – Populism – Isolationism kill identity Fed attribute exchange? How do we prevent the reification of Statism in next gen ID systems & thought
5J/ Personal API

Tuesday May 2

Self Sovereign Identity Container

Tuesday 1A
Convener: Sam & Adrian
Notes-taker(s): Maryann Hondo, Dan Finley

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

Sam---- idea behind decentralized identifiers (see spec) DID –rebooting web of trust (seeded ---- https://github.com/WebOfTrustInfo/rebooting-the-web-of-trust-fall2016/blob/master/did-spec-wd03.md)

DID--String that can identify a record on a blockchain
What should be in an identity container?

An Identity Container Contains:
1. public key to show proof -- this shows I have control of the DID
2. Service pointers ---anchored to the chain but not in the chain
3. Attributes (issues for correlation)
    a. Self asserted
    b. Verifiable

Follow the service pointer to get to an identity container (agent, hub are terms that are also sometimes used)

how do you manage tokens that control resources ? How to do this in a self sovereign way ---

UMA concerns itself with issuance of access tokens ---Background --- Self Sovereign
(UMA for healthcare background)

[Audience discussion]

DID ----Identity that I own ---
Confusion on the scope of the web…..
Lots of discussion on what is "verifiable"
In effect FIDO can address this problem

Is this a discovery mechanism?
Format of the identity container is what is in scope.

This is a self sovereign identifier not an "identity".
- An identifier that you own and use to establish permanent connections --- no one else can revoke your identifier
- Definition of self sovereign – no privacy policy needed ---- you have it under your control

This Session focus is on claim (other aspects will be discussed in other groups today):

On chain (DID) and Off chain (self sovereign identity container)

Identity container can contain an authorization service link --- this service could then (under policy from UMA) gain access to the specific resource

What is the "container"? only data? With restful api? Some look like api's (standard in interface that is implemented in different software)

Some suggestions:

- Policies/private keys
- Machine learning
- Authz server
- Secure elements
- Public attributes

Other definitions for the "identity container" scope -----

- Hub --- data only
- Agent --- code/data

Binding process of using verifiable keys is part of the yet undefined trust ---- what the relying parties require is another aspect of the problem space

An example:

- Licensed practitioner is a self signed entity
- Patient is a self signed entity
- 3rd party would be enabled to accept the self signed trust

Another way to look at it …..re-orienting the federation problem to bootstrap an alternative trust model for user centricity

If this binds the user, how can you change the record if something changes?

- Typically the chain (that is the anchor) has a mechanism to accept a new version of the record
- The default resolution returns the most recent record --- since "most" chains are write permissioned --- open read--- you can authenticate the chain of records …

Suggestion from the audience ----there is previous work to be leveraged---Bacnet/Zigby application profiles

Goal is to elevate people to be first level in API use

BYU is doing domain of one's own. When they graduate it is something you take with you.

In the EU they have GDPR and PFD2
See Phil's session on Self Signed

Additional notes by Dan Finlay
Data spec: https://github.com/WebOfTrustInfo/rebooting-the-web-of-trust-fall2016/blob/master/final-documents/did-implementer-draft-10.pdf

All quotations below are general summaries.

An identity container has a series of attributes, added permanently as part of the blockchain.
You can own many identity containers.

Resource servers publish claims in support of a container's attributes.
By creating new containers freely, you can resist correlation, albeit not fully prevent it.

It may be less confusing to call it a self-sovereign identifier, instead of identity.
What you really control is a container with a unique ID that you have personal control over (at least as well as you can manage its permitted keys).
Identity may be a more abstract concept, that is not as technically tangible.

Adrian's definition of self-sovereign:
Something you do not have a privacy policy with. No institution, no CA that certifies you are this thing, it is only your own personal claim.

Since the identity container is on-chain, you should generally only publish attributes to it that you are not concerned about disclosure in the case of key compromise.
Blockchains primarily solve the double-spend problem, so the only thing you definitely need to record on chain are things that need to be tracked over time versus double spend.

DISTINCTION:
Self-sovereign identifier DID lives on chain, and has a public key service pointer.
- This container defines the schema of the identity container.
Identity Container knows attributes that are not recorded on chain. Also known as an agent or hub.
- Policies & private keys: Things that never need to be shared.
- Authorization Server: Personal code & servers that the user runs.
- Machine Learning
- Secure Elements
- Public Attributes: Things you want to broadcast, things that require no auth, identity claims that you want to make public.
- Public APIs: Services for interacting with other containers & sites, big open space.
An external service requests the container to prove something, which can then provide a claim from a 3rd party. The external service can then verify with the 3rd party for further proofs.

In the UMA model, you ask for a pointer to an authorization service from the container.
In some cases, you might trust the container with its own claims (trusting your friends to report their allergies before your dinner party, for example).

If the DMV offers an auth API:
W3C Verifiable claims
If someone asks me for my driver's license, your container returns a DMV-signed claim of your license.

Sam says:
Application Profiles has 20 years of established work doing this same stuff for connecting networks of sensors and actuators. This is all an interoperability and federation problem.
BAC Device Profiles: http://www.bacnetwiki.com/wiki/index.php?title=Device_Profiles
Zigbee Application Profiles: http://www.eetimes.com/document.asp?doc_id=1278223

Examples:
BYU "Domain of One's Own": https://byuoit.atlassian.net/wiki/display/DOO/BYU+Domains+Home

Doc: GDPR's enforcement looming is opening companies up to "pushing liability to the edges" in ways they've never been before.

OAuth 2.0

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

Tags for the session - technology discussed/ideas considered:

OAuth 2.0. What is it? Basic overview. Tokens. API Keys.

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

What is OAuth 2.0?

- Delegation protocol

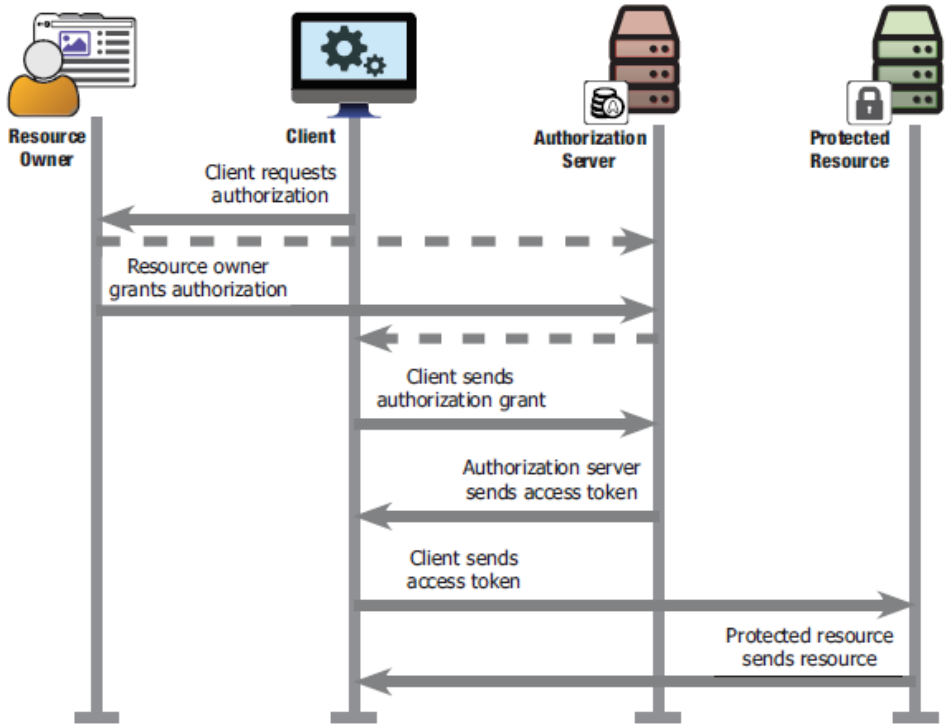


Figure 1.8 The OAuth process, at a high level

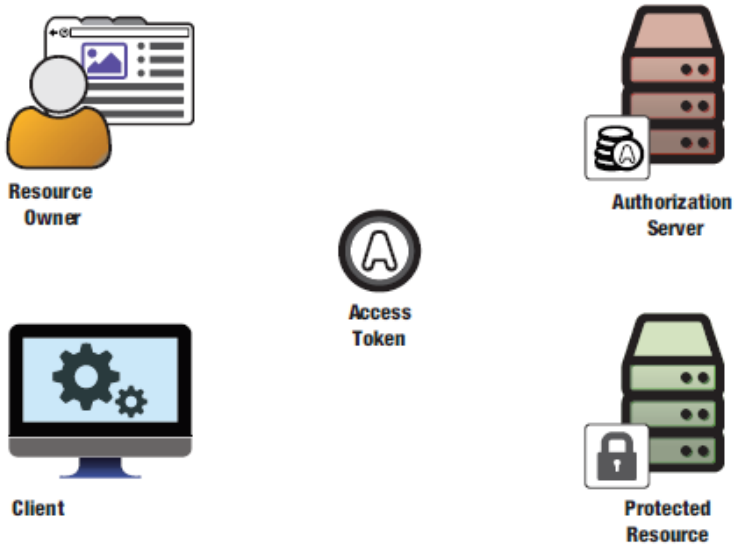


Figure 2.9 Major components of the OAuth 2.0 protocol

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 endpoint→client 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

IDPro 101

Tuesday 1E
Convener: Sarah Squire, Engage Identity
Notes-taker(s): Dedra Chamberlin, Cirrus Identity

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

Participants:
Judith Bush - OCLC
Jake Pszonowsky - KPMG
Jonathan Hard - Netflix
Ken Klingenstein - Internet2
Colin Walls - Kantara
Brad Hill - Facebook
Robert Burgess - Gigya
Jim Fenton - Independent Internet Technologist

Sarah reviewed current state:

The ID Pro group is forming, with a goal of professionalizing the field of identity management, establishing a shared body of knowledge, and hopefully making it easier to recruit and train qualified people in the identity management (so that it's easier for employers to hire good people and/or train people they hire to learn IAM).

Currently forming a non-profit membership org 501(c) (6)

Seeking founding members (corporations) to sponsor initial foundational work.

Seeking individual members to help build the body of knowledge and provide input on the effort - looking for people who have been doing identity for a long time

One of the first goals is to create a body of knowledge.

For more info, see: https://idpro.org/

http://kantarainitiative.org/confluence/display/idpro/Home

Sarah asks - What do we think of the concept, what kind of services should ID Pro provide?

Consensus that it's very hard to find qualified identity management staff, and when you do hire someone who knows identity management, they usually know only a single identity product (OIM, Sailpoint, Ping, etc). We need more IAM professionals that have a conceptual, non-product specific understanding of identity.

Body of knowledge needs to have different areas of focus (streams/tracks):

Technical
Governance
Business process

Suggestion: ID Pro should identify clear career paths in the identity field - make it appealing for someone looking for a new career path.

In terms of credentialing, Sarah reported that the plan is to outsource any actual testing for certification since there are plenty of companies already that do this well.

WRT credentialing, many in the group expressed a concern that any credentialing process not turn into a gatekeeping function. Some pointed to the (bad) example of CISSP certification. It has become a bit of a requirement to have that certification in some fields. Yet the content for the certification program is not current to the technical realities of the market, and people who are technically savvy actually hold the certification in disdain.

Examples were shared of situations where really qualified people didn't apply for critical security roles because they lacked the CISSP certification, and mediocre people who were certified got the job.

Request from the group: let's not have have a certification program that repels people who are the most qualified. OWASP has been much more successful. Useful body of knowledge that people can leverage regardless of certification (eg top 10 vulnerabilities list)

It was noted that there are important subsets of IAM knowledge where it is critical to know about how they are different from standard enterprise identity - Higher Ed and Healthcare for example

We talked a bit about the domain of information security and how it historically hasn't included or embraced identity management explicitly and that we should try to change that. Lots of people at Security Conferences don't seem to know much about IAM, even if they talk a lot about access control. BlackHat, DefCON - where are the IAM folks

Though Brad mentioned he gave a presentation at an RSA conference on the history of authN systems and it was well-received. There is an audience.

Maybe we should look at bug bounty services and make it easier to find identity-related exploits

In terms of the body of knowledge:

- focus on use case descriptions as teaching vehicles for identity concepts. Don't just give people a glossary of terms and conceptual/functional definitions. Describe real world scenarios of challenging identity integrations/problems and different approaches to solving them. That's how most people end up learning identity management in the field.
- Recognize that many organizations deal with lots of legacy tools and heterogeneous environments and in many situations, existing tools are not open source and the best future solutions are not always open source.
- Needs to be useful to decision-makers (budget authorities) and technical implementers. Be sure to include info on how investment in identity returns value to the organization.

How to get more people involved?

- Radiant Logic is sponsoring regional meet ups
- Judith had taken ID Pro flyer to regional meetings
- More recruiting will happen at CIS

Questions:

- Should the ID Pro organization offer publications for members? Sure, but make sure it doesn't become Gartner-like. Should not be a corporate mouthpiece.
- Would people like a newsletter for members? Consensus was "yes"

Joram 2.0

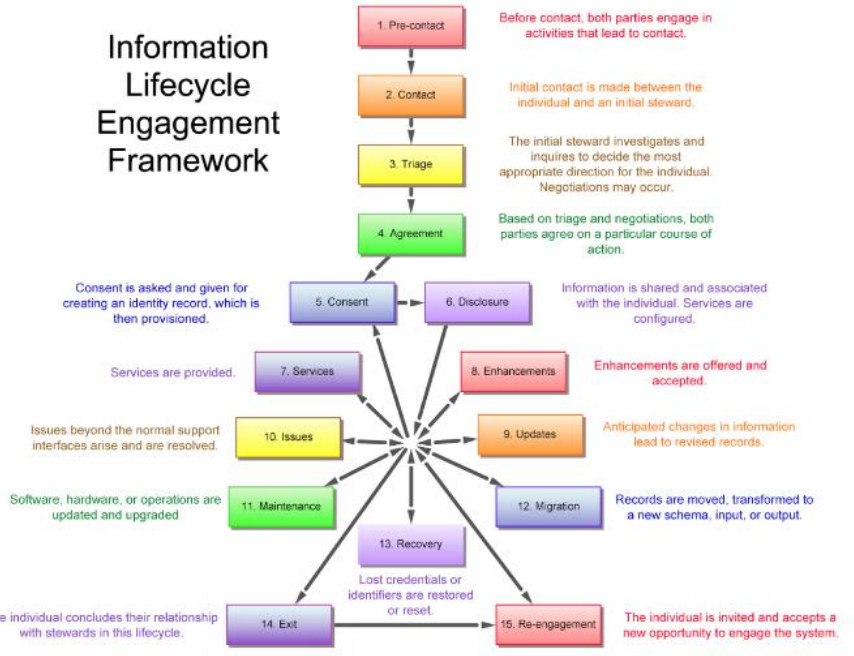
Tuesday 1G
Convener: Joe Andrieu
Notes-taker(s): Heather Vescent

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

Attendees: John Nash - Vance Bjorn - Paul Madson - Tom Brown - Joe Andrieu - George Fletcher Heather Vescent - Peter from I respond (humanitarian refugee project)

Reference link: bit.ly/joram100

- Joe walked us through the Joram narrative, stages 1-15 at bit.ly/joram100.
- Vance Bjorn, asked about the consideration of the use of biometrics.
- UN agencies, NGOs are the ones who go through the processing on the ground.
- Question: how do you manage the verification of the asserted skills (e.g. welder vs lawyer)?
- How do you do identity when you don't want to be identified (and they aren't terrorists)?
- Question: how to deal with multiple identities?
- Questions about consent – to disclose health history or work history. But did not have consent for the photograph.
- George: Need to help people build their story for their security.
- Stewards/guardians



[3] http://kantarainitiative.org/confluence/display/infosharing/Customer-Supplier+Engagement+Model+Quick+Starter

OIDF MODRNA WG Update

Tuesday 1H
Convener: Bjorn Hjelm, John Bradley
Notes-taker(s): Mike Schwartz

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

MODRNA (pronounced modernah) stands for Mobile Operator Discovery, Registration & autheNticAtion. The MODRNA WG is developing a profile of OpenID Connect intended to be appropriate for use by mobile network operators (MNOs) providing identity services to RPs and for RPs in consuming those services as well as any other party wishing to be interoperable with this profile. The WG is also developing extensions to OpenID Connect as needed in the context of GSMA's Mobile Connect initiative (GSMA = GSM Association), such as server-initiated authentication, transaction authorization, and account migration. Additionally, it will identify and make recommendations for additional standards items.

Not just about logging into stuff from your phone, but logging into web applications, and using your phone as an authentication mechanism.

Standardizing the profile the phone operators

User ---> SP <-- API Exchange
^
|
MNO

Authenticators: FIDO / SIM

Either each MNO can have a OpenID Connect, but there are also hubs serving multiple MNO's.

MODRNA has a few specs:

MODRNA Discovery
MODRNA Registration
MODRNA Authentication Profile
OpenID Connect Account Porting
OpenID User Questioning API
OpenID Backchannel Authentication

The GSMA issues software statements to the RP's, which they can use to register at MNO OP's to get client creds. It's a similar design to the OpenID Connect banking standard. The software statement is basically a Metadata Statement as defined in the OpenID Connect Federation draft spec.

Discovery is in the API Exchange... it's not required if the operators has a way to look up the metadata (i.e. an operator can setup a discovery endpoint that all the operatings in Germany might use...) In a given country, you probably already know the mappings of numbers to carriers.

Right now, RP's are not generating JWT metadata statements, but are simply going to a form to fill out the information about their RP.

Adoption is going well in Africa, India, Pakistan for banking, commerce (the Indian version of ebay).

No fee from GSMA for registration. RP's must agree to terms of service, privacy and provide contact info. MNO's may charge for advanced services like 2FA, or identity proofing (higher LOA), backchannel authentication (like a push notification).

Only fee is lookup from API Exchange (but free for first million lookups)

Software statements may be revoked, but it will be handled on a case by case basis.

Even feature phones can support SIM card implementation. However iPhones don't give access to the SIM card, so FIDO is better (UAF to a dedicated authenticator app).

Additional Material: MODRNA WG update presentation at https://www.slideshare.net/BjornHjelm/openid-foundation-modrna-wg-75588174.

12 Networked Leadership Competencies

Tuesday 1J
Convenor: Mei Lin Fung @meilinfung httpo://peoplecentered.net
Note taker: Mei Lin

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

We talked about the Wells Fargo scandal and if and how any of the 12 leadership competencies might have been helpful or relevant.

Peter, Joyce and Kaliya and I had a great conversation about this. Peter brought up how these competencies were encompassed in the 3 words Procter and Gamble used in training employees:

- Envision
- Energize
- Enable

We recognized that this level of effective work enculturation is no longer happening.

Other companies that have been doing this are Johnson and Johnson, Intel, and countries: Singapore,

The origin of the competencies out of the work funded by the US Dept of Defense looking at the Future of Health. See background.

Background on People Centered Internet and the competencies

Our digital inclusion projects across the world are linked by a common intention to improve lives. This common intention forms the foundation for why we collaborate. Other attempts to convene and act together falter when it comes to working together in a network to achieve goals beyond the agenda of each individual institution, organization or government – sometimes attempts to coordinate and collaborate internally falter.

PCI emerged from a multi-year project conducted by the US Federal agencies involved in health, including the US Public Health Service. Funded by the US Dept of Defense, we took a step back to consider amongst all the options available to the wealthiest country in the world, what strategy over decade would bring together federal, state and publicly funded agencies to work with the private sector and local communities to achieve health as a national strategic security imperative.

The concept of the co-evolution of human processes with the emergence of the Internet was first articulated by Dr. Douglas Engelbart, leader of the Augmentation Research Center at SRI in Menlo Park, known for the invention of the computer mouse, the father of human-computer interaction, hyperlinks and more. Engelbart's lab was not only the second node on the Arpanet that connected to Vint Cerf and Len Kleinrock at UCLA, he proposed that the technology which he envisioned was so powerful, it needed the development of human interaction in communities networked together, to assure that humanity would be the ultimate beneficiary of these new tools which have already transformed our world.

The US Air Force had funded Engelbart's early work and Col. Brian Masterson kept in touch with Engelbart over the years. In 2008, the 40th anniversary of the "Mother of All Demos" where Engelbart demonstrated the mouse, remote video conferencing, hypertext and more, the incoming Air Force Surgeon General Bruce Green took the first step to convening of a strategic think tank to look at the future of health and invited representatives of Engelbart's thought leadership to Sterling Air Force Base in San Antonio Texas. At that February 2009 gathering Mei Lin Fung presented the concept of Networked Improvement Communities and was one of the 5 out of the 17 thought leaders to be invited to form the core of what became the Federal Health Futures initiative.

Over the next four years, the concept of networked improvement communities emerged as a robust capability to be developed that could be strategic to a better future of health and thriving for the US and for the world. Federal health leaders were convened in roundtables, across department silos and functional specialties to consider how to develop this capability. Dr. Jonathan Woodson, UnderSecretary of Health Affairs at the Dept. of Defense concluded that the emerging Defense Health Authority would need new leadership competencies for operating in a networked world. This notion was not so surprising in the Dept. of Defense because in response to the 9/11 attacks, the US active military had already concluded that the traditional Command and Control hierarchical system had not been effective against the Al Qaeda network and the new technologies of the internet and mobile telephony required new leadership strategies. Deploying network capability and developing network leadership as a response to the national security threat has been part of the shift in the active military side of the Dept of Defense.

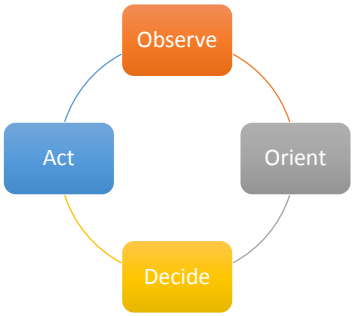
The networked capability and networked leadership imperatives for health emerged naturally within the Federal Health Futures initiative which began with alternative future scenario development. We

examined many future scenarios and determined ways which we could build capability so that no matter what future emerged, we would be better equipped to deal with whatever came.[1]

Culture takes years to change – institutions are resistant to new ideas. Yet all those involved in the Federal Health Futures saw it as a unique opportunity to serve the public in ways that might enable the public to be served in new ways by utilizing the emerging networks in all spheres of private and public life.

The Internet and technologies provided a means for tracking not just immediate actions but series of actions and decisions over time. And for tracking not just the actions, but the actual processes under which the actions are taken, including when the process works to achieve the intended outcome and when the process has inadvertent consequences. Finally, the Internet and technology can track the purpose of the processes, the parameters and conceptual framework for the process design so it can be evaluated whether it achieves not just the objectives and goals, but also fulfils the intentions of the framers.

The Federal Health Futures built on the concept of the US Air Force OODA loop: Fast flying aircraft require adaptive response to the environment and the decisions and actions of other aircraft in the air, whether friend or foe. This was encapsulated in the feedback loop which when executed repeatedly gets closer to the goal.



Within a network where information is routed at the speed of light, where more information than one human brain can process arrives, where effective decisions with long term implications must consider hundreds or even thousands of factors, only technology can handle the processing.

A key outcome of the Federal Health Futures initiative was the development of a feedback loop that ties different levels of hierarchical decision making together in a way that provides human oversight at key points of policy and decision making. This diagram offers a compass for the feedback loops required for operating a network of disparate players with different goals who work together on an overarching goal. Engelbart's insight was that coordination and collaboration do not require constant knowledge by everyone of everything. But that information needs to be shared only when overlapping interoperating actions, processes and strategies are underway in which multiple independently operating players are involved concurrently.

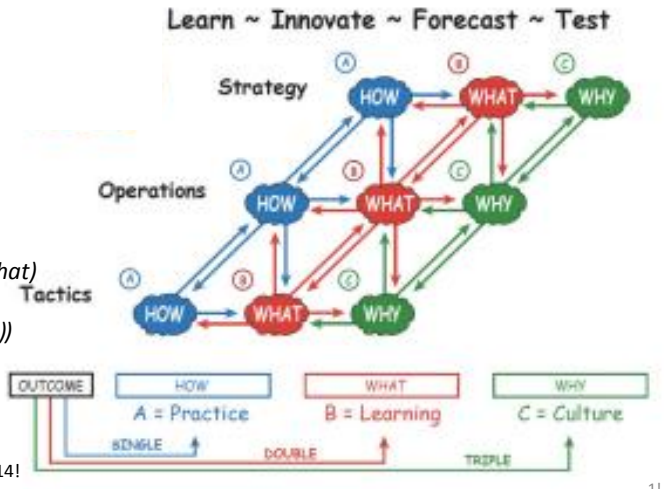
[1] Hudak, Russell, Fung, Rosenkrans – Federal Health Care Leadership Skills required in the 21st Century https://drive.google.com/file/d/0BxWhDjUmHhD6WTBxLUJGTkkxeEU/view?usp=sharing

The design and ongoing oversight of complex systems requires human judgement to assure that the technology serves the humans and is not hijacked by players with aims which would sacrifice the whole of humanity to achieve shorter term or individual or tribal objectives like power, influence and wealth.

Strategic)Triple)Feedback)Loop)) takes)Prac5ce)to)Learning)to)Culture)

Achieving!Outcomes!require!
Strategic,!OperaConal!&!
TacCcal!AcCons!with!!
Transparent!alignment!to
WHY,!WHAT!and!HOW!

Learning)Feedback)
Loops)assure)we))
always)know)WHY)
we)are)doing)WHAT)
we)are)doing)to)assure)that)
HOW)we)are)doing)it)is))
in)alignment)within)the))*
Network.)
!
!
Source:!Douglas!Engelbart!!
Memorial!Momento!July!13!2014!



A protocol for aligning actions between multi-stakeholders in a networked world can enable levels of collaboration that are currently unattainable. Not because the tools don't exist, but because the culture, learning and practice needs to emerge.

The People Centered Internet raises the flag, the Strategic Why for all technology initiatives and projects:
Does this ultimately serve humanity?
- Can you share a story that represents why this work is so important to you?

My great great grandfather was an indentured slave who left China during the famine, to work in the sugar plantations of British Guyana. I inherited his great energy and vision which enabled him to start a provision store and educate his children, they became wealthy enough that his grandson Samuel Fung was sent to London to study law. Samuel decided to take a detour to Southeast Asia on his way back to South America. There he met my grandmother in Penang Malaysia and married and my father was born there. The family moved south, Samuel Fung was a respected member of the community, a London educated lawyer, when the Japanese invaded Singapore during World War II. The occupiers sent a letter summoning him to meet them. He had breakfast that morning then cycled from his home and was never seen again. His name had been given to them as an enemy collaborator – we believe it might have been someone jealous of his position in the community, he was completely unsuspecting of why they might have called him up and went willingly.

As a lawyer he respected the rule of law, he believed that societies are stronger and people are better together when we abide by the common "rules of the road" and respect the institutions around us. At a time of disruption, his notions which had served him well up to that point, made him trust that an innocent person would not be mistreated.

If we want to function as a society, this trust is essential. We are stewards of that trust for humanity, each person has a responsibility to make sure that the institutions that operate around us earn and keep our trust. This is something that the Internet has emerged from – many people from many cultures coming together working to earn and keep the Internet functioning.

The Internet may be the most disruptive tool that humanity has encountered since the printing press. The printing press made it possible for ordinary people to participate at the highest levels. It led to the English reformation, the scientific Enlightenment, the American Revolution and much much more.

The Internet also offers one of the most powerful tools for existing powers to consolidate their authority and power.

Humanity faces a fork in the road – do we let unseen and unknown forces take hold of the steering wheel and take us "we know not where", or do we decide that this tool can be a tool which offers people greater opportunity to realize the potential of each human being.

If we decide it's the second fork we want to take. There is work to be done because others are already working and working hard on the first, using the Internet to realize their own individual, organizational, corporate or national agendas to the detriment of others.

The People Centered Internet emerges now at the next phase of the evolution of the Internet, to hold the flag high, that we must earn and keep trust for the Internet to realize the potential it offers in catalyzing innovation in networks, and in the process, many future generations of people will find and develop their passions while contributing to a better future.

We must learn to get better at getting better together. Our Institutions have developed in a "top down" world that has developed over millennia. When things go bad, we instinctively look to an authority figure to tell us what to do. When we try to collaborate, someone often steps up and says, "let's do it my way". Network capability exists now but we do not yet know how to take advantage of it. After reading and writing were invented it took centuries before universal education became a priority. Breakthroughs can emerge from the most unlikely places. Internet inclusion can unleash new frontiers of innovation by teams of unlikely people.

Our strategy is for people to work in learning networks of communities: Where people learn from others to improve their own communities.

It is a very different way to work that requires new protocols. We must develop trust and learn to listen and think adaptively. We can set goals as a network and work together as a network to realize them.

In the Federal Health Futures initiative, we realized that the power of networks was the most effective for getting better health at lower costs. Dr. Jonathan Woodson convened a multi-stakeholder summit over 2 days with federal health leaders, jointly with his counterpart Dr. Howard Koh at the Dept. of Health and Human Services in September 2012. We examined what was stopping progress and where breakthroughs had occurred. Both Dr. Woodson and Dr. Koh said that this came down to leadership:

Icon	Competency	Illustrative Characteristics
	Ability to Develop Trust	Establishing rapport and building relationships to cultivate a culture of trust.
	Active Listening	Suspending judgment to hear and understand the thoughts, ideas, emotions and perspectives of others.
	Agile Thinking	Thinking systemically with the ability to shift paradigms and perspective, with the capacity to incorporate and appreciate multiple viewpoints.
	Aspirational Future-based Leadership	Leveraging strategy, operations, tactics, to harness the collective wisdom and an inspiring vision of the future to help realize a shared vision of a desired future state.
	Building Partnerships	Ability to form and sustain effective relationships across organizational boundaries in pursuit of mutual interest.
	Creating Learning Networks	Curious and open to new ideas and information with a willingness to share and reflect systematically on the insights arising and the ability to cultivate, encourage and sustain these behavior with others.
	Creating Conditions for Success	Offering resources, building capability, anticipating and removing obstacles, to provide clear strategic intent and sustained focus.
	Developing Present Moment Awareness	The ability to see everything as new; including mature self-awareness and freedom from the fog of preconceptions and groupthink.
	Net Centric Communication	Smart and progressive use of information technology to optimize resource use in a complex and rapidly evolving environment.
	Network Goal Setting	Ability to see and shape the combined results of multiple objectives pursued by multiple stakeholders and the capacity to define and negotiate coherent action plans.
	Network Leadership	Vision and ability to reach across traditional organizational boundaries and to engage others through collaboration and mutual interests.
	Resilience	Ability to bounce back from adversity. Patience and will power to persevere in the face of setbacks.
	Thriving in Complex and Ambiguous Environments	Ability to tolerate ambiguity and act effectively under conditions of uncertainty, able to recognize patterns and adapt quickly and iteratively as new signals emerge.

That we needed new competencies for leaders operating in a networked world. Discussions surfaced 163 leadership behaviors that were not currently recognized as needed, and were not being learned or actively practiced amongst federal health leaders. These were distilled into the diagram of 12 competencies above.

Our priority at PCI is to work with our partners to set up networks of improvement communities so we can all achieve our overarching goals together, and to use our technological tools to augment our human capabilities to work together better.
The UN Sustainable Development Goals provide the set of overarching goals that tie 192l countries and stakeholders together. Coordinating and collaborating to achieve these provides clear direction to technology companies, digital inclusion proponents, actors and change agents to look for shared Sustainable Development Goals in common.

- What does success look like in the foreseeable future (say 3-5 years) for you? What are some examples of things that you will have accomplished or things that will be different?

In 3-5 years, we will have a few pilot networked improvement communities – in a country, across agencies, across countries. We will have a community-centered approach to health – where we see the health of an individual as intimately connected to the health of their family and their community. We will have a cross cultural approach to education where diversity of viewpoints is essential in helping young people learn how to operate in a networked world – to tap the wisdom of others as part of realizing their dreams, and working out how to bring dreams together to create something bigger than anyone individual can do alone.

Digital Inclusion

Tuesday 1K
Convener: Alpesh Shah
Notes-taker(s): Alpesh Shah

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

1. IEEE SA has launched a Digital Inclusion through Trust & Agency initiative that welcomes experts and interested parties to http://standards.ieee.org/news/2017/digital_inclusion.html

2. Participants discussed topics ranging from contextual identity to credentialing to fiat currency to borderless nations

3. Those that participated in the round table expressed interest in participating in the initiative to help make an impact

Others are welcome to join as well. If interested, please contact Maria Paolimbini (M.Palombini@ieee.org)

Digital India

Tuesday 2A
Convener: Mei Lin Fung
Notes-taker(s): Laurie Wang

Tags for the session - technology discussed/ideas considered:

Digital India, Aadhaar, biometrics, financial inclusion, national ID systems, role of government, privacy

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

Digital India has 3 main categories: 1. Infrastructure 2. Delivery of Services 3. Digital Literacy; Functions include digital lockers, econsent, payment.

Useful Links:

- http://sites.sph.harvard.edu/nidc/videos
- http://www.gsma.com/mobilefordevelopment/wp-content/uploads/2016/07/Towards-Shared-Principles-for-Public-and-Private-Sector-Cooperation.pdf
- https://www.omidyar.com/blog/digital-identity-no-empowerment-without-privacy
- http://documents.worldbank.org/curated/en/213581486378184357/pdf/112614-REVISED-4-25-web-English-final-ID4D-IdentificationPrinciples.pdf

Interest in Digital India	Next Step main interest	What others said about this
Development, India, World Bank, ID40 principles	Governance, Privacy issues	World Bank's ID 40 principles - who is working on this with them?
Understanding ID in a different Culture, loss of anonymity, what does Gov do? what does private industry do? Regulation? Share best practices		ID Systems: 1. Human capacity building 2. Citizen access to services
Civil Liberties	Prevent Statism in Identity Systems	
Samsung devices already in use in India		
Biometric in use for 800M. Aadhaar defacto ID	Unintended consequences of a centralized data base of e.g. biometric ID's	Tech billionaire drove Aadhaar, many Tech volunteers in India
ID-human dignity. Just at the beginning - how can rest of world help/be involved?	Human dignity, rural india, UDAI, 2 pager for Digital India architects	How can other initiatives and other countries learn from UDAI

What is ID? How data sharing? East vs West	Trust - Gov, citizens, business	Tyranny of Data. List known problems and approaches to them. CORRUPTION
Scalability, how to deal with error rate which multiplies exponentially - India's 1+ billion population presents major new challenges	Biometrics, scalability, cultural identity	Government as Catalyst; Private industry or NGO alternative to gov as catalyst: How to weave learnings and improve together for benefit of people
Well-connected family in India. Cares about how Silicon Valley can help/ be involved; Digital india started to address needs of those who come from rural areas and work in urban, ration cards were facilitated by Aadhaar (too much too fast); Culture issues ID vs Authentication	Moral responsibility to 500 million people thrust upon the edge of digital frontier	Learn from other nation's examples: UK, Canada, Singapore, Estonia, Peru, Mexico (banking the undocumented - Vance Bjorn); National ID conference at Harvard Fall 2015; ecommerce and demonetization.
Collect, Store, Transfer	What is ID?	
Journal of record for background checks, FCRA	Fraud, new frontiers	Corruption and Digital Literacy, _ standards mapping to existing
Rural India, developed open source low cost mobile phone		
Dignity		
	digital literacy surrounding the negative aspects of the Hyperion Report	Mei Lin - Iterate: Plan Do Study Act; OODA loop
Bottom up - meeting the aspirations of the marginalized	Scalability - Open identity standards	
can learn from work by Mexico on banking the undocumented - authentication		
Funded Consult Hyperion report on Aadhaar cited by Kaliya	IEEE - IEEE Standards for Internet Inclusion	David Rodriguez of Identity.com standards mapping to existing; Karen McCabe IEEE, Steve Olshansky Internet Society
Trust, P2P, When? How? Iterate	Prepare 2 pg w/ Joe Andrieu for Digital India representatives on World Economic Forum digital economy & society global future council	Trust - S Shariq interested in follow-up on trust between the 3: governments, citizens, businesses
Identity and Trust		
	IEEE - IEEE Standards for Internet Inclusion	

I. Digital India – what is it?

a. Problem: India's large rural population and urban migrants rely on gov't handouts, ration cards based on old identity systems that are local
b. Aadhaar is national biometric ID system to solve these issues, but facing growing pains and based entirely on authentication (not identity); has to led to privacy concerns – this is one piece of Digital India
    i. Consult Hyperion's Digital ID Issue Analysis
        1. Pros of Aadhaar: roll out to large #'s, strong tech security, focus on ID not citizenship, only shares relevant information
        2. Cons: no comprehensive data protection, no independent data protection authority
c. Digital India is government's big initiative to leap frog through:
    i. Creation of digital infrastructure
    ii. Delivery of digital services
    iii. Digital literacy

II. Topics / approaches proposed

a. What are other countries doing? UK, Canada, Estonia, Peru
    i. Resource: National ID conference by Harvard, 2015, https://sites.sph.harvard.edu/nidc/
    ii. Types of systems:
        1. Canada has one national ID card built into multiple systems (e.g., drivers license, health care records)
            a. Tradeoff is security and privacy for the individual in one giant file
            b. British Columbia has overcome this by allowing agencies to see only appropriate information – takes sophisticated thinking and systems design
b. India needs to overcome tyranny of data
    i. Identifier is your identity, if identifier gets corrupted, you lose your identity – system must be built to work around this
c. Digital literacy as core issue
d. Loss of anonymity – what are best practices to mitigate this? World Bank has established some but we need more private sector voices

III. How is identity viewed in India?

a. Data sharing: users more willing to share vs. EU
b. In India, "shopkeeper is king" vs. "customer is king" in US
c. The benefit of national ID system is financial inclusion for the undocumented
d. India's a very young country – 500 million "millennials" so lots of room for innovation in service delivery and new concept of identity
e. Role of government: privacy regulations far behind "best practice"
f. Corruption is the biggest danger – it's a trust issue

IV. Is financial inclusion worth the trade-off of privacy / risk concerns?

a. Example: Singapore has biometric ID system – used to drive massive GDP growth and rise in standards of living, had to give up some privacy

b. We need to get across that India is not done yet
c. Need to give user transparency and consent: example = how background checks work

V. What do we want to recommend / contribute to Digital India?

a. Should depend on what people of India want – including marginalized populations:
    i. Demonetization drives need for modernization of ecommerce and mobile wallets
    ii. Ready for large-scale adoption of digital delivery of services but need guidance
b. There will be opportunities for other actors to provide private, more secure components and build on top of India's identity stack (e.g., digital lockers)
c. Need best practices, IEEE can help influence
d. World Bank principles stipulate standards to receive funding for national ID systems – encourage systems to be open and interoperable, prevent vendor lock-in, with security, privacy and ease of use
e. This is an opportunity to not re-inforce a statist perspective on identity
    i. How do we "dance" with the states but not end up with that being the only legitimate path to identity?

VI. Additional Resources

a. Identitiesproject.com has series of compelling videos: https://www.identitiesproject.com/
b. Caribou report: http://cariboudigital.net/new/wp-content/uploads/2016/08/Caribou-Digitial-Omidyar-Network-Private-Sector-Digital-Identity-In-Emerging-Markets.pdf

Intro to OpenID Connect

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:

The presentations is posted at http://self-issued.info/presentations/OpenID_Connect_Introduction_2-May-17.pdf and http://self-issued.info/presentations/OpenID_Connect_Introduction_2-May-17.pptx.

JLINC Overview

Tuesday 2F
Convener: Victor Grey
Notes-taker(s): Dan Finlay

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

Enabling the negotiation and recording of data sharing contracts. Allowing verifiability as well as GDPR compliance, i.e. "right to be forgotten".

The source of contracts and agreements is extensible.
Riak database ends up being the signed contract store for most enterprises, but can store to any persistence method, including any blockchain.

LINC is not an identity provider, it's a data transaction layer for exchanging permissioned data.

Two questions from me:

1. Where are these user preferences stored? Anywhere the parties choose to. JLINC is a tool for creating & exchanging agreements and updating them.
2. We are still trusting these services to delete data to "forget" it, right? This forgetfulness is just a "best effort to comply" situation?

Some contracts will include a "minimum data to retain account", and if the user chooses to redact any of that information, the account would be closed as per the original agreement.

Some terms are proposed.
- iat
- context
- terms address
- data address
- REF Required
-

The rights holder signs them
The data custodian signs them.
JLINC hash generated
Stellar Ledger ID recorded (a key for lookup on whatever ledger)

Victor likes the Stellar 32-byte hash format, and will probably continue using it even if they drop Stellar as their ledger.

LINC handles the legal aspects of signing a data permission agreement. If you need to record a data permission, or the redaction of a data permission, LINC can be a framework for recording the two sides of that agreement as the points that it changes.

Delegated Account Recovery

Tuesday 2G
Convener: Brad Hill @hillbrad

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

https://fb.me/recovery
http://github.com/facebook/DelegatedRecoverySpecification
https://github.com/facebook/DelegatedRecoverySpecification/blob/master/draft-hill-delegated-recovery.raw.txt

Presented by Brad Hill from Facebook

Background:
- People still manage to forget or lose things; yubikey, etc.
- E3e email where I lose my device; One solution is just to lose the data
- Smtp / plain text email based recovery is baseline
- Pull model; use oauth to pull data towards me – current setup
- Push-based model; wrap up my identity in a recovery token
- Push token to facebook, save it for me in my account
- It's opaque, so facebook doesn't see what the data wrapped into account recovery is

Approach; similar to an oauth flow, but it's not an oauth based system:
1. User creates account at e.g. github
2. Github wraps an opaque token and relays it back through the user to fb
3. User authenticates to fb
4. Fb stores opaque token, and signs it
5. User loses authentication to github
6. User requests access to github
7. Redirects to facebook and reauthenticates to fb
8. Facebook relays the token back to github
9. Github checks fb signature to ensure it's appropriate
10. If it is, the user can recover the account

What's in the token; binary structure:
- ID: 128 bit number chosen by issuer of token
- Issuer string (e.g. github)
- Audience string (e.g. facebook)
- Timestamp
- One byte of options
- **Data field**; is opaque: notes here.
- Token binding
- Signature – nist p256
- When returned, it gets wrapped in a countersigned token
- Low-end implementation is map github UID to facebook to SHA256 of token.

Misc Information:
- FB and github each know that a party holds an account, but not who the party is
- User gets to choose where to save it, and github allows you to choose where to save it

- Question – lifetime of that token
- Root of trust is the .well-known URL
- Counter-sign of keys helps make the token useless unless it's signed, so if there's a dump of the unsigned tokens, the tokens are useless
- Key splitting is possible, but outside the protocol

Maintaining state
- Flag for status callbacks – e.g. you can get a notice that a particular token is out of scope; e.g. deleted; email addr recycled; e.g. delete your facebook account. It's gone, nag them to do something else

Building a Kick Butt Identity Team

Tuesday 2H
Convener: Sarah
Notes-taker(s): Jonathan McHugh

Tags for the session - technology discussed/ideas considered:

#IdentityTeams

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

Dysfunctional	Productive
Lack of testing/UX	Skill sets Architecture (standards aptitude] Sales to Dev PM Training (external & internal) Dev UX DevOps SME QA Infosec/appsec Communication
	Easy/accessible/open/powerful ID infrastructure
Organizationally-distributed (accessibility but lacking broad vision)	Issues-Employees have, generally, more privileges
Lack of dedicated resources for identity team/forward thinking	Auth0-Allow a lot of privilege with a huge amount of auditing
Treated as IT	Functional definition of security

Split between IT/IS	Powerful engineers/CI/Audit/Notification[ATC = Automated Test Ops]
Uninformed product owners	Breadth of and depth of team-All have broad, individuals have depth
Identity team overly restrictive	Organization-wide recognition of security and identity SME as priority
	Treated as IS
	Executive support/cover from management
	Clear policy articulation
	Minimizing glue/integrating standards
	Metrics aligned with smart infrastructure

Discussion

- What is an identity team
- Consumer and Enterprise Organizations
- George Fletcher
    - Many times the identity team is broken up
        - Manager
            - Enterprise Services Team
            - Identity team
        - Manager
            - Security
    - Consumer and Enterprise identity/security is converging
        - Least privilege
        - Unintended consequences due to complexity
        - Enterprise developers need to adopt the consumer developer attitude towards identity
    - Raising the priority of identity tech
- Jonathan Hurd
    - Sales to Dev connectivity
    - Engineers using standards but having the flexibility to
- Justin Richer
    - Pre-configuring Identity technology for easy integration
        - Libraries
        - APIs
- Matt Muller
    - Upon departure, how many systems will we have to disable their identity on?
- Jonathan McHugh
    - It's identity, stupid

Consent-Informed Attribute Release (CAR): Serving SAML and OIDC/Oauth

Tuesday 2I
Convener: Ken Klingenstein
Notes-taker(s): Judith Elaine Bush

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

Topics

- CAR basics

  – Useful related products–attribute taxonomy

- CAR in multi-lateral federated SAML families

  – Services for attribute release and consent – Informed content gathering and use – Unexpected outcomes

- CAR and the Oauth world – Services for permission setting and consent – Informed content gathering – Next steps – Possible unexpected outcomes

Consent-Informed Attribute Release (CAR)

- A system of components that serves attribute release and consent needs across all protocols – OIDC and OAuth as well as Shib/SAML.

  – Integrates organizational and individual choices for attribute release

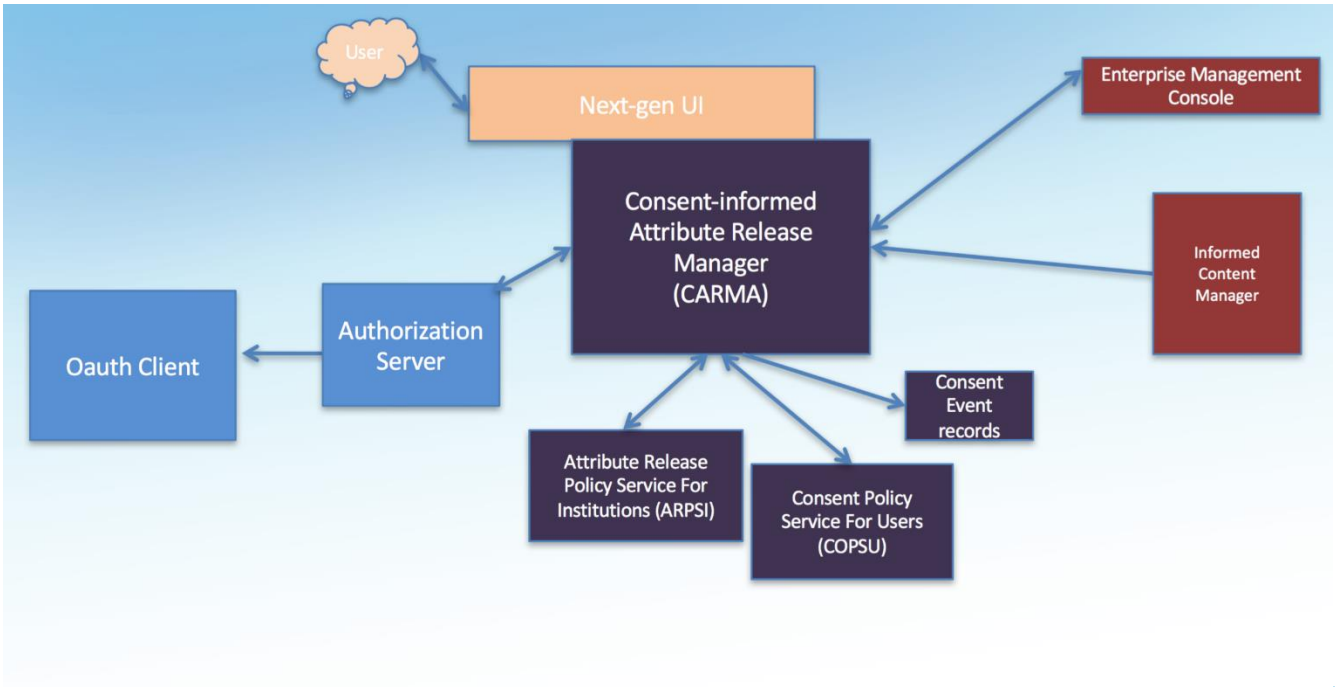
  – Support for user consent decisions that are informed, effective, revocable, accessible, etc.

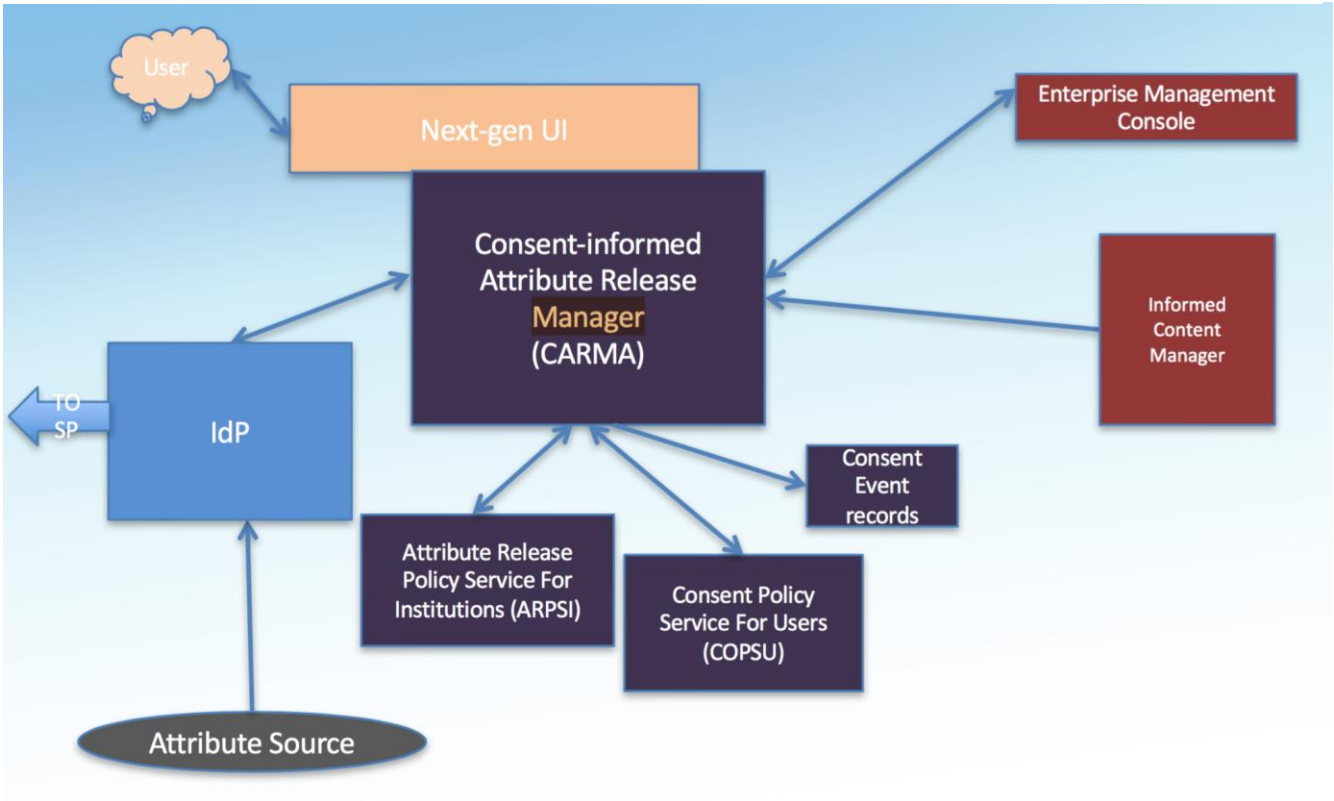
- Catalyzed by NIST NSTIC grant and now becoming an Internet2 open-source TIER component.
- Includes UI/UX, enterprise and individual attribute release policy stores, notification and event services, individual and organizational admin interfaces, all accessed through the CARMA API
- UI/UX well researched, well-designed and well-implemented. Includes
    - – Device and browser independent. Device adaptive-works well with mobile apps. I18n and locale
    - – Fine-grain controls on attribute release (down to value level of multi-valued attributes), explanations, reconsent options, friendly names and values, etc.
    - – User self-serve for bulk management, revocation,e tc.
- HA, packaged in Docker containers. Scheduled to go through alpha/beta/1.0 over the next 6-12 months.

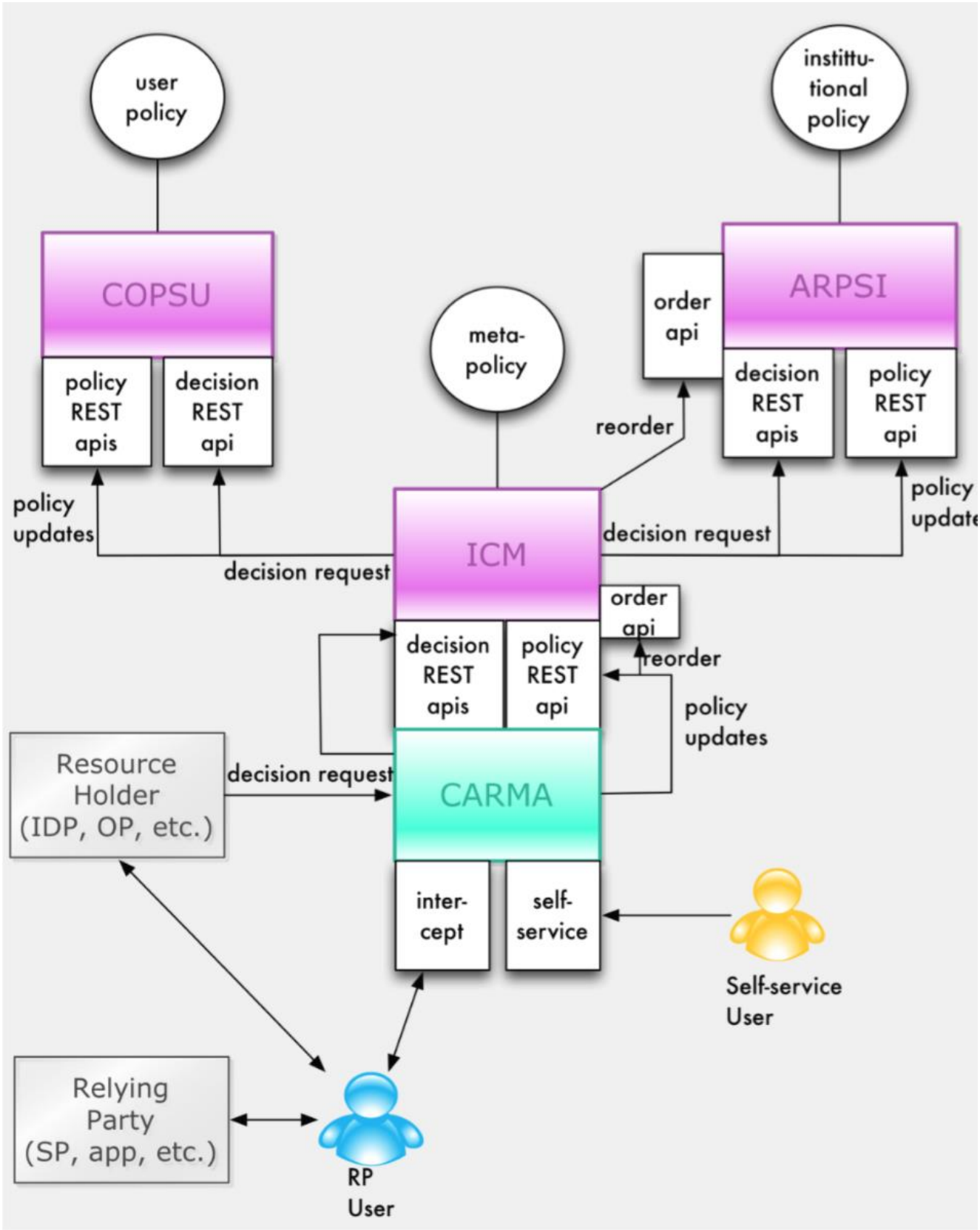
Consent-Informed Attribute Release Manager (CARMA)

- The CARMA API is the entryway for applications and users to manage attribute release; applications call CARMA to get consent and attributes or information items.
- CARMA is instantiated as: – a published API (ICM API) - ICM_July12_2016.yaml – HAcodeasaVMwithinaDockercontainerthatimplementstheAPI
- Includes UI for end-users in a variety of use cases (in-line, off-line, persistent) and management UI for end-user self-service, policy administrators, configuration, etc.

- Includes admin and super-admin consoles






user policy
institu-tional policy
COPSU
ARPSI
order api
meta-policy
policy REST apis
decision REST api
reorder
decision REST apis
policy REST api
policy updates
decision request
ICM
decision request
policy update
order api
decision REST apis
policy REST api
reorder
policy updates
Resource Holder (IDP, OP, etc.)
decision request
CARMA
inter-cept
self-service
Self-service User
Relying Party (SP, app, etc.)
RP User

What is Informed Content

- The fuel that drives effective and informed user consent decisions
- Limited, though extensible sets of marks, assessments, policies, etc. that are part of the UX
  – Additional user-centric information feeds
    - Vetted, self-asserted, reputation systems, etc
    - Far-reaching insights - https://arxiv.org/abs/1608.05661

Attribute taxonomy

• Analyzes key characteristics of attributes and how to present and manage them

• https://docs.google.com/document/d/13cFEpkaerCgit- aPPek2VZBFLwp7XhixZz0MHuZkdx8/edit

Status and Next Steps

- The core functionality of CAR code is complete
- Enhancements (policy editors, user-managed triggers for reconsent, improved admin interfaces, etc) await
- Being packaged now to TIER standards
- A cycle of code release versions and bug fixes etc awaits

Using CAR in a multi-lateral federated SAML family

- Attribute release is a major problem for R&E federations primarily due to attribute- retentive institutions wanting user consent.
- CAR is readily integrated into the Shibboleth IdP v3, with it being called for institutional attribute release policy editing and as the decision point for attribute release per transaction
- CAR gathers informed content from a variety of sources

Unexpected Outcomes

- Consistent, informed user experience across a variety of platforms and protocols
- Integration of institutional and individual attributes
  – Location
  – Emergency contact and medical information
  – Personalschedules
- Managing consent across applications and consent as a service
- Providing new options for accessibility
- Extending organizational attribute release policy from directory/IdP to other systems of record with bio-demographic attributes.
- Creates institutional policy repository and service for attribute release

Integration Of OIDC With CAR

CAR can serve as a

- policy decision point (PDP) and policy store for an OIDC authZ server
- point of administration for end user self-service of their consent policies
- point of administration for an IT admin CRUD'ing institutional policies (if they exist)
- policy store only

  We talk about each of these.....

Policy Decision Point (PDP) + Policy Store Option

• CAR has its own REST endpoints for returning decisions about a given user, RP, and set of scopes and claims -- called "info items" in CAR documentation.

– CAR relies in this case on the AS to authenticate the user (and send CAR the id in a JWT)

- CAR can operate as a PDP (& policy store) for an OIDC AS in both the user present, user offline, and "prompt = none" cases.
- If the user's policy choice is "ask me" for even a single given claim or scope, CAR will put up a UI that allows the user to
  - – make a specific choice for the "ask me" claim or scope
  - – see their existing choices -- and change them if desired
  - – **save their new choices** -- or not (using them just for this particular request)
- CAR's UI also current offers the user the choice to "show me this screen again." This choice causes CAR to put up the "ask me" UI even if there are no "ask me" policy choices.

Point Of Admin For Self-Service Option

CAR's policy retrieval and setting REST API -- along with its UI -- allow a user to create persistent policies about their claims and scopes on a per-RP basis.

- – CAR needs to be configured with an authentication service to use.
- – CAR already integratable with Shibboleth IdP V3

  Interesting features:

– "**All other claims and scopes"** required setting ensures that requests with "new" claims/scopes can be addressed

• User choices are permit, deny, "ask me" and "use advice" – "**While I'm Away"** required setting.

• As discussed, applies for "ask me" decisions if the user is offline or "prompt = none." – "**New RP Template."** CAR creates a new policy from the template when a new RP makes a request.

- Each user has their own "new RP template" and can customize it.
- Allows user to "set it and forget it"
- "Ask me" is the default policy (without any user action) for "all claims and scopes"

Point Of Admin For RS/AS Managers

While OIDC is oriented toward end users, CAR allows for the possibility of the RS/AS's own policies about users, RPs, and claims and scopes. These

– typically serve as “advice” shown to the user.

– can serve to override user choices in emergencies (or as SOP).

Policy Store Only option

In this case, CAR is simply holding policies for an AS. The policies would conform to CAR’s policy language of course.

- The AS would retrieve a user’s policy for a given RP -- or any subset of policies it wants using CAR’s REST API.
- The AS would then act as to make permit/deny decisions on requested claims and scopes.
- The AS would also serve as the point of administration for policies, putting up its own UI, instead of using’s CAR’s.

Modeling Resources & Scopes For Self-Service

In CAR, to allow for self-service**, the resource id needs to be the user’s identifier**, not a low level resource (such as a single photo).

Scopes In CAR:

- – Called Information items, “info items” for short in CAR documentation.
- – Can be “anything” since CAR doesn’t interpret the info item string.

• CAR needs a display name and description for each info item (see next section!)

– scope itself doesn’t need to be a clickable URL for UI to inform user. – **We recommend that each scope represent an “action on category” pair. E.g.**

• view_familyPhotos • print_Selfies

The type of scope modeling allows for easier management by a user:

- – Too many scopes could overwhelm a user (in our opinion).
- – Exceptions to a category -- e.g. a single photo -- could still be called out.

Informed Content Registration For Scopes

The CAR team is “in-progress” on creating the API that allows for registration of key information about scopes, claims, and attributes.

Note: OAUTH does not define the interface or protocol between the resource server and the AS. Here’s a quote from OAUTH 2.0 Authorization Framework Section 1.1 Roles:

• The interaction between the authorization server and resource server is beyond the scope of this specification. The authorization server may be the same server as the resource server or a separate entity. A single authorization server may issue access tokens accepted by multiple resource servers.

We expect the RS to register scopes/claims with the AS, which then registers them with CAR.

- – The “resource id” would be the user’s id.
- – **No need to pre-register users** (we have a “new user config” that creates policy on the fly).

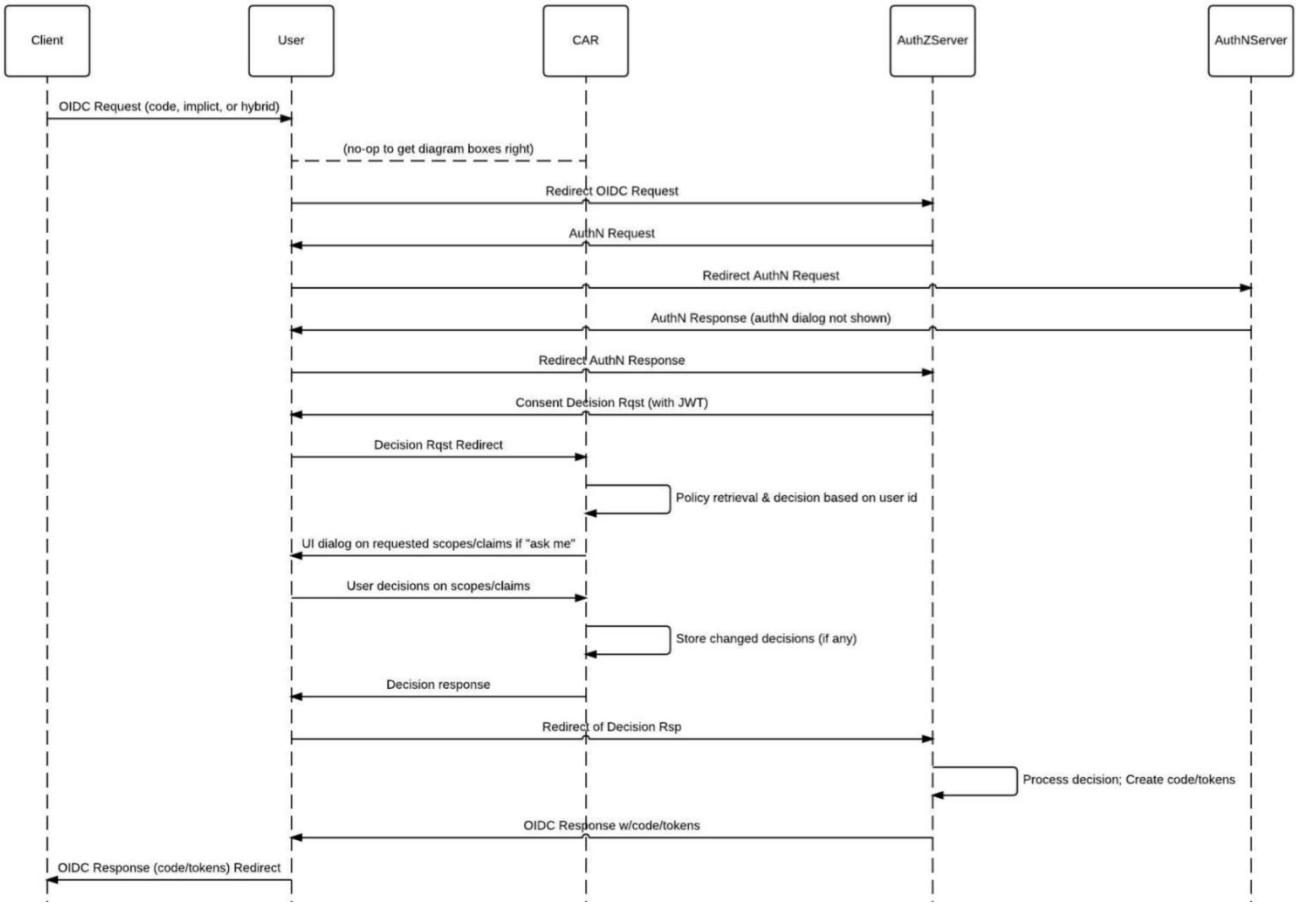
  Here is an over of the registration info CAR needs.....

Registration Info Overview

- Raw id of the scope/claim/attribute as defined by its Resource Holder’s (RH)

- Display string for item
- Description string for item
- Is the item “sensitive” as per GDPR and other standards?
- Is the item a “negative permission” input?
    - – E.g. “Malevolent User,” “persona non-grata”
    - – CAR “always sends” but “never displays” these items.
    - – Reason: We don’t want the user to “consent away” a negative permission.

    There is further registration info, more pertinent to attributes than scopes/claims.



Privacy and Correlation

Tuesday 3A
Convener: Nathan George
Notes-taker(s): Colin Jaccino

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

People, Organizations and Things
- If you can correlate the IDs of people, correlations, and things
  AND
- If you can identify the interactions among those things, you
  - undermine supply chains
  - undermine negotiating power

- If you introduce verifiable identity to an at-risk population and the capability to verify gets into the wrong hands, the at risk population could be at stake.
- Different IDs w/different services w/tselected correlation; "throw-away" IDs you can't throw away
- Some RPs may not accept non-correlatble IDs.

Three way relationship
Issuer - provides the credential (token) proving that you are who you say you are
R.P. - Relying party
Proover - Agent delivering the credentials (or assertion that credentials are valid/viable to the relying party.

How to undermine correlatability?
- Intermediate the issuer and prover using a delegated credential provider.
- Intermediate the prover and the relying party using selective disclosure.
- Intermediate the issuer and relying party using a distributed ledger.

IEEE 2410 Biometric Open Protocol Standard (BOPS)

Tuesday 3C
Convener: John Callahan

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

John Callahan, Veridium CTO, described the IEEE 2410-2016 Biometric Open Protocol Standard (BOPS2) - a framework for secure biometric authentication. The presentation included use cases, background, description of the RESTful API, available client SDKs, sequence diagrams, and a Q&A session.
Slides for public download at
https://s3.amazonaws.com/dist.veridiumid.com/20170502IEEE2410BOPS.pdf

Hiring a Student with a Masters Degree in IdM

Tuesday 3D
Convener: Kaliya
Notes-taker(s): Kaliya

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

You are Hiring a Student with a Masters Degree in IdM what should they know:

Yoti was in the session - Identity on a Cellphone their goal is to be ubiquitous in the UK.

Properties of Identifiers
Zookos Triangle - persistent, universal, human understandable.
https://en.wikipedia.org/wiki/Zooko%27s_triangle

What are the cultural practices of identity
amongst the target audience
do they have cel phones - download apps? free apps?
do parents allow their kids to buy stuff
What are their demographics

Technical Landscape
- what are the companies
- what do they do?
- what are the protocols

Market Analysis
Proof of Ages - clubs
How many gov issued
Photo ID
Will call tickets

Regulatory Landscape
- What legally allowed to do
- What happens in data breach
- PII where when you can hold

Agile Scrumm
Integrate a web service - Jive just got bought
Need to get integrated with enterprise - token passy thing - setup
Active directory (MSFT) or the Anti-MSFT Axis descendent of SUN LDAP

API's Interop-Middlewear

Product develop balanced with Marketing
Backlog -> get features into product and get it done in right order.

Attend SOUPS / be familar with the latest in Usable Security http://cups.cs.cmu.edu/soups/2015/index.php-

Colin Jaccino submitted the following.
——
- Identity as a Concept
The graduate should have a foundation in Identity as a concept, its role in philosophical thought, and in human self-understanding.
- Roots in Philosophy
- Roots in Language
- Roots in Psychology

- Identity: Privacy, Rights, and Ethics
The graduate should understand the grounding of privacy, rights, and ethics as they relate to identity, or by virtue of being an individual.
- What are the foundations of privacy and different notions of privacy across nations and cultures.
- Understanding of identity and privacy in legal contexts.
- Ethical questions that arise from identity and related.
- Who owns the data
- who has the right to act on information. Synthesized information?
- Implications of systematizing identity data - intended and unintended identification and correlation of attributes. erosion of anonymity. bindability of attributes. "Big Data Analytics" as an well-known example of correlation, and discussion of its desirability. "Minority Report" scenario and its implications

- Foundations in Security for stewards of organizations
- Easy enough to borrow from CISSP curriculum as a surface level overview
- Enrich with philosophical topics of identity in organizations. What types of things must be identified. Evolving organizations rely more and more on outside parties and partners; how does impact organization's identity programs

- Identity and association. Membership into groups. Deprecation of identity when a group is a proxy. When is this desired, undesired?

Enterprise Identity
Key aspects of enterprise identity systems
- Identity Management as a data lifecycle topic. Discussion of identity and data lifecycle.
- Access Management as a security control employing Identity data and Authorization
- Authorization Management. what do we authorize? How do we manage this? Problems in authorization management: with a diversity of applications and resources that were not designed to be managed together, how do organizations deal with managing authorizations across the enterprise?
- Audit: What is it? Needs that are met through audit.
- What records do we keep?
- Challenges to audit?
- Role management. What happens when a role changes? How does this impact the data about the person, authorizations for that person? How to ensure role separation and division of authorization to preempt conflicts of interest. Conspiracy and how to manage it.
- Standards and Compliance regimes: What are the sources of policy, how is it enforced, and how is it assured?
- Data and Attribute management, challenges in diverse application environments
- Federation: Extending organizational identity services to third parties for cross-organizational service delivery.

- Crypto Services
- Integration Services
- Organizational challenges with “Legacy"
- What does an identity team do?
- Near-term challenges for enterprises. GDPR, changing obligations to individuals, regulatory bodies.

Internet and Digital Identity
Use cases differentiating Internet and Digital Identity
History of Digital Identity
Key Organizations contributing to digital and Internet identity
Evolution of the online ID:
- Local Network Access Identifier
- Online Services Identity
- Early Internet and email
- World Wide Web and Web 1.0
- Web 2.0 and cross-site identity
- Highlight on Microsoft (Passport, etc) Google, Facebook, and other commercial online identities
- OpenID, OAuth, OpenID Connect, and adoption
- Current state of Internet Identity, Problems solved, Current Challenges, near-term advances.

Frontiers In Digital Identity
(A sampling of IIW topics and themes)
- Rootless Identity
- Addressing the imbalance between individual users and platform owners.
- and so on

Identity and Data in Life, Government, and Business
Identification of users, stakeholders, and constituents is not new. Many ways of identifying parties exist today, and are deeply entrenched.

- What is a background check? Have you done one on yourself?
- Have you googled yourself?
- Government ID
  - What IDs do we have?
    - Citizen IDs SSN, Passport, (TSA Precheck)? E
    - Employment Ids: Enlisted person ID? Government employees? Clearance levels (and associated ID)
    - Organization IDs: EIN, Tax IDs, etc
  - Challenges to standardization for citizens
- IDs in Enterprises. Employee IDs.
- IDs in commerce and public life:

Phone number? (Mobile telco thinks this is your Identifier. Lobbies for this to stay entrenched as customer primary ID in standards)

Financial IDs: Bank account #, Credit Card #. As with telco, financial institutions want to view identity through this prism.

Institutions with an inherent interest in a set of IDs anchor to identification methods that serve their strategic interests. Student should understand these organizations' (problem of legacy uplift, protection

of marketplace relevance), and the problems of these positions (not serving the public interest, creating technical obstacles to overall progress solving other problems).

- ***IDs in systems*.** We identify lots of things, including people. When we do this, we represent a real (unique?) thing with a unique ID, enabling us to make that real thing the target of digital attribution, association, processes, etc. We then apply changes in the real world to reflect changes made against the identifier. We move to/from your bank account, we make a phone call to you using your phone ID. These systems don't have to be digital, though digital is becoming assumed. An ID is stronger than a name, but we used to use names when unambiguous…
- A discussion of data flows a knowledgeable identity person should know:
- Types of data and terms
- Personally-identifying Information (PII)
- Customer Private Network Information (CPNI)
- Intrinsic information (DNA? Fingerprint)
- Health information
- Financial
- What info is out there? Is your purchasing history collected? Aggregated? How is it used?
- Reputation and Credit?
- Activity information, Location Information
- Agreements, Relationships, Associations
- What decisions are others making about what they know about us?
- Whether to offer a loan?
- Whether to make an offer? Offer a coupon? Provide a discount?
- Whether to grant or deny membership
.. Maybe someone has structured this well..

Identity: Best Practices for The Layman
- Managing your:
IDs. When to create. When to link
Credentials and Passwords
- Managing Trust
- Spotting when information collection is happening. Understanding what you are trading.
- How to lead the public toward better habits
- Teaching, training, and communicating about Identity within organizations.
- Identity Fraud, ID fraud protection, and response to fraud.

<u>Identity-related topics (electives?)</u>
- Cryptography
- Authentication, methods, challenges, and the future
- Emerging: Blockchain
- Enterprise ID Foundations: LDAP/Directories, Databases, Kerberos, 2-factor ID tokens, enterprise password recovery, etc etc
- Reputation, Trust, frameworks
- Privacy Law
- Identity and System Integration (APIs, common workflows, managing confidentiality in integration)
- Issues of Identity and IOT
- Technical competencies required for contributing to Identity Innovation. API development, document definition, what is an ontology, etc etc

Code of ethics for the identity professional.

OpenID Connect Account Porting Overview

Tuesday 3G
Convener: John Bradley, Bjorn Hjelm
Notes-taker(s): Bjorn

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

OpenID Connect Account Porting specification available at http://openid.net/specs/openid-connect-account-porting-1_0.html.

Hybrid Personal Cloud

Tuesday 3H
Convener: Dave Sanford
Notes-taker(s): Dave Sanford

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

Dave Sanford sketched on the white board and discussed the ideal enterprise model for 'hybrid cloud'; where systems are completely created by code/scripts (and data needed by that code/scripts) which is located on a different system than the one created by it. Another requirement of this model is for all of these system generating information (code, scripts, data) to be under version control, which enables roll-back etc. This creates a high level of control, autonomy and visibility for systems created and managed this way. In particular, they can be deployed in the cloud, on-premise, on new hardware on premise - with the push of a button. Horizontal scaling and avoidance of hardware and/or cloud service provider lock in becomes relatively easy. Disaster recovery comes for free. Dave indicated that his 'vision' of personal cloud would follow the same model - avoiding IoT hardware vendor lock-in, unknowable information sent by home devices to cloud vendors, etc.

Phil Windley talked about the fact that this model is hard, unless you have architectural assumptions that are shared with a larger community and indicated that this was one of the benefits of the picos (persistent compute objects). Phil also talked about the AWS 'Green Grass' model for IoT and how the corresponding System Development Kit (SDK) and corresponding 'device shadows' will allow API creating and loosely couple architecture for either accessing AWS services (e.g. Alexa application) or custom code behind a well defined API.

Dave talked about using the 'strangler' architectural pattern used to transform monolithic applications into microservices to use and interoperate with proprietary IoT device software components while maintaining the ability to replace or migrate away from them if appropriate.

Intro to Fast Fed

Tuesday 4A
Convener: Darin McAdams
Notes-taker(s): Darin McAdams

Tags for the session - technology discussed/ideas considered:

#FastFed

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

FastFed is a new proposed standard to make federation easier. A document was presented which discusses the motivations and proposed solution.

The document is available at: http://lists.openid.net/pipermail/openid-specs-fastfed/attachments/20170430/ce22951d/attachment-0001.pdf

Intent in Open Source

Tuesday 4C
Convener: Rafael Rocco Salles
Notes-taker(s): Rafael

Tags:

Intent, open source, governance, strategy

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

The session's main objective was to discuss the use of a manifest schema to declare intentions of OSS projects and identify the policies and considerations that were already in use by individuals, enterprises in order to engage with the projects.

The group managed to 'set the stage' in terms that showed the gaps and misconceptions of third parties hindering effective collaboration.

Linux Foundation is working on core principles to support OSS and the group extended this to an ethical level in a few domains such as health and finance.

10 Foot Platforms – Device Pairing

Tuesday 4D
Convener: Jason Richey
Notes-taker(s): Jason Richey

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

I delivered a presentation (https://docs.google.com/presentation/d/1KBKaLHTE12ZTurIVnjZ10VAVwfTMUmGLR-xZTYOuNU8/) on the topic, and then we had an open talk about where the current "best practice" solution is insufficient.

The discussion led down the path of using agents for logging a user in to the devices rather than having them log in directly.

The Agent itself could be an Amazon/Google/Custom device, or could even be built into the TV itself. Basically, there is a need for better support before the ultimate flow can be supported reliably.

AI/DAO/Identity

Tuesday 4E
Convener: Trent McConaghy
Notes-taker(s): Heather Vescent

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

Attendees and opening remarks

- convener, host, want to know how people are thinking about DAOs and AI
- Jon
- Alexandra, identity is an evolving concept, as we have more computational power, how can we tie them together
- Greg k, compare notes on use cases, stretch the boundaries
- forgerock
- Laili L, use cases
- Dave H
- Aaron S
- Francisco C
- Ruben, using AI to make sense of the what the user wants to do, to rethink the DAO or corporations, how compromised of individuals.
- Paul Madson
- Kaliya Y, get worried about the hand waving in this realm, b/c we still need human beings to do people and processes and looking each other in the eye.
- Dan Finlay, dealing with identity and blockchain
- Laurie Way, new to space and learn what are DAOs

- Abil Y
- David
- Heather Vescent
- Shri D, intrigued, PM at pivotal, building open source identity server,
- Will, I saw AI, used to work with Sri, Automatic, AI, Autonomous vehicle technology
- Intersection with cyber physical systems

Notes

- What are ways that identity can help AI/DAO systems or visa versa?
- Blockchains encourage data sharing & decentralized.
- Identity, claim of copyright,
- Am AI that knows all the data that I have, and who to show. To act on my behalf. Running on a data hub. And source how to run it on your own data container.
- AI is inspectable and you build trust
- Issue with the auditable aspects of the AI, how am I able to audit it?
- Different global regulations
- Health dashboard where you can crunch your personal health data and compare with other anonymous data to suggest health changes based on data analysis of self data and greater anonymized data.
- We are not used to or read for a world that is smart but not conscious.
- I might know people who trust the algos and I can choose the best algos. Software is built from people (Like IFTTT).

JLINC Deep Dive

Tuesday 4F
Convener: Jim Fournier
Notes-taker(s): Colin Jaccino

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

Personal data solution for enterprise under GDPR.
Requirements

1. Transparent Consent
2. Data use notification
3. data rectification
4. data portability
5. right to be deleted
6. user control over 3rd party data sharing

JLINC - a platform on a new protocol layer for user data control and management

“Intent Casting”

- “r3 banking consortium ledger”

End-to-end Encrypted Data Sharing for Everyone

Tuesday 4G
Convener: Isaac Potoczny-Jones, Tozny ijones@tozny.com
Notes-taker(s): Isaac Potoczny-Jones

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

Developer Need

- More developers need to handle Personally Identifying Information
  - PII can mean anything from email, phone, and home address to medical info
- Everyone wants to do the right thing: Protect that data
  - Encryption is extremely effective
- Many developers even have a regulatory requirement to protect
  - Work in a semi-regulated industry? Want to get European customers?
- Developers have to do more with less time
  - Expectations for deliverables are always on the rise
- A solution can't compromise business requirements
  - Analysis and processing of data is everyone's business

Problem

- Developer tools for cryptography and security are terrible
  - "Never roll your own" is typical guidance
  - But the pre-rolled security solutions aren't available for your specific needs
- Security works best when it's built-in at the code level
  - The vast majority of vulnerabilities are developer errors
  - But most security is bolted on at the end
- There never seems to be time to do it right
  - Security is always a requirement, but developers don't worry about it until it's too late
  - The timeline for delivery is always tight

Solution Approach:

Collect and Protect

- Add a few custom tags to your HTML or mobile form
- Our client-side SDK encrypts the data and manages keys for you

Store and Control

- Data is transmitted and stored encrypted
- Our policy engine lets you configure access based on your business needs

Analyze and Empower

- SDKs to analyze data with options for no-human-in-the-loop processing!
- Easy templates to add user visibility and opt-in/opt-out rules for users

Picos Everywhere

Tuesday 4H
Convener: Bruce Conrad

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

Picos are persistent compute objects. They allow us to restructure data, moving it from a manufacturer silo and giving control of it to a consumer. Both consumer and manufacturer benefit. There was much discussion about this.

Doc Searls described the buy/use cycle as viewed by a manufacturer, mostly "buy" with very little concern about "use", and as viewed by a consumer, as very little time spent in "buy" but a whole lot in "use". The information produced during use of a product could be extremely valuable to a manufacturer, resulting in improvements enjoyed by both manufacturer and consumer.

D.S. and Jimmy Pasquale both had "square tag" QR codes attached to their backpacks, and J.P. also has one on his snowmobile. When he scans it, he is given access to maintenance history, etc. When someone else scans it, they are told, "if you are scanning this I must be under it. call 911." When D.S. scans the QR code on his backpack, he is given access to his relationship with the manufacturer, but if someone else scans it, it is assumed to be lost and contact information would be given to the finder so that it can be returned.

Talk turned from these passive things, which are represented by a pico in the cloud, identified by the QR code, to devices which can communicate directly. Phil Windley spoke of his connected car project, join fuse, and there was much discussion of the role that picos can play for vehicles. J.P. spoke of an aged relative whose vehicle's location could be tracked. We spoke of a pico being created when a car began manufacture, and ownership of that pico transferring with it when sold, maintaining all its history. When sold as a used car to a new owner, the pico could be transferred, but without trip and other confidential information, leaving maintenance and other information intact.

P.W. diagrammed the relationships among a drug manufacturer, a pharmacy, batches of pills, pill bottles sold to customers, with each party represented by a pico. When the manufacturer detected a bad batch, its pico would notify the batch pico, which would notify the pharmacy pico, which would notify the bottle pico, which would be able to notify the end consumer. All because of the relationships among the parties.

Token Binding – Proof-of-Possession for cookies, ID Tokens, JWTs & OAuth Tokens

Tuesday 5A
Convener: Brian Campbell
Notes-taker(s): Brian Campbell

Tags for the session - technology discussed/ideas considered:

Token Binding, TLS, Proof-of-Possession, HoK, OpenID Connect, OAuth, cookies, HTTPS, etc.

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

The session was an introduction to Token Binding, which is a soon to be set of RFCs that enable long-lived bindings to client/browser generated asymmetric keys that span multiple TLS connections. Cookies and other security tokens can be cryptographically bound to such a client key via the TLS layer, preventing token export and replay attacks.

Some additional resources (draft specs at this time):

Token Binding:
https://tools.ietf.org/html/draft-ietf-tokbind-https
https://tools.ietf.org/html/draft-ietf-tokbind-protocol
https://tools.ietf.org/html/draft-ietf-tokbind-negotiation

Token Binding Application in OpenID Connect:
http://openid.net/specs/openid-connect-token-bound-authentication-1_0.html

Token Binding Application in OAuth:
https://tools.ietf.org/html/draft-ietf-oauth-token-binding

Why Isn't IIW Wiki Secure?

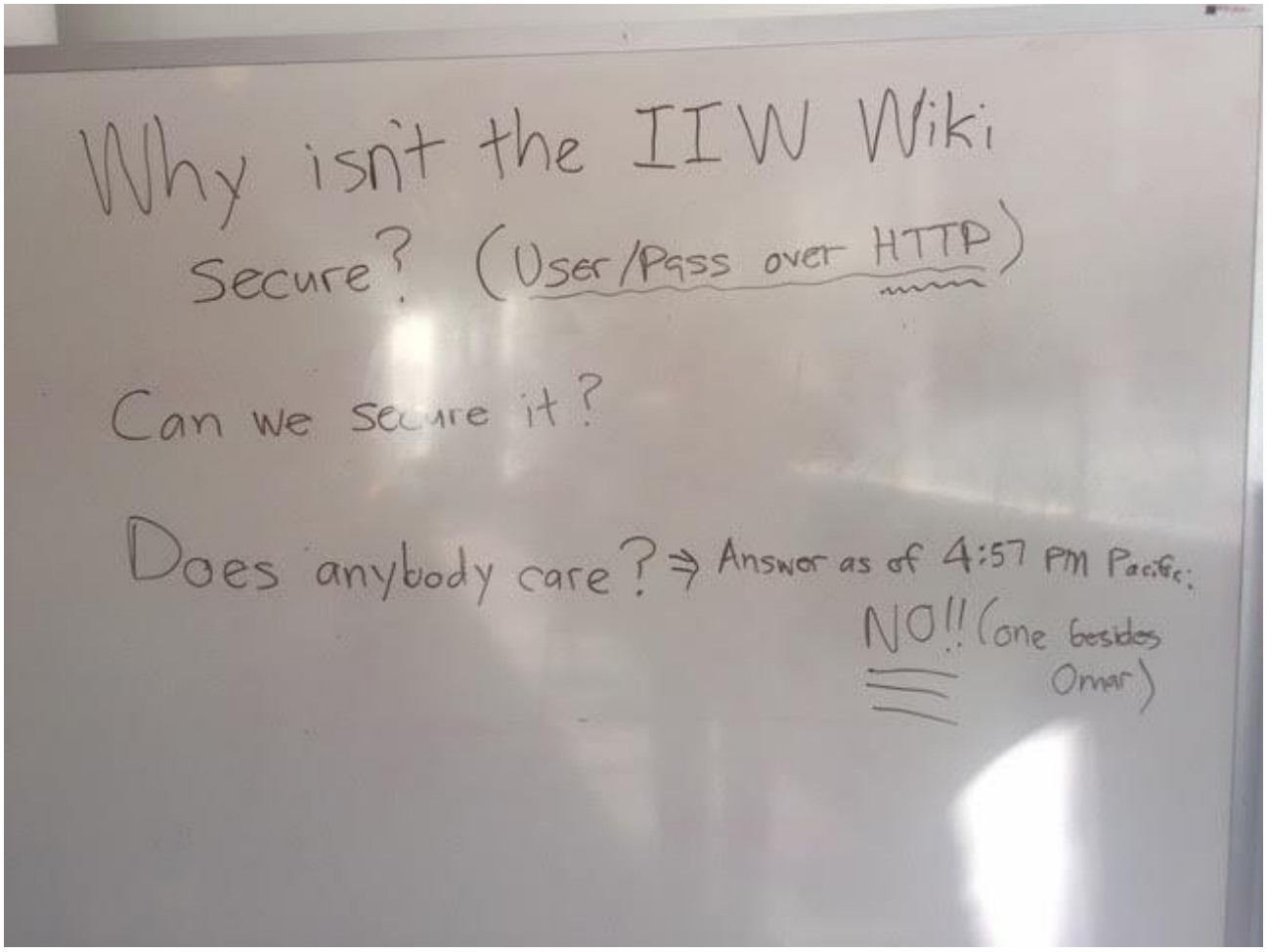
Tuesday 5C
Convener: Omar Shafie
Notes-taker(s): Omar Shafie

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

Because no one showed up, I did not have anyone to discuss my ideas with, but my basic ideas as I communicated to Heidi / Phil / Doc before the event via "Contact the Organizers" were the following: (1) Use Let's Encrypt (https://letsencrypt.org/) to provide free, automated, server-side TLS certificates

(2) And/or use Cloudflare (https://www.cloudflare.com/ - protects one domain for free), which could also help with load sharing / distribution
(3) Review password implementation to make sure passwords are uniquely salted and adaptively hashed with appropriate work factors (PBKDF2, bcrypt, etc.)
(4) Review software (OS, web server, database software, application software) used to make sure it's up-to-date to guard against well-known security vulnerabilities

During my summary comments at the end of the day, I think Phil and Kaliya suggested that IIW could consider moving the Wiki platform to a place that already provides some of the basic security features.



HashD: IO Protocol Web of Trust + Blockchain + Proof of Work + IPFS

Tuesday 5D
Convener: Harrison Stahl
Notes-taker(s): Harrison Stahl

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

Discussed the main concepts from the whitepaper. Discussed defeating Sybil attacks and fraud networks.
https://hashd.in/hashd-in-draft0/

What is Sovrin

Tuesday 5F
Convener: Phil Windley

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

Information about Sovrin can be found here:

http://www.windley.com/archives/2017/05/hyperledger_welcomes_project_indy.shtml

Intuition, Identity, and the Internet

Tuesday 5G
Convener: Sharon Franquemont
Notes-taker(s): Sharon

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

1) Intuition Definition: intueri (Latin), to know all at once
2) Intuit, *verb,* rare use of verb form rather than noun whose constant use relegates intuition to something that understand rather than an action to take. Please consider using or at least pondering, using the verb:
    a. "I i*ntuit* that this is…(the best course of action, decision, etc)"
    b. "To what degree am I *intuiting* this answer?"

Topics Addressed and some not touched on due to time and conversation:

- **Definition** discussion. To add or not to add 'without the use of logic or reason' to definition
    - We are embedded already in an information field
    - Field has unique properties, e.g. time/space freedom, copious use of pre-verbal language such as symbols, rich nourishment of creativity, pattern recognition, vision

- Some professionals exploring space distribution concepts rather than time in their identity work

- **Language** considerations: You won't be respected in engineering or tech communities if you attribute a proposed project or product to intuitive insights
  - Solutions can arise before you know how you got there
  - Use of language…my gut or my heart tells me, not sure exactly why I think this, but…a sense we might explore this possibility
  - Importance of integrating logic and intuition
  - Distortions of intuition due to projections from the past or wishful thinking of the future. Be present. Be here now.
  - Question: Is your logic always right? Why ask more of intuition than we do of logic
  - Comfort with unknown:
    - Dancing with probability
    - Importance of not solidifying intuitive answers as they are often like a moving field
  - What are intuitive identifiers in a sea of information

- **Brain Intelligence/IQ Definitions:** With internet information, brain is no longer viewed and experienced primarily as a good or bad container, e.g. I.Q. often determined by container's ability to spit out storage

- NOW: Brain needs to discerner of what is of most value in a sea of information.
  - Asking right question, discerning what is relevant
- Role of intention and passion in accessing intuition
  - ***Intention***, laser like purpose focuses your intuition and is vital:
    - Importance of intention and curiosity, e.g. as a child Einstein's favorite game was to imagine himself jumping on a light wave and riding out to time
  - ***Passion*****,** tap into passion for work (or whatever), provides energy that fuels your intuition that your intention invites intuition in, intuition active aliveness, energy that fuels intuition
    - Want to invest more in your intuitive knowing=feel deeper your connection, love and dedication for your field or inquiry
  - **Passion** and **Intention** unite heart and head for enhanced intuition
  - Humanity is outsourcing information to internet
    - What skill base will humans outsource next, empathy or compassion skills?

- **Identity, Collaboative intuiton, and Field Identity**
  - Multiple levels of identity, more than one level of identity
    - Human dignity preserved in identity issues
- Collaborative intuition/Field Identity
  - Shift from ego/self identity to team/group of individuals to experience of field identity
  - Teams come alive 'in the zone' resulting in creativity and innovation
  - Shared information field = not necessary to know everything as individual because knowledge needed is held by someone, something, some experience in or relevant to the shared field
  - Shared information field exists
- Is energy behind field identity, shared spirituality, or a shared spirit
- Importance of consciousness to human evolution

Closing Poem:

The Clear Bead by Rumi

The clear bead in the center changes everything.
There are no edges to my loving now.
I've heard it said that there is a window that opens from one mind to another
But if there is no wall, there's no need for fitting the window or the latch.

Simple Practice for 1 Week (Didn't get to this, want to share with community)

- Evening:
    1. Make To Do list 1 to 8 activities for next day
    2. Prioritize activities
    3. Go to sleep
- Morning work:
    1. Review your list
    2. Identify one thing that attracts you, excites you, and/or makes your heart happy. Should be something that doesn't take too much time or something that you can at least begin on
    3. **Act FIRST** on your chosen To Do
    4. When you finish, enjoy a few quiet moments
    5. Return to your prioritized To Do list
- Evening:
    1. Repeat morning and evening processes every day for 1 week
    2. At the end of 1 week:
        - Evaluate the results of having acted FIRST on something that attracts you or excites you.
        - Intuition travels on, thrives in a place of passion, attraction, excites

Recommendations arising out of our dialogue:

De Landa, Manuel

Manuel De Landa European Graduate School Lectures
The Materialist Theory of Language
History of Cities
War in the Age of Intelligent Machines
Error! Hyperlink reference not valid.
Social Organization and Philosophy

Gaeber, David, *Debt, The First 5000 Years* (role of

Morley, Barry, *Beyond Consensus : Salvaging the Meaning of the Meeting* (Collective wisdom)

O' Loaire, Sean *Spirits in Spacesuits*

Recommended Books and Articles:

Intuition Books**:**

Franquemont, Sharon, *You Already Know What To Do* (Self-Help, old addition available Amazon, new addition in late 2018)

Franquemont, Sharon, *Do It Yourself Intuition,* (like intuition for dummies, new addition late 2017 or 2018)

Franquemont, Sharon, *Intuition: Your Electric Self* (6 hour audio training program published by Sounds True)

Gladwell, Malcom (Author, well researched book about immediate insights) *Blink: The Power of Thinking Without Thinking*

Radin, Dean (Einstein of psi or parapsychology research), *Entangled Minds: Extrasensory Experiences in Quantum Reality; The Conscious Universe*

Sadler-Smith, Eugene, (Professor, :Organizational Behavior, Scientific exploration of intuition and its application) *Inside Intuition (2008)*, *The Intuitive Mind (2010)*
Schon, Donald A., *The Reflective Practioner* (about just in time and in action learning)
Vaughan, Frances, *Awakening Intuition,* (old, but excellent intuition guide for therapists and healthcare professionals.

Beyond OAuth2: End to End Microservice security

Tuesday 5H
Convener: Will Tran
Notes-taker(s): Will Tran

Tags for the session - technology discussed/ideas considered:

JOSE, JWT, JWS, JWE, OAuth2, Token Exchange, Service Registry, Microservices, Chain of Custody

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

Video

https://www.youtube.com/watch?v=G7A6ftCbVQY

Slides

https://docs.google.com/presentation/d/1gmMlvBW8JNGGo0rY_CnMt6qRYGCGVfQCvevkxVYhXWs/edit?usp=sharing

Feedback

Whether we see more of this solution or not entirely depends on feedback from the community. Please direct any feedback, both about the presentation, the ideas, or the solution, through github issues on the repo linked below. You can also email me.

The Code

https://github.com/william-tran/microservice-security-jose

Questions After the Talk

Isn't having to specify a policy against an entire call stack breaking encapsulation? It feels against the spirit of micro services.

In my demo I was very specific in the policies, and I neglected to show you the case where "Other than needing to know that the request came through the front door 'Shop', I don't care." Here's such a policy:

```
suppliers:
 policy:
  for-each-of-the-following:
  - enforce-the-first-matching-rule:
    - tokens-that:
       have-operation:
         equal-to: resupply
      must:
       come-from:
       - any-number-of-apps: true
       - app-name:
          equal-to: shop
```

The idea here is that you should be able to specify a policy that enforces only the things you really care about.

Can I use something other than UAA as the Authorization Server (AS)?

Absolutely. The most important property that underpins this whole scheme actually lies in your edge application. Let's consider two scenarios, the first one where the client is a web application where the token is stored in server side session, as I describe in my talk. The second scenario, one that I didn't illustrate in my talk, is where the client is a mobile app or browser based JS app. In this second scenario the client is a non-confidential client, and the user's token can be used to invoke the edge service directly.

In the first scenario, the browser can invoke the web application through an authenticated session, where the session identifier (eg JSESSIONID cookie) can be seen as a sort of "token". This JSESSIONID never gets propagated downstream. The token from the AS is stored in the server side session and contains the claims statelessly eg as a JWT, or statefully as an opaque token. Whether the AS token is a JWT or not doesn't matter, what does matter is that it cannot be used on its own to invoke any service, either downstream, or to be replayed back onto the web application. This can't be allowed because this token is supposed to be reused, but only as a way to determine what the AS says the user is allowed to do. Downstream services cannot take the AS's token and replay it, on it's own, to any other component. In the second scenario, a non-confidential client (eg mobile app or SPA) gets a token from the AS and invokes a service with it. Because the service can be invoked with this token, it cannot propagate it downstream, otherwise downstream services can use it to re-invoke that service. The user's claims still need to be propagated however, because downstream services need to know things about the

user. In this case, the service at the edge can either generate and sign its own assertion about the user, or exchange the AS token it received for an assertion signed by the AS. In either case, this user assertion cannot be used to invoke any service on its own, or be used to derive a token that can be used to invoke any service directly.
This is the situation I talk about in https://github.com/william-tran/microservice-security-jose/issues/1. In the descriptions above, UAA doesn't give you anything special over any other AS that helps with this. You just need to be careful about how services can be invoked, and that the thing (eg token, session ID) used to invoke a service, either at your edge or anywhere downstream, is never propagated.

How does the authorization server and the service registry authenticate clients? Can we use client certificates?

In UAA, clients can authenticate with the UAA via client_id, and in the case of confidential clients, a client_secret, via HTTP Basic. Client registration in UAA is done by an actor (user or system) with the permission to register clients, the registration contains the client_id+client_secret. Services must authenticate with the service registry to register their public key in a trusted way. In Spring Cloud Services (SCS), services authenticate with Eureka using an OAuth token obtained from UAA via client credentials grant. This is the value add that SCS provides on top of the OSS Eureka server. I mention in my talk other service registries like Zookeper and Consul that include their own authentication mechanisms / plugins out of the box, but I personally haven't used these.
I've also seen Google Service Accounts use self signed JWTs to authenticate clients, instead of client_id+client_secret. The act of registering a client in Google is done by the Devloper and they get back a private key for their app to create self signed JWTs.
You can definitely use client certificates to authenticate clients instead of OAuth tokens (and transitively, client_id+client_secret), as used in PCF and SCS. If using mutual TLS, you might not need to do the JWS wrapping step, as mutual TLS provides the non-resuable, not propagated authentication; the authorization in the form of the nested JWT tokens remains the same though.

Can we use a full PKI instead of the lightweight service registry? Or can I combine them?

Yes, if you have a PKI you can use that to provide the key material for signing. For verification, certificates can be imbedded in the JWS header itself and in that way the JWS is truly self-verifying (as long as you trust the thing that signed the certificate; that trust anchor is provided by your PKI). Embedding the certificate in the JWS header via x5c (https://tools.ietf.org/html/rfc7515#section-4.1.6) is pretty heavy size-wise, so the service registry could be used as a way for the recipient to look up the full certificate given an identifier in the JWS header like the "kid", and then cache this locally.

What happens if the central service registry is compromised?

If you are using the registry on its own without a PKI, then the entire system would be compromised. It's as if you were using a PKI and the private key for your CA were compromised.

RSA signing for JWS is expensive! You should look into HMAC.

Key exchange for the symmetric key could happen via a signed and encrpyted JWS/JWE using key material registered in the service registry, and then cache that locally for some interval. Thanks for the suggestion.

Links

Spring Cloud Services for Pivotal Cloud Foundry
http://docs.pivotal.io/spring-cloud-services/

Nimbus JOSE+JWT
https://connect2id.com/products/nimbus-jose-jwt

Here are some excellent blog posts by Prabath Siriwardena, who explains the fundamentals very well.

Securing Microservices

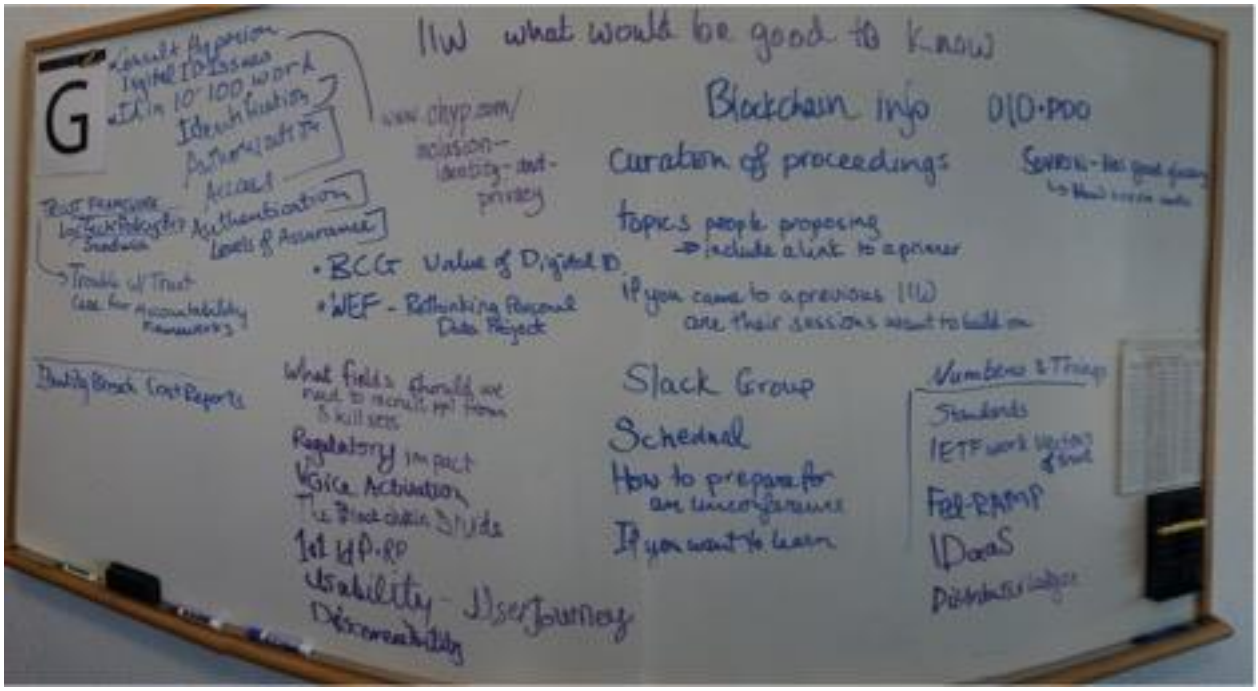
JWT, JWS and JWE for Not So Dummies!

Wednesday May 3

Women's Breakfast

Wednesday G
Convener: Kaliya
Notes-taker(s): Heather

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



DID 101

Wednesday 1A
Convener: Drummond Reed
Notes-taker(s): Andrew Hughes and Colin Jaccino

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

Notes by Dummond Reed:
Drummond Reed shared this presentation based on work funded by the U.S. Department of Homeland Security, and specifically Anil John, Program Manager for Identity and Data Privacy.
Here are a number of the questions asked and answered:

1. **Will the DID spec go to a full SDO (standard development organization)?** At some point, yes, but no SDO has been chosen yet—currently it is just a community spec. See these links:
    1. PDF version (static).
    2. Google doc version (live version accepting comments).
2. **Can anyone create a DID method spec?** Yes.
3. **Are all DID methods intended to be global in scope?** Yes and no. Yes, the DIDs under the method must be globally unique. But no in that the method spec may only address the needs of a specific community that may be relatively narrow.
4. **Will there be a registry or authority for DID method specs to ensure uniqueness?** No. The DID spec is explicit that uniqueness of DID method names will not use a centralized authority (after all, this is decentralized identity infrastructure), but will be accomplished by community consensus just like an open source project.
5. **What can be customized in a DDO (DID descriptor object) by a DID method spec?** The main thing that can be customized is the control block. Usage of DID fragments, paths, or service endpoints that is still consistent with the DID spec is also an option.
6. **What other work is now being based on DIDs?** They are the key to a number of other specs. For at list of five more specifications specifically based on DIDs, see The DID Family of Specifications.
7. **How can I get involved with continuing work on the DID spec?** Contact Drummond Reed directly at first name drummond dot last name reed at evernym dot com, or join us at the Rebooting the Web of Trust, http://www.weboftrust.info/, or the Sovrin Forum, http://forum.sovrin.org/.

See: DID (Decentralized Identifier) Data Model and Generic Syntax 1.0

Notes by Andrew Hughes

The DID spec was funded in part by a SmalL Business Research (SBIR) grant from the Dept. of Homeland Security.

DIDs are a new type of globally unique identifier
They enable internet-scale digital ID w/o centralized services.
DIDs are designed for "blockchain identity". All verified cryptographically.

Requirements were:
- Something LIKE a URN
    - That can last forever
    - With no central registry
    - Cryptographically verifiable.

DID format:
{scheme}:{namespace}:{namespace-specific identifier}
urn:uuid:ae84-d5c2-2845f922d59842-2984252ae

DID Syntax:
did:sov:234927420kabaoerha9823h;af983h;a23;9a8
scheme:method:method-specific-id

Initial DID Method specs & prefixes:
Sovrin- did:sov:
Bitcoin- did:btcr:
Ethereum uPort - did:uport:
Ethereum Consent- did:cnsnt:

The 3 purposes of DID methods:

- Specify the syntax of the method-specific identifier
- Specify any method-specific elements of the DDO
- Specify the CRUD ops on DIDs and DDOs.

{key: value} : {DID: DDO}

The DDO is what you get back from the DID.

The elements of a DDO:

- Context (link to spec)
- DID reference (to self)
- List of public keys owned by
- List of controlling DIDs (for key recovery)
- List of service endpoints (for interaction)
- Timestamps (for audit history)
- Signature (for integrity)

Question from me: Could a DDO specify an arbitrary signature recovery mechanism? To allow for rolling forward cryptography, or implementing custom multi-sig logic, beyond the scope of the spec itself?

Answer: YES! The owner and controller specs are extensible, and uPort for example already has complex smart-contract powered key recovery strategies.

Guardians: a guardian of a decentralized ID, that can later pass control over to that user. Useful in refugee camps where users don't have key signing powers, or when minors are not legally permitted to manage their own identities.

Additional notes from Colin

Interrelation between **Verifiable Claims**, **Distributed ID**, and the **W3C Web Payments** working group.

DHTs - Distributed Hash Tables

Several groups came together with the need for another type of identifier.
Drummond Reed - Trustee of Sovirin Foundation.
DID's (Decentralized Identifiers): Solving the Root Identity Problem
DID partly funded by a Small Business Innovation Research grant from US Dept of Homeland Security.
Google: Rebooting the Web of Trust Spring 2017. Find DID family of specifications.

DIDs:

- new type of globally unique identifier
- enable internet-scale digital identity without centralized registry services.
- DIDs are designed for "blockchain identity" - they are generated, registered, and verified cryptographically.

Why is this a breakthrough?

- Distributed ledgers are massively secure, scalable, and reliable.
- For digital identity, a distributed ledger can solve the "root of trust" problem: How can there be a global source of identity that everyone trusts, but isn't owned or controlled by any one company?

Work with all blockchain models:
Axes - Validation vs Axis
Access: Public/privat
Validation: Permissionless,Permissioned.

Wat do DID's look like?
URN (RFC 2141)
Examples: UUID, DOI

How do we make DID's work with *any ledger?*

DID syntax
did:sov:3k9dg356wdcj5gf2k9bw8kfg7a

Initial DID Method specs (in development as of May 3 2017):

Method	DID Prefix
Sovran	did:sov:
Bitcoin Reference:	did:btcr
Ethereal uPort	did:sport:
Ethereal Concent:	did:consent:

Three purposes of DID methods:

1. Specify the syntax of the method-specific identifier
2. Specify any method-specific elements of the DDO (DID descriptor objecT)
3. Specify the CRUD (Create, Read, Update, Delete) operations on DIDs and DDOs for the target ledger.

What is a DID?
{"Key": "Value"}
{ "DID": "DDO" }

Elements of a DDO

1. DID (self-describing)
2. 2. List of public keys (For the owner)
3. List of controlling DIDs (for key recovery)
4. List of service endpoints (for interaction)
5. Timestamps (for audit history)
6. Signature (for integrity)

DID and owner public key blocks
{ example JSON document }
Includes JSON LD (JSON Linked Data)

Spec example provides the “owner block"
“@context”
“id”
“owner”:
  “id”
  “type”
  “curve”
  “expires”
  “publicKeyBase64”
  “id”
  “type”
  “expires”
  “publicKeyPem”

Current spec draft does not define a specific type of key. But as it develops, standard key descriptions will be provided, or may become best practice or de facto standard.

Another example:
“control and service endpoint blocks

“control”: [{
  “type”: “OrControl”,
  “signer”: [
  “did:sov:21tDAKCERh95uGgKbJNHYp”,
  “did:sov:8uQhQMGzWxR8vw5P3UWH1j”
  ]
}],
“service”: {
  “opened”: “https://openid.example.com/456”,
  “xdi”: “https://xdi.example.com/123”
},

(continued) Timestamp and signature blocks
“create”: “…date…”,
“updated”: “….date..””

“Signature”: {
“type”: “RsaSignature2016”,
“created”: “….date…”,
“creator”: “did:sov:8uQhQMGzWxR8vw5P3UWH1j#key/1”,
“signatureValue”: “IOmA4oaisjdoiajsdflkjasdf=“
}
}

Discussion of JWT and JWS

What is a guardian?
A guardian manages a a DID for a Dependent
Sovrin spec will account for subordinate/child identities under the guardianship of a parent DID.

IEEE/SA and the Human SID Hackathon

Wednesday 1C
Convener: Alpesh Shah
Notes-taker(s): Alpesh Shah

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

Advancing the Human Standard Hackathon and Digital Inclusion considerations
Involved organizations - Evernym, Swirlds, iResponse, IEEE/SA, IIW

Key Points of discussion:
Refugee anonymity, Pseudonymity and Identity
Employer and credible refugee abilities validated via a track and trace mechanism while meeting the appropriate policy considerations
Event will be hosted in partnership with the IIW for Fall IIW
We will provide the use cases in advance and training links for the various platforms
Links to the platforms to be provided on the IIW site and once up, the hack microsite
Winners will be announced at Fall IIW

Outcome aim will:
1. Provide a solution that could inform a successful solution for a real problem
2. Lead to a possible repeatable framework that can be utilized across a number of similar identity challenges around the world
3. Allow greater awareness and applicability of distributed ledger technology as a means towards increased knowledge of creating realworld blockchain solutions

How to Achieve Fair Dice Rolls in Online Games

Wednesday 1G
Convener: Kazue Sako
Notes-taker(s): Tom Brown

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

Currently, in most games, the outcome of roll is determined by servers

PRNG needs a seed. Propose to generate seed collaboratively by players and server

Server's portion of seed is not disclosed (until after the game) but hashed and committed to blockchain prior to receiving contribution of seed from players

After game, server's part of the seed is disclosed

Players cannot guess the next dice roll (although server can)

Design criteria: No limit to number of dice rolls after seed creation. Players can verify the outcome of dice rolls after the game

Usability: How easy can a player choose a random seed? Most players hate to see this information.

App has a review mode to see hash function outputs. Also has "verify-dice off-mode"

Blockchain as the third party.

Discussion: third party services like random.org do not seem to be verifiable

Application Identity and Trust in Healthcare and Beyond

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

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

The group discussed primarily health care use cases for application trust and endorsement.

Summary:

The POET method where a signed JWT is used to convey a pedigree of an application is a reasonable approach with some caveats thought presented by the group:

- There must be rules and governance for how endorsing bodies (i.e. JWT signers) manage public keys. Perhaps these rules could be based on the same rules used by certificate authorities, but less stringent.
- A governing body must exists to managing all endorsers who meet this criteria.
- A uniform display for the endorsement or lack thief should be adopted. It took the browser community 7 years to come to an agreement.
- No significant difference between using x509 and JWKs for key pairs. x509 certificates could be self-signed in this use case.

Links:

https://github.com/TransparentHealth/poet
https://github.com/TransparentHealth/python-poetri
https://www.healthit.gov/facas/health-it-policy-committee/hitpc-workgroups/api-task-force
http://carinalliance.com/

How to Live with Shadow IT

Wednesday 2A
Convener: Justin
Note taker: Heather Vescent

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

Shadow IT is when IT work it done unofficially by non-IT people in a company.
It would be easier to use an official solution instead of slapping something together.
Went and got internal approval before doing a DIY solution – an identity federation server.

Companies ask, How do we prevent shadow IT?
A better question: How do we enable shadow IT in such a way that doesn't hurt us?

What culture helps and hurts us?

Shadow IT – using dropbox and github not authorized
How many used? Admit 20-40, really more like 900

Migrated corporate identities?
What do you bring to a company?
What do you take with you?

Bring your own devices is the beach head for shadow IT.
Invest in infrastructure to build auditing and anomalies detection – you can be looser, but most places won't invest in that.

Companies don't know or don't want to admit this is happening?
People are going to be sneaky about using these things.
People are more likely to be fired for not doing their job than using something unsecure. People will avoid the stick, not stop doing what you want them to stop doing.

"Ask for forgiveness, not for permission."
But **should** we encourage this attitude?

Official solutions have restrictions.
People are doing shadow IT to avoid the restrictions. But there are concerns with proprietary information.

Monitor the use of shadow IT, understand what they use it for, then pick one for a corporate standard. This is how a company figures out what to pick. People will then use the officially selected solution.

Costs for using shadow it
Cheaper for the individual (time, attention, easier, etc)

Figure out what people are doing and
Listen to what they really need

Pop-up enterprise – what we use to think of as long standing enterprise structure, is something that is more contextual and contemporary bound.
Email forwarding as opsec.

How much data really needs to be secure and classified?
Do we need full data perimeter security?

Users have a different set of values.
Feature parity? Not all choices work.
Might work great for the business, but doesn't work great for me.

Business values vs user values.

If you are going to use shadow IT,
Practice safe shadow IT
Enterprise provide security condoms.
Abstinence only vs realistic safety.

Blacklisting

What does “support” mean?
If something breaks, call us and we’ll fix it
Vs Allow – you won’t get in deep trouble,

Sign up for these things, inform corporate? But this might not always work because people in companies have different feelings about what should be permitted – anything but the blacklisted stuff vs only whitelist stuff.

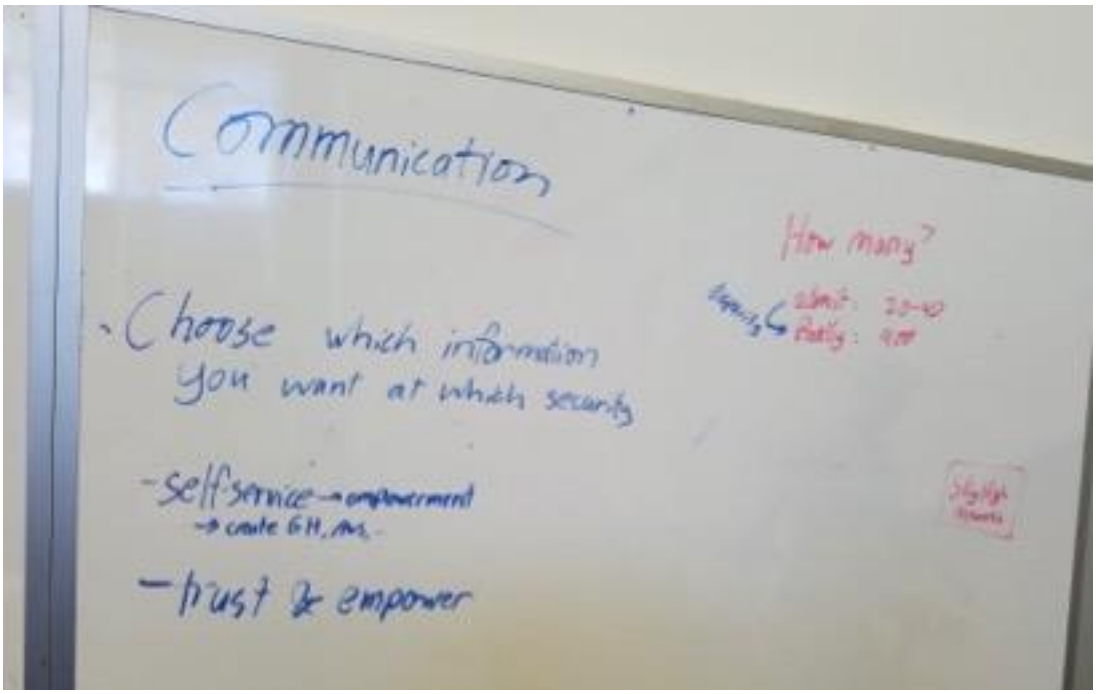
Whitelist: we support
Greylist: we allow
Blacklist: not allowed

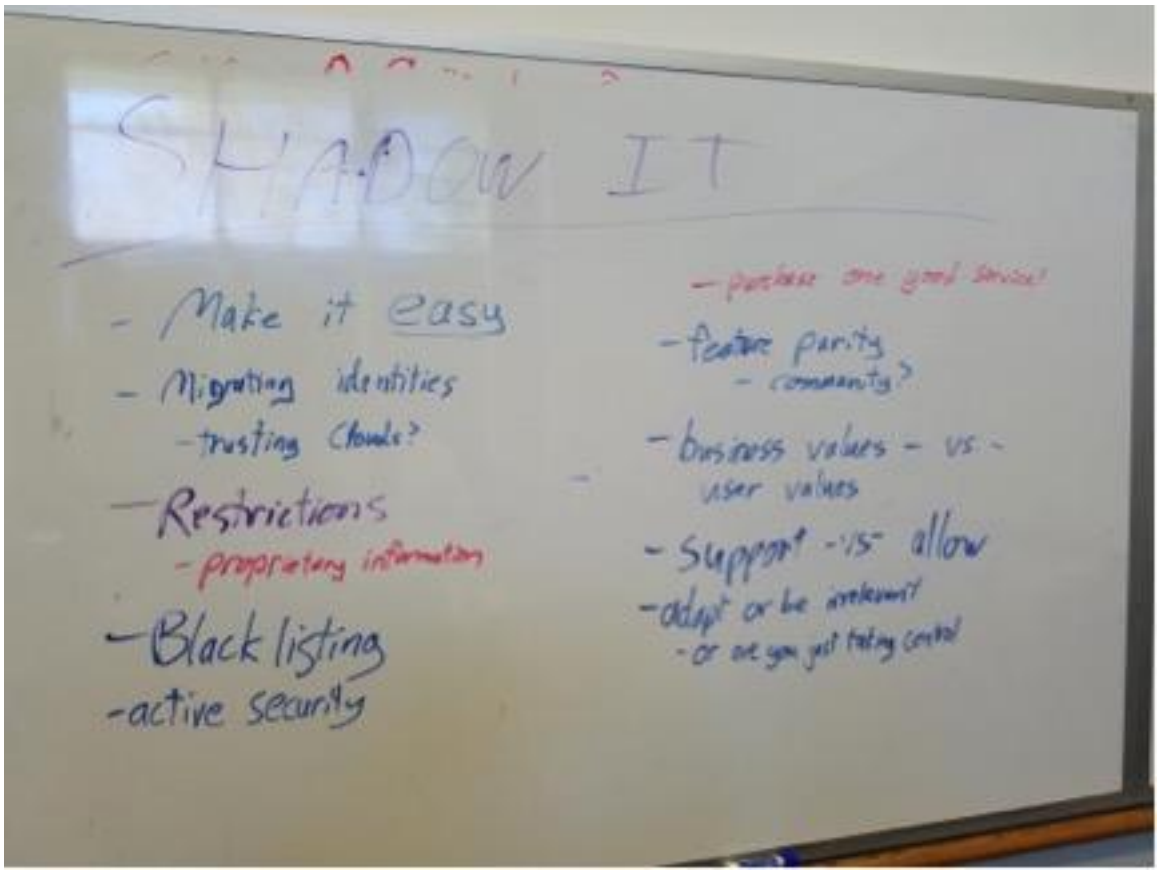
How can we allow this without freaking out the IT people?
“50 shades of greylist”

Support the people doing what they want.
Previously it was to make the technology work.
Adapt or be irrelevant.

Opt-into IT services or you build it yourself.

Empower self-service. Give a way for people to do it themself.
Active security.
Trust and empower your users not to do something.




SHADOW IT
- Make it easy
- Migrating identities
- trusting Clouds?
- Restrictions
- proprietary information
- Black listing
- active security
- feature parity
- community?
- business values - vs -
user values
- support -is- allow
- adapt or be irrelevant
- or are you just taking control

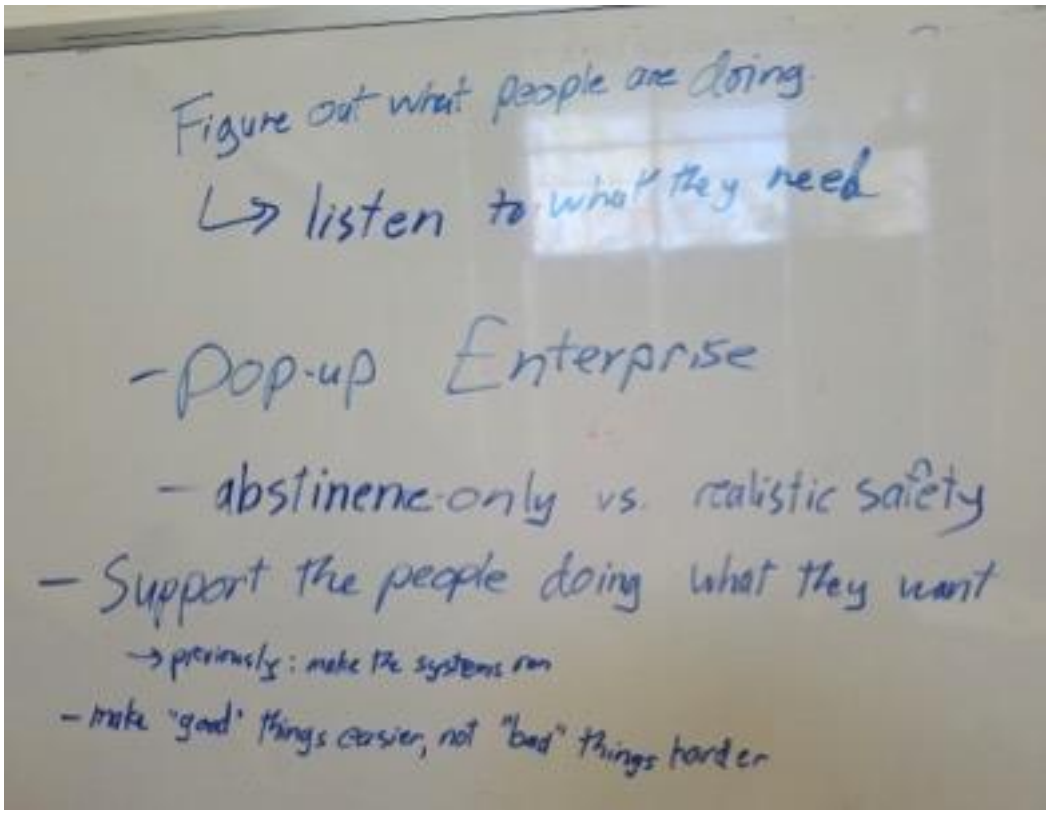


Figure out what people are doing
↳ listen to what they need
- pop-up Enterprise
- abstinence-only vs. realistic safety
- Support the people doing what they want
→ previously: make the systems run
- make "good" things easier, not "bad" things harder

Neural Science of Persuasion

Session: Tuesday 2C
Convener: Nathan Schor, nathan@rcsm.io
Notes-taker(s): Nathan Schor

Tags for the session - technology discussed/ideas considered:

neuroscience, persuasion, marketing, sales, negotiating, startups

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

More has been discovered about the brain in the last decade than in all history. The session discussed applying findings from Neural Science, Evolutionary Psychology and Behavioral Economics to improve two skills vital for commercial success – communicating persuasively and earning customer traction.

Drawing from the work of Nobel Laureate Daniel Kahneman's Thinking, Fast and Slow, Influence: Science and Practice (Robert B. Cialdini), and Start with Why (Simon Sinek), we discussed how those disciplines have much to say about why humans approach certain offers, while avoiding others.

Simon Sinek – Why His Work Matters to Startups – Sinek's seminal marketing insight defines the criterion for distinguishing messaging that earns customer's attention from those which don't, making it highly useful to startup teams.

Understanding Consideration Sets Vital for Startup Success – Like energy in physics, DNA in biology or functions in math, a Consideration Set is foundational in modern marketing. Properly fabricated, it results in another concept vital for commercial success – *Unique Selling Proposition (USP).* Far too many startups do not give these dual principles the attention they deserve.

Background On The Neural Science Classes – A one-page document describing the Influence Others meetup which applies findings from Neural Science, Evolutionary Psychology and Behavioral Economics to improve startup teams with two skills vital for their commercial success – communicating persuasively and earning customer traction.

IDPro Taxonomy - and Body of Knowledge

Wednesday 2H
Convener: Andrew Hughes
Notes-taker(s): Nathan Rowe

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

In April 2016 Kantara formally kicked off an initiative to start a professional organization for ID Pro

Over the past year Kantara has provided the technical infrastructure and support organization to move it forward

What do you think you should know & How does one get certified - Initial focus is on establishing the common ground of what you should know, what we expect to know what we expect others to know

Pledge page was established summer 2016 to survey the market to assess interest
- By end of August had 355
- Survey was sent to the group - professional certification was relatively low

From previous IIW sessions held survived what should an IDPro know and resulted in a very broad list

- Vendors
- Terchnologies
- Terms
- Coding
- Legal.Compliance
- Standards/NPO
- *Other Stuff??*

it was clear that a single definition didn't exist - Out of this a working group was created to focus on creation of a common taxonomy

At top level 4 categories were defined

- Identities
- Management
- Authentication
- Authorization

The second level of each of the top 4 categories are

- Concepts
- Regulations
- Good Practice
- Standards & Protocol

Step 1 is to define the index or full scope of what needs to be captured prior to engaging writing or getting into the details

Initial taxonomy is largely focused on enterprise IAM, it is recognized that consumer and citizen IAM are evolving too rapidly to be able to be described

How to move forward

1. Collect references and links into a single document and categories them
2. Hire experts to create the content
3. Continue to grow with new vendors, technology, and references

Looking for members to join the working group and contribute

Intro to Verifiable Claims

Wednesday 2J
Convener: John Tibbetts, Joe Andrieu, Nathan George, Drummond Reed
Notes-taker(s): John Tibbetts

Tags for the session - technology discussed/ideas considered:

Verifiable Claims

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

Verifiable Claims
Data Model Deep Dive
IIW 24
Wednesday, 10:30 AM
By John Tibbetts, Joe Andrieu, Nathan George, Drummond Reed
Deck created by Manu Sporny

Components of a Verifiable Claim

- Set of Verifiable Claims
- Digital Signature by Issuer
- Claims about Subject
- Subject Identifier
- Claim Set Metadata

Components of a Verifiable Claim

- Set of Verifiable Claims
- Digital Signature by Issuer
- Claims about Subject
- **Subject Identifier**
- Claim Set Metadata

```
{
  "id": "http://example.gov/credentials/3732",
  "type": [
    "Credential",
```

```
    "ProofOfAgeCredential"
  ],
  "issuer": "https://dmv.example.gov",
  "issued": "2010-01-01",
  "claim": {
    "id": "did:method:f36100c0-1dfb-957c-e403f8b0dbd5",
    "ageOver": 21
  },
  "signature": {
  }
}
```

Components of a Verifiable Claim

- Set of Verifiable Claims
- Digital Signature by Issuer
- **Claims about Subject**
- Subject Identifier
- Claim Set Metadata

```
{
  "id": "http://example.gov/credentials/3732",
  "type": [
    "Credential",
    "ProofOfAgeCredential"
  ],
  "issuer": "https://dmv.example.gov",
  "issued": "2010-01-01",
  "claim": {
    "id": "did:method:f36100c0-1dfb-957c-e403f8b0dbd5",
    "ageOver": 21
  },
  "signature": {
  }
}
```

Components of a Verifiable Claim

- Set of Verifiable Claims
- Digital Signature by Issuer
- Claims about Subject
- Subject Identifier
- **Claim Set Metadata**

```
{
  "id": "http://example.gov/credentials/3732",
  "type": [
    "Credential",
    "ProofOfAgeCredential"
  ],
  "issuer": "https://dmv.example.gov",
```

```
  "issued": "2010-01-01",
  "claim": {
    "id": "did:method:f36100c0-1dfb-957c-e403f8b0dbd5",
    "ageOver": 21
  },
  "signature": {
  }
}
```

Components of a Verifiable Claim

- Set of Verifiable Claims
- **Digital Signature by Issuer**
- Claims about Subject
- Subject Identifier
- Claim Set Metadata

```
{
  "id": "http://example.gov/credentials/3732",
  "type": [
    "Credential",
    "ProofOfAgeCredential"
  ],
  "issuer": "https://dmv.example.gov",
  "issued": "2010-01-01",
  "claim": {
    "id": "did:method:f36100c0-1dfb-957c-e403f8b0dbd5",
    "ageOver": 21
  },
  {
  "signature": {
    "type": "RsaSignature2016",
    "created": "2016-06-18T21:19:10Z",
    "creator": "https://dmv.va.gov/keys/1",
    "domain": "www.example.com",
    "nonce": "598c63d6",
    "signatureValue": "BavEll0/I1zpY...W3JT24="
  }
}
```

Why Linked Data?

- Global meaning for “attributes”
- Open-world assumption (say anything about anything)
- Native support for URLs (linking to other information)
- Graph-based data model aligned with the Web
- Data model natively supports querying and merging
- Maps to multiple syntaxes
- Rich data typing
- Link to external resources creating a “knowledge graph”

What is Linked Data?

- Linked Data allows resources to unambiguously refer to each other
- Statements about a Person or Claim use URLs to describe those things
- URLs are links, which can be used to find out more information about that thing.E.g.: to say a Claim is a "Credential", causes "Credential" to be resolved to "https://w3id.org/identity#Credential". Dereferencing that leads to a description of "Credential" (or will, eventually).
- JSON-LD describes statements which relate entities with each other, or describe literal attributes of that entity.
- Each statement becomes a triple in the RDF data model
- Collections of statements become a graph
- JSON-LD can be turned into triples, and triples back into JSON-LD using core algorithms

Linked Data

- Linked (Open) Data – Separate the past from the future
- RDF is about the links, not the syntax
- Use URLs as names for things
- When someone looks up a URL, provide useful information using standards
- Link to other URLs, allowing discovery of new things
- JSON-LD is an RDF format

But I Don't Care About Linked Data!

- JSON-LD is designed to be unobtrusive
- Treat it like JSON
- Most developers don't have to care - that's the goal
- We should be open to people rejecting Linked Data
- Verifiable Claims should continue to work if this happens

CTI Credentials

- Express CTI credentials via VC
- Launched by Lumina Foundation
- A global registry includes defined achievements of many types: competencies, apprenticeships, degrees, badges, certificates

Public vs Private Data

Wednesday 2K
Convener: Dan McNeece
Notes-taker(s): Dan McNeece

Tags for the session - technology discussed/ideas considered:

DataGovernance

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

Permissions to access data should be given contextually (when needed). For example, when a application needs to access a camera, permission is asked at the time it gets used.

Cameras are becoming the keyboards of the future. Much of our data is being collected without using a physical keyboard.

Be careful with third parties that share our data. We need to verify their data retention policies and make sure they fit our expectations. We should apply risk assessment questions.

It is hard to put 'property' rights on our data, like we would a house or car. Data attributes are often **shared** between people and companies rather than being exclusively private (our data) or public (everyone's data).

We need to decide what the principles are for our companies. What do we use to decide when to share data?

DKMS

Wednesday 3A
Convener: Drummond Reed
Notes-taker(s): Jin Wen

Tags for the session - technology discussed/ideas considered:

DID, DDOS, DKMS, Decentralized Key Management System

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

Note: this is an effort of DHS contract

Source: https://github.com/WebOfTrustInfo/rebooting-the-web-of-trust-spring2017

Checklist for the DKMS, please use NIST 800-130 -- a spec on how to write the spec.

http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-130.pdf

Distributed Ledger is used here

Different types of keys:
- ?
- ?
-

Revoke Rotate Replace, Recovery
Delegation:

Promise:
- the ability for individual to control the key, including recover the key -- the key

Recovery methods:
- Smart Contract for social recovery
- Recursive Recovery w/ smart contracts
- Biometric recovery
- Key escrow services
- Key recovery networks
- Hybrid / Multiple approach

HD Key
Master key and

Potential implementation:
Smart Contracts in BlockChain
- allow Access Control
- does not require master key and secrets

Additional notes from Colin Jaccino:
DIDs - a community-produced spec sponsored by DHS.

Neal John is program manager

Distributed Key Management System
How are we going to manage the keys for the distributed identifiers?
How do we do this in a privacy-respecting manner.

Sovran anticipates managing thousands of DIDs for an individual.

Defining DID is the tip of the iceberg. Management of these will be a tougher challenge.

Additional notes by Drummond Reed
Did decentralized identifiers sponsored by home land security (stir grant)

Rebooting web of trust may

Did family of specification

New identifier for web
1 did:method name(e.i div: 22 char identifier (method specific identifier)

2 ledger

method -identifier

-crud operation

3

Individuals could have thousands of key pairs

Master secret not a credential
DKMS decentralized key management (develop

NIST 800-130 spec to for writing key management spec

-Generate keys
- Key distribution :trust establishment (mainly asymmetric keys
-Types of Keys
- revoke/ rotate/ replace keys (change)
- recovery
-Delegation

Promise is in individuals controlling their keys

Master key can generate pki
Using seed with master key

New key pair for each transaction in bitcoin

How does IOT an owner would be a Guardian for IOT

Ethereum -smart contract representing an identity allows using the contract to do key management

Recovery Methods

- Smart Contract for Social Recovery (Uport recovery)
- Recursive recovery w smart contracts
- - TCS is implementing
- Biometric recovery
- Key escrow services
- Key recovery networks
- Hybrid/multiple
- Hardware recovery token

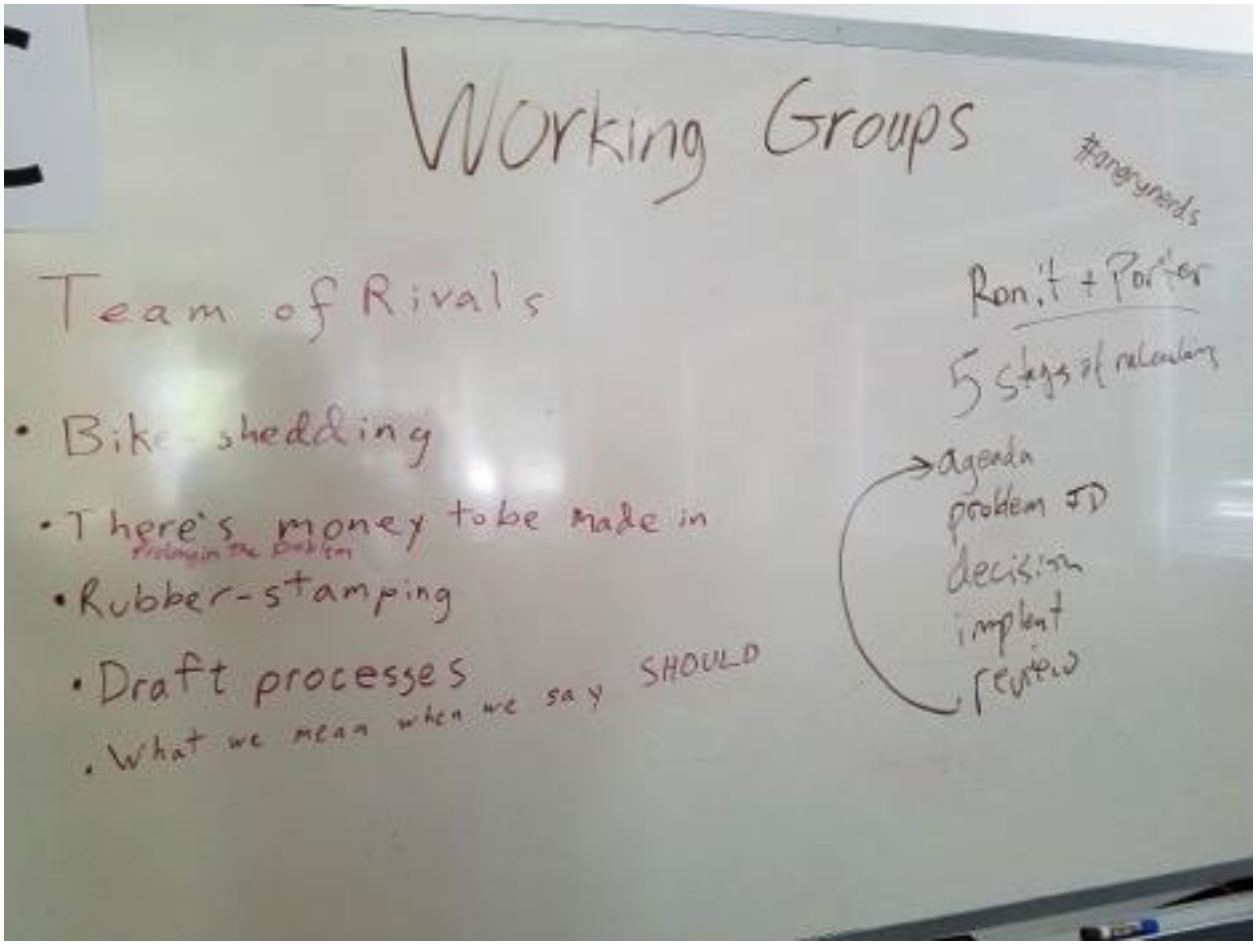
Resilience w/key recovery

Compromise & Monitoring
Fraud detection

What is it like to be part of a working group?

Wednesday 3C
Convener: Justin Richer and Sarah K Squire
Notes-taker(s): Justin

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



Storing Crypto Credentials in the Browser

Wednesday 3G
Convener: Francisco Corella
Notes-taker(s): Francisco Corella

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

We discussed methods for storing cryptographic credentials in persistent browser stotage, taking advantage of web technologies that have emerged over the last few years: the Service Worker API in conjunction with HTML5 local storage as specified by the Web Storage API, or in conjunction with the IndexedDB API and the Web Cryptography API. The security posture of each method was compared to the security provided by storing keys in smart cards, in tamper resistant hardware such as a secure element or a Trusted Platform Module (TPM), or in a Trusted Execution Environment (TEE).

Slides can be found at
https://pomcor.com/documents/KeysInBrowser.pdf

The UX of secure key management

Wednesday 3H
Convener: Dan Finlay
Notes-taker(s):

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

MetaMask is a bridge that allows you to visit the distributed web of tomorrow in your browser today. It allows you to run Ethereum dApps right in your browser without running a full Ethereum node.

MetaMask includes a secure identity vault, providing a user interface to manage your identities on different sites and sign blockchain transactions.

We're initially building MetaMask as a Chrome plugin, but eventually plan to support Firefox and beyond. If you're a developer, you can start developing with MetaMask today.
Our mission is to make Ethereum as easy to use for as many people as possible.

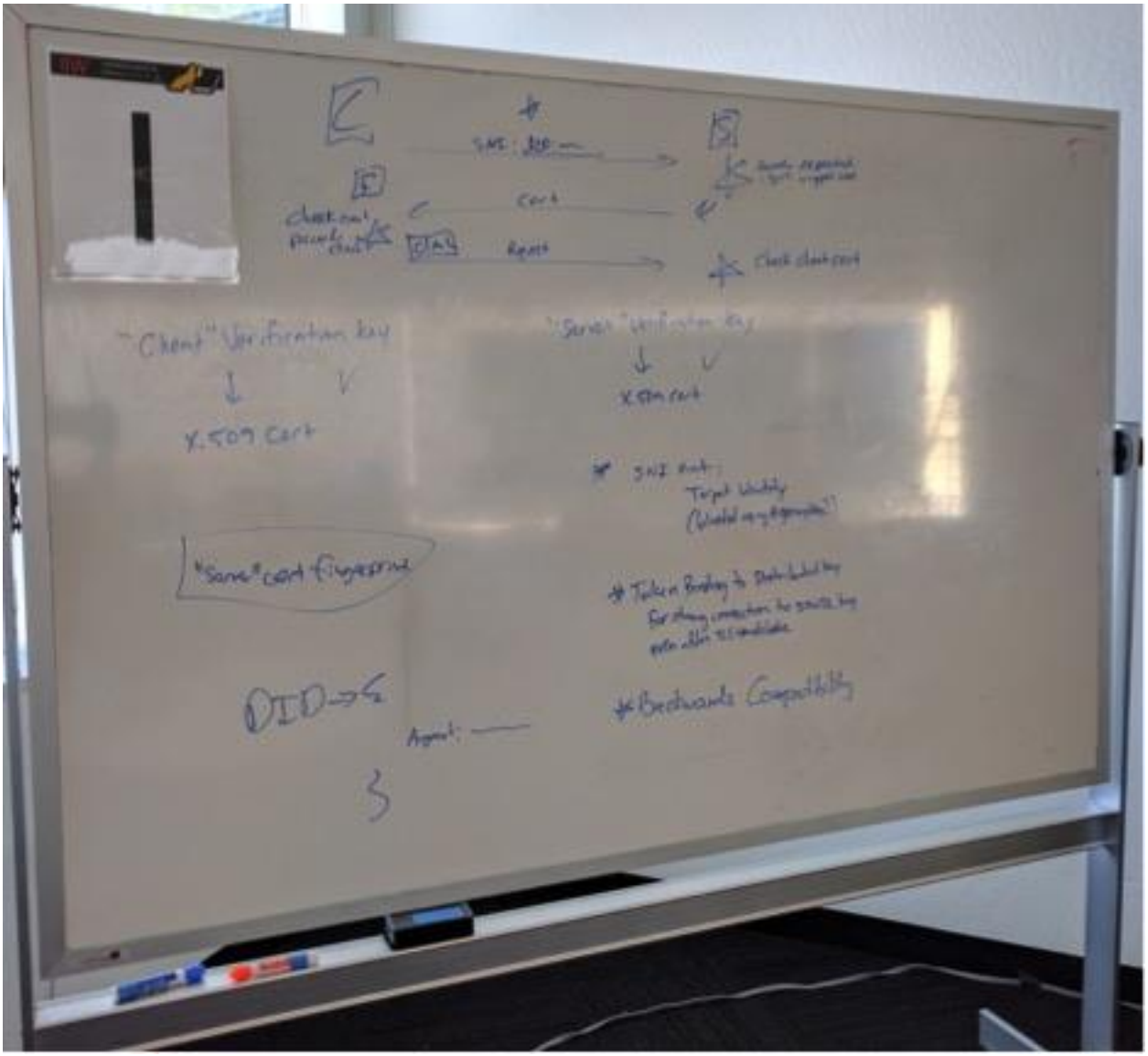
To learn more check out https://metamask.io/

DID TLS

Wednesday 3I
Convener: Nathan
Notes-taker(s): Sam

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

Mutual authentication using certificates and token bound connections with ledger-backed roots of trust.



OTTO Schema

Wednesday 3J
Convener: Michael Schwartz and Judith Bush
Notes-taker(s): Darin McAdams

Tags for the session - technology discussed/ideas considered:

OTTO, FastFed

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

Both the OTTO and FastFed working groups wish to enable groups of actors to agree on a shared schema and communicate that agreement as part of their federation metadata. This session reviewed the OTTO proposal for modeling these schemas. The vocabulary builds upon schema.org and is available at https://rawgit.com/KantaraInitiative/wg-otto/master/html/otto-vocab-1.0.html

In addition, there was general discussion about single-sign-on federation in the commercial sector and how that differs from other sectors, such as education/government. One difference is that in the educational/government sectors, there is often a need to know/trust the identity provider or service provider, know they comply with certain policies, and agree on attribute meaning. A single organization can provide many services. Certification can occur at the top-level organization and be reflected in each service they offer. The OTTO schema handles this case. The OIDC federation specification also addresses this circumstance: https://openid.net/specs/openid-connect-federation-1_0.html

The OTTO schema also enables users to describe the bindings into other protocols such as OIDC and SAML via a "sameAs" attribute. This describes the links between the different data representations.

Additional notes from Mike Schwatz

Federations like InCommon are a good place to publish schema, like what user claims (attribute) should be used to enhance interoperability.
One of the goals of the Kantara OTTO working group was to create a machine readible way to describe such supported schema.

To this end, it was decided to use JSON-LD to describe schema. Schema.org provides a useful baseline: see https://schema.org

OTTO has two current specs relevant to schema:
http://gluu.co/otto-vocab
http://gluu.co/otto-openid

In the "vocab" spec, you should look at the schema object. Other objects, like a federation or entity, can use the "supports" property to reference schema that they support.

The base schema class can be subclassed to make it more specific. For example, in the "openid" spec, we define the Scope class, which adds a property called userClaim, which links to the associated userClaim for that scope.

Another interesting challenge solved was "catagory"--for example what if you only want to get back the OpenID scopes supported by a federation. Category is a subclass of Enumeration. We patterned after https://schema.org/DayOfWeek.

Another interesting feature of OTTO schema is that we could use "sameAs" to link certain schema. For example, an OpenID Connect userclaim called "given_name" might be linked to an LDAP attribute called "givenName".

One idea that was posited was to create a spec to define SCIM schema.

Also, there was some question as to whether OTTO could be used for 1:1 sso, to perhaps align with requirements for FastFed. Maybe... not sure.

Distributed Identity

Wednesday 3K
Convener: Joe Andrieu
Notetaker: Heather Vescent

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

Distributed Identity vs Decentralized Identity

Identity substrate, where identity data accreted over actions.
Grounded in the subjective
The function of identity, when I recognize you, now I have connected other attributes to form a verson
A subjective notion of identity.

Digital identity, mechanisms to
Multi-lateral, mechanisms,
It can never be symmetric,
Receiver, perceiver.
Is this symmetrical? No.

Want this to be with permissions.

Substrate – permission to write and present the data from his substrate.
Subjective identity.

The notion of a distributed architecture – didn't require a centralized source.

Me – I give you permission to make a claim about me.
You make the claim.
I choose who I show the claim you make about me.

Personal note: we are becoming both more machine like and more human. We are splitting the two aspects of ourselves.

Legal identity. What are the criteria for a legal identity?
Nationality: the internet. Is there a non-national legal identity.

Any identity that a court will recognize.
Complicated social proofs.
You have an affidavit of identity.

- Facts
    - Legal name
    - Current address
- Legal notary

"Rigorous identity"
Using blockchain for identity creates timestamps that can be used to bootstrap identity.
We can use to bootstrap a legal identity.
It's a verifiable identity. And under some circumstances it can become a legal identity.

Kaliya's Paper: ASN.planetwork.net
Identity persistent correlated identifier.

To write to the bitcoin blockchain you have to pay a $1…
Energy use ½ gigwatt per

Digital India II

Wednesday 4A
Convener: Mei Lin Fung
Notes-taker(s): Sean W. Bohan

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

Digital India – Briefing at IIW May 3, 2013 @meilinfung

Aadhaar: from an identification project to flagbearer of Digital India, it's come a long way

Aadhaar is the largest biometrics programme in the world. What started out in 2008 as an effort to create a national identification programme, soon became the world's most powerful programme for driving inclusion. Aadhaar-linked payment systems, such as the newly launched 'AadhaarPay' and UPI, could transform the digital payments landscape in India. If you have an Aadhaar number, all you need is your 12-digit Aadhaar number, and a biometrics reader to do financial transactions. Thanks to Aadhaar, India could, in the next five years, leapfrog into a less-cash world, that no longer depends on debit and credit cards, expensive POS machines, ATMs and other such expensive hardware infrastructure. With 1.08 billion citizens already enrolled, the 'mandatory vs. voluntary' debate on Aadhaar is now mostly a thing of the past. The value proposition of Aadhaar has been strong enough

that people have voluntarily enrolled into Aadhaar across the length and breadth of India. In the next couple of years, Aadhaar will aim for universal coverage.

Delhi tops among states in Internet readiness: report

New Delhi: Delhi has emerged as the top ranked state in terms of overall Internet readiness including e-infrastructure and e-participation, overtaking last year's winner Maharashtra, according to a report titled 'Index of Internet readiness of Indian states' by Internet and Mobile Association of India (IAMAI) and Nielsen Holdings PLC, a global information and data measurement company unveiled on Wednesday. "Significantly, even within smaller states, the northeastern states ranked low in terms of overall Internet readiness. Therefore, much more needs to be done in the form of investment and infrastructure development in the region," the report said.

Bhim: India's ticket to a cashless economy

While many banks have launched UPI apps, the Bharat Interface for Money (Bhim), the common app that can be used by anyone who has a bank account with a linked mobile number, is seen as the most promising. But can Bhim really be India's ticket to a cashless economy? Our research with users (and potential users) of Bhim across four states in India suggests that it has a lot going for it, but ensuring mass adoption will require important product tweaks and a carefully executed go-to-market strategy to make the app go viral. So what exactly needs to be done?

There are five specific asks to ensure Bhim can scale.

First, make on-boarding simpler and guided; Second, quickly launch incentive schemes.; Third, drive behaviour change by targeting the right transactions. Fourth, ensure Bhim is accepted in key payment networks, especially those backed by government entities. Fifth, nudge banks to promote Bhim uptake in its existing customer base.

Bhim holds great potential to help realize India's vision of a cashless economy at the household level, and the building blocks are clearly in place. But well begun is (only) half done. Converting the digital promise of Bhim into a digital dividend for India will require a concerted effort.

The road to digital India

With the cash situation set to return to almost the same state as it was pre-8 November, I believe that there's a lot more that remains to be done if a less-cash economy is to become a reality. Here is what I think it will take: 1. Cash is not inconvenient: [Digital] has to be 10 times better, else people won't switch. Clearly, a large chunk of Indians haven't found digital payments 10 times better. 2. Switching to digital cash as a business case: if [digital] technology solves a real problem—in this case increase the earnings substantially—I bet that the users will switch to digital. 3. The government must take the lead: government offices and agencies must adopt digital payments 4. It has to be a lot more than just convenience: The one place that has been a let down for me is the failure to communicate the benefit of a digital footprint to those to whom it would make a meaningful difference. It's nice to tell the common man that going cashless will help strengthen the nation or cut down black money, but frankly, what's really in it for him?

Making 5-minute inclusive loans a reality with "India Stack", a research report with two experiments

This note captures the learnings from two proof of concept projects focused on disbursing small ticket size loans to financially underserved communities by using digital data trails as proxies for credit appraisal. Both these projects leveraged one or more layers of the India Stack, which, makes it easier

for digital pioneers to run faster, reach more people by enabling a paperless, presence-less, cashless transaction experience. Broadly, these studies provide clear evidence that the India Stack can transform the way in which financial services such as credit are made available to scores of financially underserved consumers. However, fully realizing the benefit of the India Stack requires overcoming a range of roadblocks which are regulatory, technical, operational and behavioral in nature.

The first study referred to as Project A throughout this document brought together Capital Float (marketplace/lender), Aditya Birla Finance Limited (lender) and Eko (remittance data provider). Eko merchants who carried out remittance based transactions through the Eko wallet received small ticket size loans within minutes of applying for the loan on a mobile-based app created by Capital Float. By using eKYC (for verification), eSign (for the loan agreement) and Aadhaar (for authentication). The second study (Project B), was based on the partnership between Suvidhaa and Axis bank, where Suvidhaa customers (comprising the financially underserved segment) received short-term, small ticket size loans at Suvidhaa retail outlets. Even though this was an assisted model where retailers carried out the eKYC process and eventually handed over a prepaid card (PPC) to the customer, the entire process was cashless and the customer was able to access the money within 24 hours.

Critiques and Concerns

Beyond governance by intentions

Already, [Modi's] critics are denouncing the way the demonetization, digitization, Jan Dhan Yojana and Aadhaar linkages have been pushed in the country. This is something that Modi would want to avoid at all costs in light of his national status. The question then is: Does Modi have the courage to go beyond headlines to address implementation and sustainability-related concerns? Efficient decision making and effective implementation will require Modi to go beyond governing by intent. To truly make progress, the government will need to encourage impartial impact assessment of initiatives like mandating Aadhaar for social security schemes, Digital India, Make in India and Startup India. It will also need to take a long-term approach and introspect over its stand on issues like citizen surveillance, privacy, data protection, and consumer choice and protection. A comprehensive plan of action, outlining the objective of government policy, stakeholders involved, estimated impact, defining implementation, monitoring, compliance responsibilities and fixing accountability of actors, will need to be adopted. Such plans must be formulated after efficient public consultation and taking into account the concerns of diverse groups.

^i guess there's no published plan of action and published assessments of Digital India

The impact so far: Has Jio's entry delayed Modi's Digital India goals?

The Mukesh Ambani-run firm has consistently promoted its telecom subsidiary Reliance Jio as a key driver of Digital India.Jio's impact so far has been limited to mostly increasing urban teledensity while depleting the Universal Service Obligation fund (USOF) – a government fund that is used to build rural telecom infrastructure – by about Rs 1,600 crore in the fiscal ending March 31, 2017. This depletion is largely because revenues of India's telecom industry have seen a big fall after the entry of Jio – contributions to the USOF are based on a share of total revenues. The fall in revenues therefore seriously delays the Modi government's ambitious project of providing connectivity in rural and remote areas, which is the backbone of Digital India.

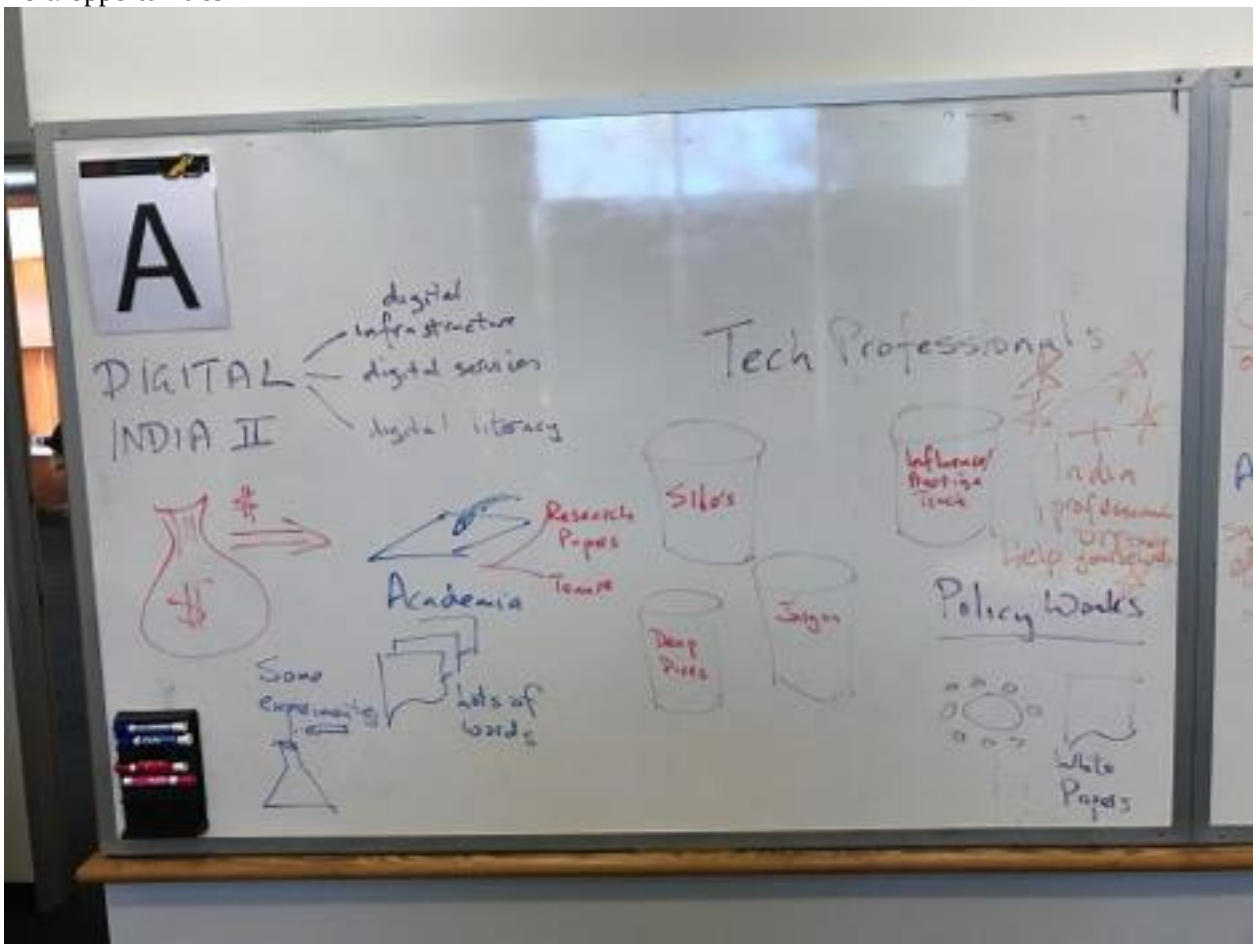
Govt's 'Digital India' push fails to help disabled

The government had in 2009 formulated a national policy for electronic accessibility; however, the

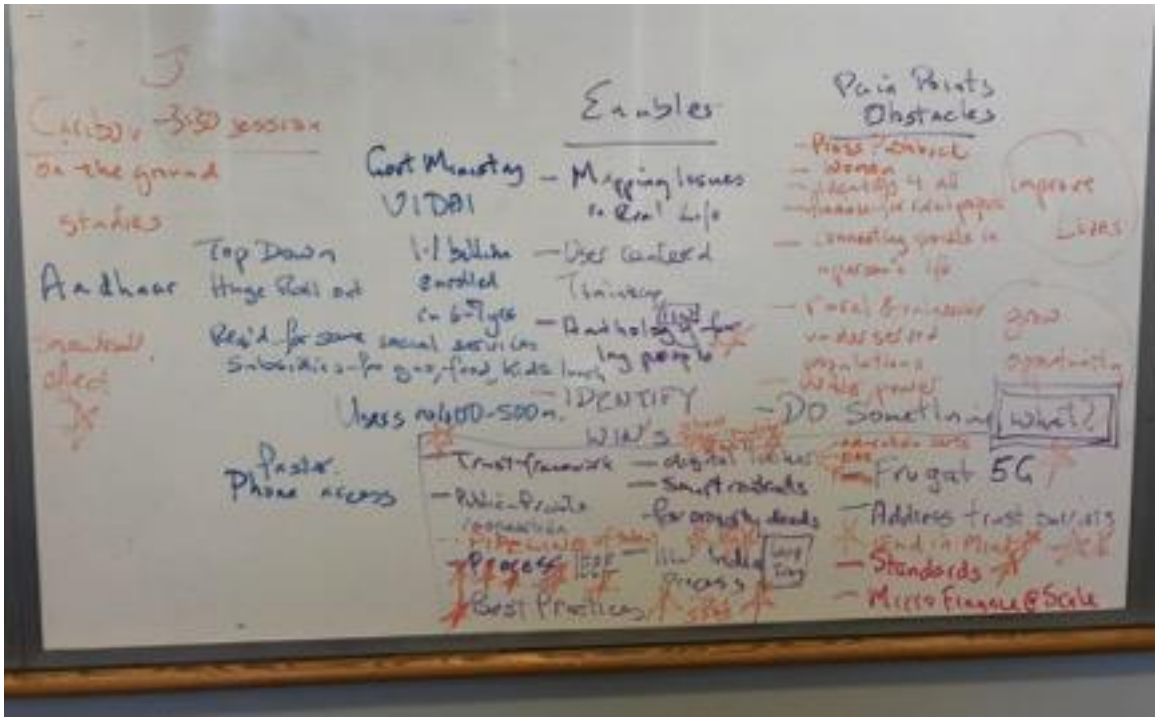
websites could never become “user friendly” for all, irrespective of their ability. Formulated in 2009, the guidelines, experts say, have not been implemented in their letter and spirit. “In our audit of “accessible” websites, we found huge gaps. Even as the government is pushing to go digital, the guidelines need to be adhered to”

meilin@peoplecentered.net Joe@andrieu.net

WHITEBOARD
Left: opportunities



Middle: Notes



Mei Lin Fung (MLF)

- digital india 2
- Follow-up to Digital India 1
- gap between what goes on in the first world and silicon valley
- perfect identity world vs. real life in india
- huge gap, reason for this discussion, what can we do to breach that gap
- digital ID rolled out to more than a billion people
- brian from caribou has been on the ground and doing studies (room J at 3:30)
- IEEE making huge effort on internet inclusion
- How can we as a community help, share knowledge
- aardhar system
- huge infrastructure, lots of bad press, successes and issues
- Infrastructure influenced by the west
- impact and how the system has been experienced by epople on the ground
- UI DAI (https://uidai.gov.in/) - govt ministry built and managing
- 1.1B people enrolled
- tremendous success story but not 1.1B using it
- gap between enrollment and use
- most have it
- for many it is something they were told to get
- technically voluntary but govt ratcheting up reqs for access (gas, food, kids lunches, cellphone in india, need bank card or aardhar card)
- 90% people dont have a bank card
- issues in deployment or access

Brian from Caribou

- formal and codified system and processes
- esp when digitized and invisible

- more important and critical for day to day
- harder it can make for people who formal systems are difficult or challenging to access
- women due to cultural issues
- disabilities - hard to access enrollment centers
- once you set down monolithic syst that is structured and all need to get onboard, takes away choice
- current user has arsenal of options - Pan card, drivers license, ration card - to engage in id transaction now being taken away (?)
- monolith that is rigid, hard to access - is a problem
- vary by states of india
- tremendous differences between states
- lot of differences, not all

Mei Lin Fung (MLF)
- IEEE has a role and see what the role could be
- reached out to architects in Modhi govt in digital india
- needs "on the ground" feel - what is useful?

ABHI
- 3 thingsdigital india is trying to do
- 1. pub priv cooperation for digital infra
- 2. digital services (but govrt hasnt like singapore)
- how does india compare
- like UK, etc.
- 3. digital literacy
- stories about rual women getting microfinance
- what is proliferation of cellphones

Lily - have to fork from dumb to smartphones
- very high
- close to 100%
- Kenya

Joe -
- we need to infect this with user-centric thinking about identity
- use open conversations

Kaliya
- thought we should have an anthology of the best canon of work from this community
- Body of Knowledge - disconnected, hard to find and really needed

Joe - it's dense, PHD dissertation,

Mei Lin Fung - network improvement communities, PCI , ways people can connect to each other

Julian - result needs to be doing something, no reason why we can't do something as well as talk about it

ABHI
- Modhi and government- people's aspirations and hopes this will be a gamechanger
- Dont want to be at par
- need to be innovative - the leapfrog, jumping a stack

Lily
- value creating, be those wins to do the leapfrog

- not immediately monetized the govt would want to take on
- eg - deeds

Alpesh

- leapfrogging incredibly important
- whats on the board - core aspect
- dont want to be a hammer looking for a nail
- worked for IEEE - look at the problem the other way
- user needs and design product that works for them as opposed to "this is the solution"
- Example: Frugal 5G
- instead of worrying about 3g or 4g, interested in leapfrogging to in 5g
- great advantages
- high degree of cost and infra required
- how do we make this work?
- IEEE - frugal5g
- does not require full infrastructure in 5g but uses current access points and community hubs for similar outcome for bandwidth
- connect the unconnected
- drive trust
- push barriers to be much lower
- working together - pulling communities together to implement successfully
- economies for local societies are important
- suggest - as we talk broad strokes
- sometimes what works well
- what is the probelm we can do something about that is sustainable?
- take advantage of low technology
- Example - power
- dont have to bring 24 hours of electricity to a place that has none - 1 to 2 hours is a gamechanger

MLF

- here are areas we are interested (left side of board)
- build credibility
- one approach
- what is doable

ABHI

- example - smart contracts and deeds using blockchains
- huge issue to get court date

Lily

- example
- do leapfrog via education
- registering do education and have credentials on the blockchain
- authentic truth - get education and grad degree, shared not just from w/in india

Kaliya

- interesting to have an IIW in India?
- bring THIS experience, the open space, community, mutual learning
- only interested in doing it there if invited and collaborative, needs to be interaction not presentation

Joes - back to leapfrog

- Rebooting Web of Trust example - what do users really want?

- what is the reframing to get them to do it?
- Idea - let us hold a leapfrog summit
- tech and political and social implications in india
- how to help leapfrog?
- take adv next gen of identity

Kaliya
- not talking africa
- how the latest african id conference was walking ad for gemalto and smart card people
- thats what id is
- whats the alternative vision that is accessible

Julian
- Id consists of 2 parts, identification data and activity side
- we could do something this year, they are looking for a digital locker in india
- just to put certs of education in
- leapfrog to med rec, all other stuff
- immediately get to self sovereign piece
- save billions
- get to microfinace, get to phone record that becomes worthy of level of credit
- stuff we can do
- show digital locker / self sov owning data can demo that, tangible, they havent done
- leapfrog to not use infra

Brian
- worth pursuing
- Aardhar horse has left the barn
- not getting it back in
- Brian is not personally familiar with digital india initiative
- DAI - dont want help on ID tech
- they have vision, and executed on it
- its done
- not looking for technical assistance
- doing w/ india stack and priv sector involvedment
- really interesting and invite outside companies

Abhi
- from outside everyon can see stark issues, no trust framework

Julian
- additive, provide value and expose fact here is an opportunity
- move existing to make more use of the new

Joe
- a paper needs to be short and sharp "tip of speak"
- "here are some opps to leapfrog" to the decision makers
- 1-2 page paper, what he could get

MLF
- he wants help to 1000s of problems
- wants a process that is helpful

Alpesh - Is DAI looking for help?

MLF

- I work from intuition
- They need to work out what help is needed
- reached out on behalf of IEEE
- recognition there are challenges
- mired in firefighting

Group

- Core problem statement is not there
- tons of bad press
- is the help for other or for Digital India Initiative

Karen

- needs a process in how to address it
- IEEE does this for a living
- overwhelmed - needs help to rise up above to address the problem

Kaliya

- expansive of version 1
- paper for what it should do on systems level to have leadership in identity
- not answers but process for building functional system

MLF

- India has committed to connect the internet to 250k villages (across subcontinent)
- some dont want, others have land rights issues
- There may be something the IEEE and global comm could do for digital india
- dont want to come up on their own
- needs a diversity of ideas
- one example
- looking at countries
- Modhi invited singapore
- first speaker
- said education was key thing to find promise of leapfrog
- every head of state went to that meeting
- digital literacy and literal literacy
- first thing to address

Lily

- framework to use to facilitate that vote
- 3 things -
    - 1. do those things provide immediate value financial or benefit to the person enduring the pain in the situation
    - 2. is there a benefit to the govt
    - 3 what is the heft of blockers
- example: deeds
- more immediate benefit than ability to get a job b/c education has been certified
- whereas deeds prevents bickering over issues (massive implementation blockers)

Joe A

- category confusion
- whats the "doing"?

- cool concepts but is "the doing" we suggest and stand up a frugal 5g
- what is the doing, not seeing it for a lot of those

MLF - instinct to the process
- what they feel would fly
- process to tap global expertise in manner

Alpesh -what would process look like or id which one

MLF
- roll out process
- advancing solutions for internet inclusion
- committed to 10 meetings with number of players
- regional components
- have meeting in india
- w/in meeting in india
- have process that is consultative and helpful is a good kickstart
- existing processes going on in IEEE could with ID crowd jump in

Abhi
- IDENTITY SUMMIT IIW
- education needed
- sharing best practices
- only 1, nothing scale of IIW there
- or like a major security conference
- good start

Joe
- open space approach
- people show up bring their issues
- not bringing our message but collaborating, sharing ideas and work and issues

not to say "this is what you should do w/ identity
Alpesh
- in order to be successful, requires a pipeline of talented individuals coming downstream to avoid this happening again
- seen as a leader, sustainable perspective
- lot of strong talent there, not always understanding of talent

MLF
- Yes and - poeple centered internet, IEEE< team up, open doors
- demo things
- some action needs to occur
- action taken by that community
- driven by them
- beyond our interjecting in their ecosystem
- show or demo - issues that have occured in similar domains

Julian
- iceland example of identity and personal data pilot
- new living lab w/in iceland
- whole of iceland startup community built on Digi.me

- banks, telcos
- whole of the startup community in the framework
- do similar things
- code, process, consensus

Alpesh

- important concept in this process, ID is seen as utility
- everyone should have ID
- seen as something only a set of folks could have or own
- sustainable growth from there

Around the room for last thought on action (what might we do):

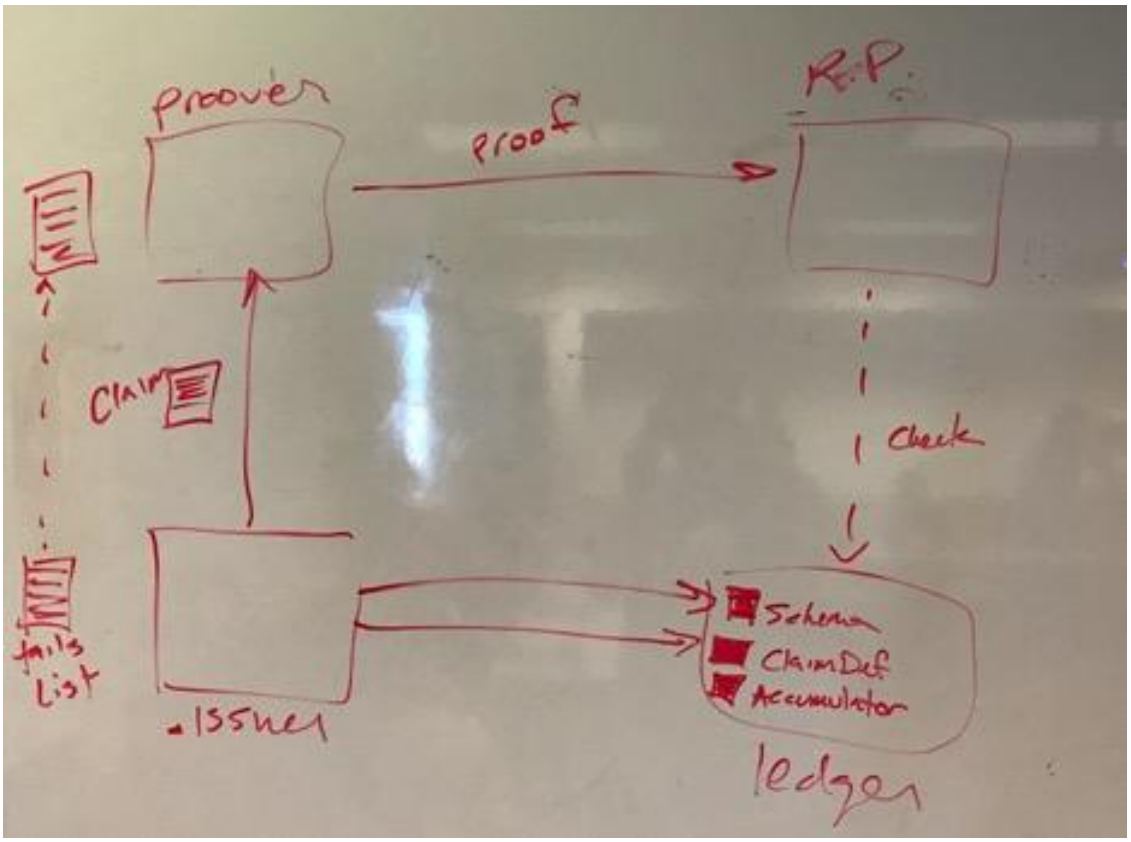
- frugal 5g actively pursuing
- trust frameworks
- processes and standards
- talking to the people who are there, living day to day
- issues and help
- IIW India - most effective - get the people to help themselves - coalescing awareness to solve problem and get peopel together could help
- connect to peopel there, create snowball effect
- move forward
- conversation w/ indian pros - IIW India
- engage in

Libsovrin and Anoncreds

Wednesday 4B
Convener: Marcus and Nage
Note Taker: Nathan George

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

https://docs.google.com/presentation/d/1hlWqNZ3yLeOPL_zYnONQGqI9Ho5dOso5huTJgw3yZvc



5 Types of DLT Privacy

Wednesday 4C
Convener: Timothy Ruff, Evernym
Notes-taker(s): Colin Jaccino

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

DLT - Distributed Ledger Technology

5 Types of Privacy for DLT-Identity

1. Decryption
2. Correlation
3. Leakage
4. Revocation
5. Future-Proof

This list will grow

What do you call a block chain with no blocks and no proofs of work?

"We believe" that there should be a ledger for the whole world that is publicly available, immutable.

High stakes because if you screw up the privacy, you screw up for everyone.

- Some schools of thought that everything should be on the ledger

Evernym's thought - nothing that is private should be on the ledger. (for future proof)

Privacy is much more than encryption.

Decryption - If you use an encrypted, hashed ID to work with multiple parties, those parties can get together to deanonymize your ID.

Correlation -

Leakage - Disclosing more than you need to. If your college gives you a detailed transcript. Lots of info on there. They may give it as one verifiable claim. What if someone asks "did you really run the 100m in under 12s?" And buried in that transcript is that info. If I don't have a way to convey that info that prevents leakage, I have to share the whole basket of info in that transcript. I don't want to give more than I have to.

Revocation - The

Future-proof - What goes on the ledger and what doesn't?
A public ledger that is there for the whole world to look up forever.
In the future, we will have really really really fast computers that might decrypt anything. So we don't put anything that might be subject to decryption or correlation risk.

Comment: Maybe future proofing is something you would want to build into all of your privacy protections.
Timothy: Pair-wise identifiers.
Scenario: Sign into Facebook. Under the hood, an identifier is generated for logging into other web sites. Because of this, the web sites logged into by the user could correlate the logins and deanonymize the user. Facebook began using a different ID for each site.
But if users volunteer their information to each web site, it's fine. We can't stop them. BUT On a global, permanent, immutable ledger, we DON'T want to put corrrelatable data on the ledger.

Will privacy make a comeback? Timothy thinks so.

Audience contribution: Marketers aren't going to like this.

Timothy Scenario:
Suppose I can raise three flags to the world anonymously.
- I have an $800k house to refinance.
- I have $1M net worth, attested cryptographically by a trustworthy third party.
- I have a 5-star rating for buying what I say I'm going to buy.

Audience:
- People may not accept or trust this DLT and these DLT-enabled services.
- People don't think it's spam if it matches the needs.

Internet of Things is a huge security problem. Tim thinks it's an Identity problem. How do I know it's really my car that is calling me to tell me to it needs an oil change.

Scenario: The pairwise ID problem. If you have a unique ID with each relationship, especially with IOT, you will have thousands of pairwise IDs. But the costs may be significant. Using the bitcoin transaction fee of ~$1, this means thousands of dollars in management costs.

A solution is the DLT-based ID management method that sovrin is advocating

The End-User Identity Paradox - "Don't lose your phone number."

Wednesday 4D
Convener: Jay Carpenter
Notes-taker(s): Jason Wrang

Tags for the session - technology discussed/ideas considered:

Phone Number Identity
System level End-user Identity
End-user ENUM
Identity Paradox
Registration/Vetting Database

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

Jay Carpenter
JayCarpenter@DesertBlockchain.com
+1-602-228-4486 cell
1-800-HOLLYWOOD
PHONEWORLD.com

Rich web experience through a phone #
Who controls a telephone #?

PHONEWORLD: Human friendly telephone number with an embedded phrase

The end-user Identity Paradox
http://phoneword.com/images/1-800-AFTA-2008-09-16-11-00-00-USA-AZ_End-User_Identity_Paradox.pdf

An assigned telephone number has an end user, but the end user has no face.
The phone # has become a key identifier, but who has the rights to that number?
See article

1. "Hackers Have Stolen Millions Of Dollars In Bitcoin – Using Only Phone Numbers"
2. "I-Team: Thieves Take Over Phone Numbers to Steal Identities"

Circular Logic:
The Catch-22 or Liar Paradox

Carriers don't perform any end user authentication -- easy to hijack phone numbers.

Proposed Solution
Central DB to break end user paradox

Electronic Number Mapping (ENUM): RFC 6116

Identity – Determination of End-User Identity for a given telephone number is a current dilemma at the overall telecommunication and media delivery system level without an objective database that contains the definitive identity of the End-User

Self-Referential - The existing circular structure of the End-User designating the Carrier-of-Record/RespOrg while the Carrier-of-Record/RespOrg designates the End-User Identity created a key Next Generation Network telecommunications and media delivery paradox.

External Database – Creation of objective database such as End-User ENUM for registration and incorporating public vetting and aging to establish definitive End-User identity for a given telephone number could break the current circular dilemma surrounding determining End-User Identity.

Registration, Pubic Vetting and Aging – This **process** could contain key components for establishing and validating overall system level End-User Identity for successful implementation of Next Generation Network services. Moving forward with End-User ENUM implementations and an enhanced End-User ENUM registration process could be the key to ending this vexing paradox.

Discussion
Registry constructs allows for whitelists, blacklists, present information based on who is attempting to contact the number.

Concerns:
Consider mobile phones as a dial-able SSN.
If phone/device is stolen, attacker can assume the identity.
In this construct, the number may relay a lot of information about the person.

There is a security concern regarding spoofing caller-id.

The database is dependent on the quality of the vetting, and the quality of the vetting is a problem today.

Can this globally registry remain secure?
Shared plans with single subscriber controlling multiple phones.

Anonymity could still be achieved through the use of burner phones, where registration is set as anonymous.

There are 3rd party vetting services today that offer similar services.

Use case:

- Financial transactions:
    - Numbers to exchange crypto currency.
- Rich Media
    - Lookup number in browser for rich media, fallback to telephone call
- Mobile carriers could become trusted 3rd parties

Using Sovrin for Decentralized Student Profiles – A Proof of Concept

Wednesday 4F
Convener: Matthew Hailstone & Phil Windley
Notes-taker(s): Phil

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

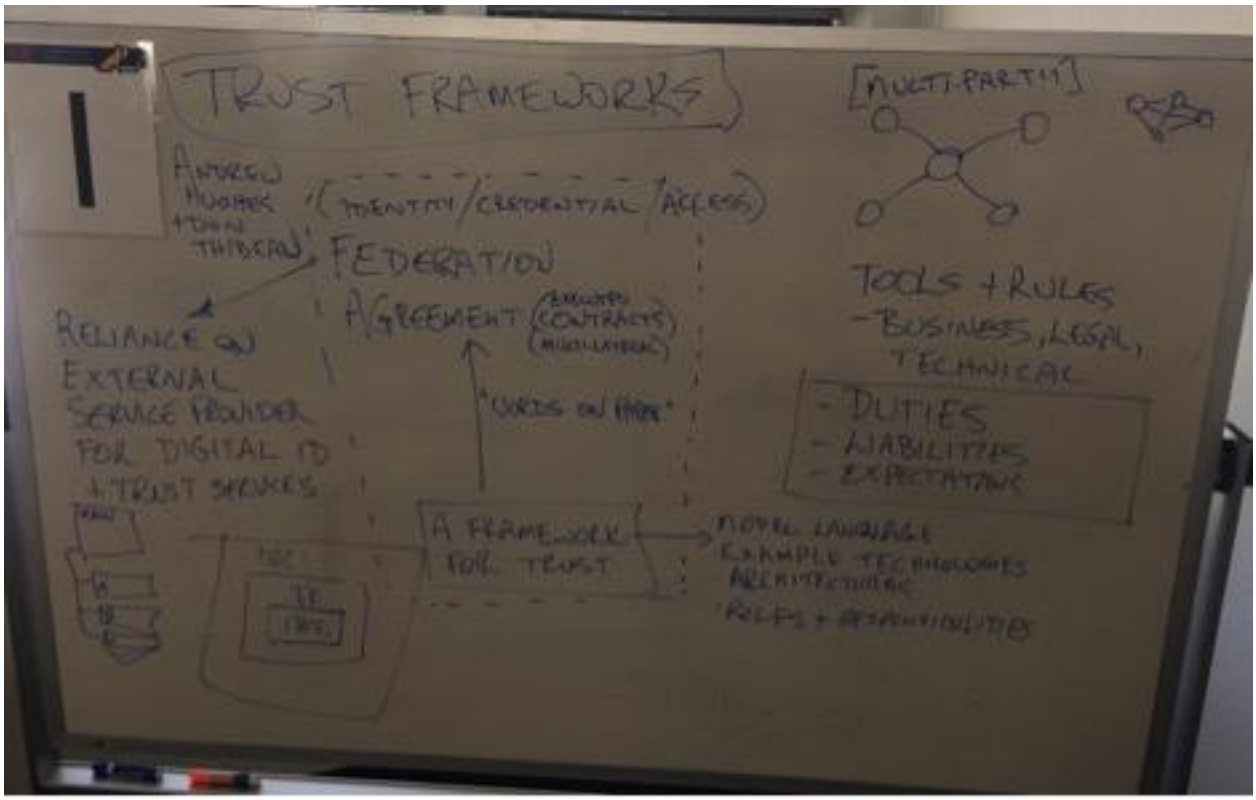
This post describes a proof of concept for a personal learning system called a student profile. The student profile gives students control over their personal information, including learning activities, and demonstrates how other parties can trust learning records kept in the student profile and shared by the student. This is a critical factor in creating personal learning environments that support life-long learning and give the university greater flexibility in system architecture.

http://www.windley.com/archives/2017/02/student_profiles_a_proof_of_concept.shtml

Trust Frameworks

Wednesday 4l
Convener: Andrew Hughes
Notes-taker(s): Andrew Hughes

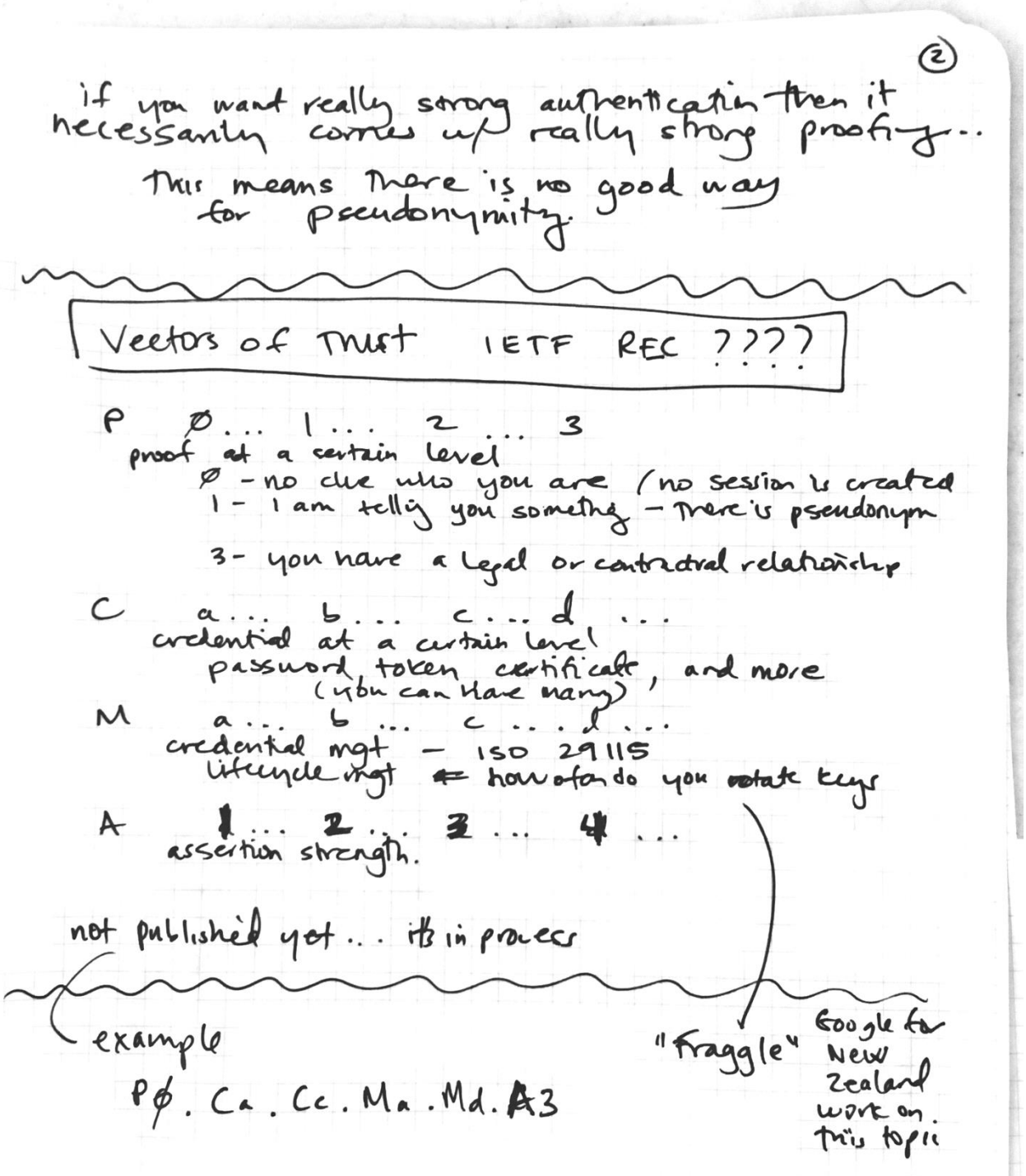
Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:



Levels of Assurance

Wednesday 5A
Convener: Sarah K Squire
Notes-taker(s):

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



(3)

"NIST SP 800-63-3" Digital Identity Guidelines ← on Github ☺

IAL 1... 2... 3... identity assurance level DOC= 63A = M-04-04 Proofing + Vectors of Trust P

AAL 1... 2... 3 Authentication assurance level DOC = 63B = M-04-04 Authentication + vectors of Trust C

FAL 1... 2... 3 federation assurance level DOC = 63C = M-04-04 doesn't consider + vectors of trust A

Vectors of Trust is a broader set of info and 800-63-3 has more detail on execution

LOAs have been interpreted and added to by LOTS of entites so now you have LOA 2++ and LOA 2+ so how do they talk to each other?

in Post-Final Public Comment now.
This will turn into a federal guideline in 2017

NIST 800-63-3 | M-04-04 | [redacted] | IETF REC ??? (4)

IDENTITY / PROOFING

IAL 1 = LOA 1 (Phone) ~ (proof)

IAL 2 = LOA 2 (P remote) = [redacted]
LOA 3 (P remote)

IAL 3 = LOA 4 (P in person) = [redacted]

this needs more examination arguably they don't be out-tech driven schema

AUTHENTICATION / CREDENTIAL

(credential)

AAL 1 = LOA 1 / LOA 2 (1FA) = [redacted] Ca → ?

AAL 2 = LOA3 (A 2FA) = [redacted]

AAL 3 = LOA4 (A 2FA + HW) = [redacted]

FEDERATION / ASSERTION

FAL 1

FAL 2

FAL 3

(assertion)
A1, 2
[redacted]
A 3
A4
(needs validator)

DIGITAL IDENTITY GUIDELINES

eAUTHENTICATION

VECTORS OF TRUST

PSTN - Public Service Telephone Network

Text message is not recommended for 2FA due to tenuous use for phone porting.

Rotating passwords on a regular ~~basis~~ basis = BAD

Longer passwords = GOOD

Unicode space = GOOD

No max password length = GOOD

Composition Rules = BAD
special character + lower case + upper + #

DID Auth – Interoperable Auth'n w/ DIDs

Wednesday 5B
Convener: James and Nathan
Notes-taker(s): James Monaghan

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

We reviewed the problem statement and some of the progress made at Rebooting Web of Trust on collecting requirements for an interoperable authentication mechanism based on DIDs. The uPort team shared some details of how their implementation works and the existing standards which influenced their design. We talked about how CurveCP, Self Attested HTTPS URLs, SQRL and OpenID Connect all contain goodness a future specification could benefit from. We concluded with an agreement to continue working towards interoperability and to reconcile the uPort approach with the Verifiable Claims based method we explored in Paris.

Reinventing National Identifier Systems

Wednesday 5C
Convener: Kaliya
Notes-taker(s): Kaliya

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

How can governments use the new self- sovereign identity technologies might be used by governments to support citizens interacting with them but getting out of the challenges that persistent correlateable identifiers like SSN present.

Here are some parts of the paper that Kaliya wrote based on the conversation from the session.

Markus also drew on the conversation to present to the Austrian Government the weekend after IIW.

This report lays out the case for a new federal agency, The Non-Identity Agency (NIA), that would over five years completely replace the Social Security Number with Invisible Identity Numbers (IINs) that will be usable by citizens across the federal government. The new system will be largely resistant to identity fraud caused by the current system design that uses a persistent correlateable identifier, the Social Security Number (SSN). Cryptography allows IINs to be masked and will completely transform how individuals interact with governments because no persistent correlateable identifiers are used, so there is nothing to "steal" and use in other contexts. Each time an individual uses the IIN, they share a cryptographic proof of the number rather then he actual number. IINs use several relatively new technologies in combination: mobile phone applications, distributed ledger technology and cryptographic proofs.

Infrastructure for Invisible Identity Numbers

Several technologies are available to create this new system including a combination of mobile phone technology and cloud technology that enables individuals to have software agents working on their behalf. Three different types of cryptography are used:

- **Public Key Infrastructure** using pairwise identifiers to support the creation of secure cryptographic tunnels for communication between and between individuals and institutions.
- **Zero Knowledge Proofs (ZKP)** lets individuals obtain claims issued by another party (typically an institution) and then produce and share proofs derived from the claim without reveling the actual claim. So for example an individual could take claim such as a birthdate issued on a state drivers license and use it to share with a bar only the fact that the individual presenting it was over 21. The zero-knowledge proof would not reveal the exact birthdate or their mailing address.
- **CL Proofs** that allow Zero Knowledge Proof claims issued by institutions to be revoked.

Distributed Ledger Technology is used to support the management of the public-private keys and agent pointers for individuals and institutions along with verifiable references to the ZKP and CL Proofs.

The core of this network is a permission-based distributed ledger that is kept current by the validator nodes on the network. A distributed ledger means that the database doesn't live in one location, but rather exists across the whole network of nodes. As information is written to the database it is permanent— it cannot be changed. Everything written into the ledger is public. In this unique governance model set up by the Sovrin Foundation, which is very different than the Bitcoin or Ethereum ledgers, all validator nodes are run by institutions like banks, universities, hospitals, credit unions etc. They sign an agreement to join the network and are bound by the conditions of this trust framework.

Creating New Identity Assets

Using these infrastructure pieces, how does the government issue Invisible Identity Numbers to individuals that can replace the Social Security Number system? The first step is to setup a system of enrollment so people can get the new IIN. There will be a process for identity proofing that is rigorous, using a points system similar to how New York State issues Drivers Licenses (NY State, 2015), with different types of documents providing a different number of points that are acceptable for identity proofing. Individuals will present themselves at the NIA with this documentation, including their Social Security Number, Birth Certificate, Drivers License, Passport and other documents that are used to prove they are indeed the person that a given SSN points to. The government would then issue the claim of an IIN to the individual. The government would also publish a record in a public database stating that the person with a particular SSN now has and IIN. This would "retire" the SSN so that everyone knows to not accept it from anyone claiming to be that person because the "real" person has an IIN and should be using that. There will also have to have a dispute resolution system in place as fraudsters will try to attain IIN's that really belong to other people.

To get the claim of an IIN from the NIA, an individual must sign up with an Agency and download on to their phone an application that provide them with a IIN Agent. A company named Evernym makes the software code and in the future there will be different companies that will also make agent codes so individual will have a choice of agent provider . This is the secure application that enables the individual to store their claim information and manage all their interactions using these claims.

Both the individual (via their mobile app and agent) and the NIA would next register a DID on the Sovrin Distributed ledger. A DID (decentralized identifier) is a globally unique long number generated cryptographically. With each DID comes a DDO—a JSON document containing the public key from a public-private key pair. Both the individual's agent and the NIA get unique public private key pair that allows them to open a secure cryptographic tunnel for secure communication. Though this

tunnel the NIA sends the IIN to the individual's Agent. The NIA also writes to the Sovrin ledger a cryptographic proof that they issued the IIN. This proof does not reveal the IIN, but will enable the individual to prove to any institution or agency that the individual has a unique valid (non-revoked) IIN.

Using the IIN

Now that the individual has an IIN, they can use it to interact with their employers, banks or government agencies. With every agency or institution that they interact with they go through the same ceremony using the Sovrin ledger to create a unique cryptographically secure communication tunnel. When that tunnel is established they send along the proof that they have an IIN and proof it was issued to them by the NIA. **They never send the actual IIN.** They use Zero Knowledge Proof technology that transforms the IIN into a cryptographic proof when it is shared so the actual IIN isn't reveled. This is what makes it very secure—and can virtually end identity theft/fraud as we know it. This can seem hard to understand because the fancy math can accomplish something that is not possible using ordinary paper-based physical systems that are usually used to track identity. It is critical that we leapfrog the mental models that paper and traditional systems of unique identifiers like SSNs have created for us, We need to leverage the strong new security and privacy-protecting properties these new types of cryptographic identifiers can provide.

Adoption and Use

Employers will be encourage to switch away from using SSN's (with all its ensuing security risks) to accepting IIN proofs. Individuals can create a cryptographic tunnel with their employer, in the same way they did with the NIA. They share the proof they have of their IIN with the employer who then passes along a proof of the proof to the government when submitting their taxes and other government benefits. If an individual has three different employers - each employer has a unique proof of the IIN of the individual. When the individual goes to file one's taxes the individual can support the Tax agency knowing the three different they proofs they of the same individual from three different employers actually represent the same individual. This totally leap frogs the SSN in terms of its ability to keep individuals and businesses secure.

Relating to Other Agencies

An individual will be able to use the proof of their IIN with a whole range of government entities. Each agency an individual interact with creates a cryptographic tunnel with the citizen's agent, in the same way they did with the NIA to get the claim of the IIN. They use this tunnel to communicate the Zero Knowledge Proof of their IIN, not the actual IIN. In this way the agencies know it is the same individual they are interacting with over time. The individual will also be able to communicate with the agency via the cryptographic tunnel - messages about needed updates, payments, to or from the government, services, appointments. This could include text messages or phone calls.

The NIA does not interact directly with any other government agencies and shares no identity information with them directly. The main way that other government agencies know that the IIN proof they have from an individual is unique is via the proof they record to the Sovrin ledger that other agencies can check to see if indeed the IIN proof they have from an individual is legitimate. They can also use the other proofs the individual presents, see the Appendix below about how Jain uses it to open a bank account for filling the know your customer requirements.

References

New York State Department of Moter Vehicles (2015), Proofs of Identity, Document number ID-44 (12/15). https://dmv.ny.gov/forms/id44.pdf

OAuth High Assurance FAPI

Wednesday 5G
Convener: Nat Sakimura
Notes-taker(s): Michael Schwartz

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

OAuth 2.0 is not optimized for high assurance use cases.

Authorization request and response is not protected.
Susceptible to insertion attacks: eg code insertion, state insertion

Token and client credentials are 'bearer'
They are susceptible to a variety of token capture attacks, including
code phishing

There is no explicit issuer for the tokens (incl. code)
Redirection URI at the client is a proxy for the issuer identifier
This means the redirect uri needs to be unique for each AS

In Finc'l API working group:

- Use request object / request URI / signature required
- Use hybrid flow with id_Token in the front channel as a detached signature
- include s_hash in the id_token - state hash

Bind tokens to TLS client certificates or use token binding.

Mutual TLS profiles for OAuth Clients - draft-cambell-oauth-mtls

Perhaps client private key authentication at the token endpoint is almost as good mutual TLS, althouhh it lacks some of the replay protections. But due to specification of mutual client authentication by UK banking regulations, and
the greater availability of infrastructure to handle this, mutual TLS was preferred.

The following is an example of a JWT payload

{
"iss": "https://idp.example.com",
"aud": "https://rp.exmaple.com",
"sub": "foo@bar.com",
"exp": "1493726400",
"nbf": "1493722800",
"cnf": {
"x5t#S256": "bsdfsdaflkasjdflksadjfkldsklfbnsadlfnsdklflkasdfasdff-dg2",
}
}

The client would have to register the auth_subj_dn and the auth_issuer_dn at the AS. From a

deployment perspective, it adds some complexity. Certain deployment models could interfere with this mechanism (like use of Amazon ELB service.)

The OpenID Connect federation spec perhaps could be used to add
extra security over TLS. How do fintech services get authorized to register for client credentials at banks? How do banks publish their stable signing keys?
What format software statements would use to register is still up for discussion.

OpenID Connect Financial API

http://openid.net/wg/fapi
Currently working on part 1 and part 2

Part 1: Requirements for Read
Section 5.2.2 Authorization Server
    5.2.3 Client requirements

Part 1: Requirements for Write (more risk)

FAPI proposes a new request object endpoint in the AS--the RP would POST the request object to the API which would return a JSON with the request object URI. The client could then use the request_uri in the authorization request.

Brian Cambell from Ping expressed some concern about requesting the request object from a URI, which has low adoption in practice right now anyway. He said it's hard to get right.

Certified Self-Sovereign Signature

Wednesday 5H
Convener: Adrian Gropper
Notes-taker(s): David Huseby

Tags for the session - technology discussed/ideas considered:

Self-soveriegnty

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

- The target application is e-prescribing controlled substances by doctors for patients.
- Patients and doctors are reluctant to use an institutional system for tracking prescriptions because of privacy issues.
- The regulatory framework is enforced by the DEA and is well understood.
- All prescriptions have DEA mandated items:
    - MD-DEA #
    - System audit
- The software solution is comprised of two main pieces: one part for the MD, one for the patient.
    - The MD has a DID for logging into the electronic health records (EHR) system.
    - The MD uses their DID for signing prescriptions.
- The DEA requirements for e-prescribing:
    - Requires 2-factor auth and one factor is a MD-FBCA issued certificate used for signing.
    - Access to the e-prescribe software has to be signed off on by at least one other person who has a MD-DEA #.
- Can we build a system that meets these requirements using any of the verifiable claims and distributed identity solutions.

Solution 1

1. Provisioning
    a. Generate an ECC master keypair for the MD.
    b. Submit the ECC master public key, DID, and MD-DEA # to the FBCA to issue a certificate.
    c. Store the certificate in the DDO.
2. Prescribing
    a. For each prescription, generate a nonce use to generate signing keypair from the master keypair.
    b. Sign the prescription including the nonce and the DID.
3. Verify
    a. Use the DID to look up the DDO to get the certificate containing the master public key and the MD-DEA#.
    b. Use the MD-DEA# to check the DEA API for revocation status.
    c. Verify the prescription signature.
    d. Verify the public key is derived from the master public key.

How do People Manage Identities? Prelim findings from user research in India

Wednesday 5J
Convener: Bryan, Caribou Digital
Notes-taker(s): Heather Vescent

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

URL: Identitiesproject.com
bryan@cariboudigital.net

User research from India

Identity
- State run systems
- Sim, what's app

Qualitative research
Talk to couple hundred people across 3-4 states
No intent in making a general sample
Uncover and surface, practice and behaviors
1:1 interviews – worked with Indian University in Bangalore, driven by Indian research teams. Sit down interviews.
Ask what's in their pocket they use for identity
Experience of using their identity- last time used, how, challenges, what are the implications for the individual's agency. To prove who they were. Gain access, etc. That is privacy and dignity preserving.

Identity mosaics. Identity systems.
Credentials are embodied in an artifact. Show someone an identity credential.
How the artifacts (voter card, drivers licenses) mediates the relationship with the entity that uses the identity.

What did we learn?
There are no greenfield identity systems. There are a lot of different identity systems. Most people bring a variety of identity "cards"
Sequential layering of credentials.
A lot of time people use the credentials for different reasons than they were originally defined.
Any new identity system has to be seen in context with the systems that are already out there.
When you multiple credentials, you have choice in what you present to authenticate yourself. This gives individuals flexibility and resistance to shop. If you have others that get you by if one has an error, it gives more resilience.

Material artifacts matter. Most people used photocopies of the actual artifacts (left at home). Not because it would be stolen, but because it's a hassle to replace. Aadhar started out as totally virtual – 12 digit number – only available as biometric. Was never going to be a card to authenticate. People struggled with that. People started using the aadhar receipt (get it laminated). Eventually aadhar cards are used to assure in lower level of transactions.

It is being used for less formal authentication measures. There was a sense of pride that if I have this ID by the government, that I am not a terrorist. Introducing a concept of university dignity – you don't have to have a social standing or a place in society – as long as you are in india, you can have an identity. (Prior you had to give your address and father's last name to get an identity card.)

Aadhar card
Name
DOB
Address
Gender
Optional email & mobile number

You don't have to have a verified proof of address to put it on your card.
This is an inclusive system.

Identity systems don't eliminate vulnerability – they shift it. Getting different identity credentials requires supporting documentation. In order to get certain credentials, they had to have proof of address, but they were in living situations with landlords who would not give a proof of address.

Idea that Aadhar reduces bureaucracy, but it didn't do that. But now there is more paperwork.

Formal processes and systems are harder for poor, illiterate, disabled. None of the forms are in braille. Forms are almost always in English.

There is an urban/rural difference between enrollment.

Identity credentials are embedded with power.
The ability to have a pan card and exist (as being alive) was really empowering. I am a person and I exist in the eyes of the state. The artifact being used as an exercise of power. In an example a brother in law took his brother's wife's ID cards. And the brother had to go back with to his brother to get his wife's ID cards back.

Intermediaries play critical roles.
E.g. illiterate person shows up to bank and asks for help filling out a form. A lot of informal and formal intermediaries. They can wield power. Intermediaries take on vulnerabilities themselves. If you are the person accepting the documentation for someone and it's not complete – you assume some of the risk/liability for going outside the system.

Privacy is contextual and cultural – not an abstract concept. Poor people don't care about privacy, but once they have food… pyramid of needs. Poor and illiterate people have little concept of privacy in a general context – but in specific cases, e.g. identity theft. "I don't care, I'm so poor, let them." Attitudes that are at odds with how we think about it.

What are the right questions to ask, to peel back beliefs on this. They do care about privacy, but in the context of what is important to them.

Instead asking different questions:
Would you be ok with your neighbors learning your health care history? Or share financial information/loans and payments? Reaction is always no. Share with family but not with strangers.

Looking for better ways to uncover these beliefs.

Thursday May 4

DID Discovery Service

Thursday 1A
Convener: Sam Curren
Notes-taker(s): Drummond Reed

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

Sam began by explaining the "service" block in a DDO (DID Descriptor Object).

A slide deck describing DIDs and DDOs was given in session #1 yesterday—the link is https://github.com/WebOfTrustInfo/rebooting-the-web-of-trust-spring2017/blob/master/topics-and-advance-readings/DIDs-solving-the-root-identity-problem-2017-03-14.pptx.

George Fletcher asked about whether the DID spec will standardized service name types. Sam explained that it will, but Sam feels that it will not matter. George thought it was important.

The x-dash convention was suggested, but Justin and others argued against it as x-dash specs often become permanent. They suggested to use a URI, and to have widely adopted URIs receive short names in the JSON-LD context description.

Sam suggested that the value for each service name should be a list (an array), and there should be a SHOULD to keep the number of URIs short.

George suggested that each service name spec should specify if there will be more than one (arity) and how to choose if there is more than one.

Sam suggested that service names do not include any other metadata, so that any additional discovery takes place on the discovered URI and not via the DDO.

Sam then proceeded to described his ideas for a protocol for DID Service Discovery. This specifically applies to "agents" that are associated with DIDs and DDOs.

The overall approach is to use the Well Known spec to publish a JSON object at the standard well-known location:

//.well-known/

At that location would be a well-known file that would define the extensions supported by that particular service.

There was discussion about whether it was a good idea to try to fix a path for services or whether you should discover the path via

RFC 7320 is the IETF spec on avoiding Web squatting.

Justin also pointed to the Webfinger spec as an example of how complex that URI construction can get. Mark Atwood agreed, saying that "path construction is pathological".

Sam pointed out that retrieving full URIs as the locations for extensions allows the service definitions to use other protocols than HTTP. That's an advantage.

Each of the services that would be described in the Well Known document will have a Swagger description that can be retreived. The general format is:

{ "extensions": {

"XYZ-API": "uri",

"ABC-API": "uri"

]

}

Sam proposed that the API names (XYZ and ABC above) are DIDs, so they are long-lived. The alternative is to use URIs as the names for the specs.

The URI is the URI of a Swagger specification that describes the implemention of the API/service.

The overall result is an Extensible API description spec.

Sam explained that the Swagger spec does not support evented APIs, so Sam wants to extend it to work on that.

There was a question about supporting services like OAuth that do not have Swagger specs.

George suggested that OAuth could be used to access all the service names in the Well Known document.

UMA was brought up as an example of a service that could be support in the Well-Known list. This could be a great way to expose UMA endpoints via a DID.

There was a discussion around the need to resolve human-readable names to DIDs, and how important that was for some use cases. Justin suggested that Webfinger could be used that points to a Well-Known/DID file.

We also discussed correlation. Sam talked about protecting the Well-Known endpoint using authentication. George took it to the logical conclusion that a DDO just supports a single service—a Personal Discovery Agent—that handles all further discovery.

We agreed that the DID service block can support any number of services, including a standard DID Discovery Service.

Drummond said that the plan is to turn this into a written spec quickly, and asked anyone interested in working on it to loop back with Sam.

Justin asked how to "round-trip the trust" between the DID and the Well-Known endpoint.

****** ADDITIONAL NOTES FROM GEORGE FLETCHER *******

Looking for an Agent that is connected to a DID

Service names rules are defined in the DID spec. Service names have semantic meaning. Need a way to added small specs for service names to describe the semantics. For example, “openid” means do OpenID Connect discovery on the URL.

Sam would like to see support for multiple URLs in regards to the service name. Order matters. Rather, allow the “service name spec” to define what to do with the list (order matters, or randomly pick one). The list SHOULD be as small as possible. Additionally have the “service name spec” describe whether the value is single or an array.

If there is no “service name spec”, use a collision resistant name (e.g. URN/URI)

Agents accessible via HTTPS using the TLS via DIDs certs instead of CA issued certs.

— make sure this is implementable in all the common SSL libraries

Agents

— use .well-known mechanism for discovery of agent features

— return JSON plus API exentions

— composeable set of APIs

— API extensions defined in swagger (OpenAPI v3?)

— add path of API location part of extension JSON block

— make the “extension name” be the swagger spec, URI is where that spec is implemented (it’s a base URI)

Sam would like to extend Swagger to support evented APIs

What about “private” services that shouldn’t be public?

— can only put one things in the user DID service spec and it points to an agent that does permission exposure of services

One last question: How do you do relationships on the blockchain?

"Verifier Impersonation Resistance" (anti phish) & OIDF EAP

Thursday 1C
Convener: Jim Fenton and John Bradley
Notes-taker(s): Tom Brown

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

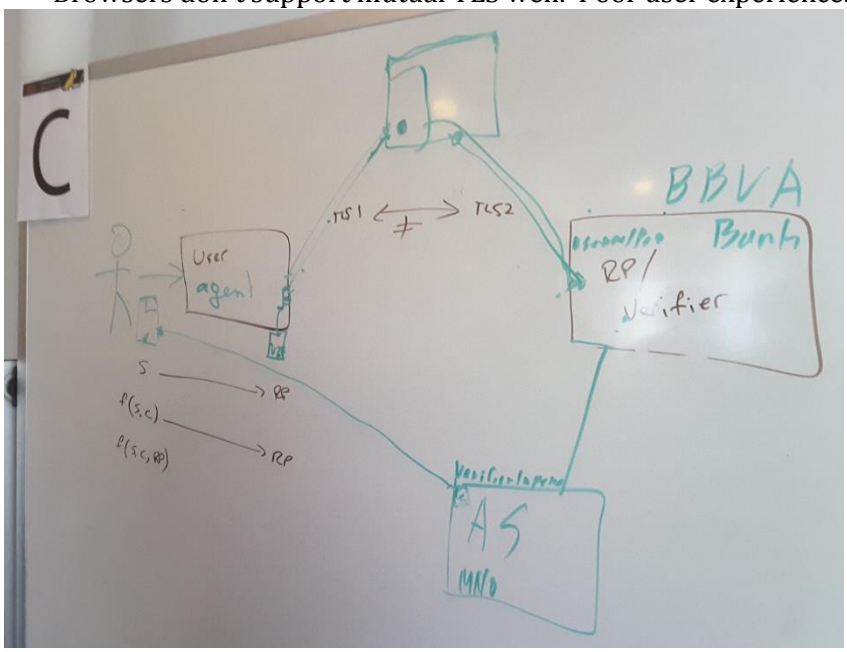
- Phishing can occur by clicking a link to a phony site in an email or a link to a phony site from web search results
- How do you present a credential to an RP/verifier without it being replayed?
- If you don't have an audience restriction in the authentication token/assertion or bind the token to a channel, you are at risk
- If you sign something, someone can replay it

Problem of bad guy posing as an RP cannot be solved with only challenge-response: Bad guy gets challenge from real RP and sends it to user agent and proxies response back to real RP

1. password S → RP
2. challenge response f(S,C) → RP
3. verifier impersonation resistance f(S,C,RP) → RP

Attack against #2 is real. E.g. Fancy Bear MIM attack on DNC (google authenticator)
BBVA – 10 million euros stolen. Hacked DNS and got certificate issued

- If you can highjack cert (sophisticated attack), simple FIDO is vulnerable. Need to be able to detect that TLS channel 1 does not equal TLS channel 2 (see diagram)
- LOA 4 – strong man-in-the-middle resistance
- Browsers don't support mutual TLS well. Poor user experience.



Functional Identity

Thursday 1F
Convener: Joe Andrieu
Notes-taker(s): Jeremy Rosenberg

Tags for the session - technology discussed/ideas considered:

Functional Identity

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

- What is functional identity?
    - As engineers, how can we talk to lay people without confusing them? Reinforced by ID2020.
    - Nobody seems able to answer what Legal Identity means
    - The fish doesn't need to define the water and we tend to use shorthand.
- Not philosophical, meta-physical, cultural
    - Not just digital (Identity is bigger than that)
- What is the subjective notion of identity?
    - Who Joe is, resides in the minds of everyone who knows Joe.
    - Inherently distributed in the eyes of the beholders.
    - Joe doesn't exist if you can't recognize Joe.
    -
- Names are pointers
- How we keep track of others and how others keep track of us
- If I'm alone on an Island, do I need an identity?
    - No, functional use for an identity if you are alone?
- Identity is the property of being known
- It seems very hard not to get philosophical.
- ISO Definition of Identity, fixates on a golden set of attributes
- A lot of identity is contextual, separate identity and personae depending on context
    - You identity will always be bigger than your attributes
- Tendency is to think that we can model this with a digital model
- The model or the map is not the territory, which can lock us into the tyranny of data
- When talking about people who deal with money laundering or refugees, there is nothing in the system to anchor to
- Self is part of others
- A DID is like a stem cell that hasn't differentiated until it's correlated
- Identity is prehistoric, so what is it? We are trying to talk to soccer moms and engineers.
- Descartes – I register on facebook therefore I am
    - Ubuntu, I am who am I because of who we all are
- Identity changes over time
    - Mountains used to be a place for exile, so a mountain climber was a witch
    - Then mountain climbers became conquerors
    - Today Mountain climbers are athletes
- Social identity theory vs identity theory
- Who you are informs who I present myself to be informs how I am seen which informs who I am. (A triangle)

    - Who you are = how I see myself
- In Brazilian tribes you often meet people who can refer to 18 generations of their ancestors by name also a child is not the property of their parents, but is a child of the tribe
-

- Potential Answers

    - Nouns and Verbs in an identity system
        - Nouns
            - Identifiers
                - Used to identify someone across contexts
            - Attributes
                - Correlate identifiers and they become attributes
                - Providence of attributes is turtles all the way down
                - Perhaps Descriptors?
                - Only becomes an attribute if evidence is meritorious
                - Characteristics
            - Evidence
                - Perhaps "observations" is more accessible?
                - There is a step that needs to happen to go from evidence to attribute (Apply?)
            - Inferences
                - Conclusions feels is a more accessible word?
        - Verbs
            - Accumulate
                - Collect
                - <group>?
            - Correlate
                - Group?
                - Connect?
            - Infer
                - Reputation is a more accessible word
                - Deduce may be more accurate
                - Conclude?
                - Intuit?
                - Reason?
            - Apply
                - Proving?
                - Validating?
                - Disclosing?
                - Proof?
    -
    - Case studies lead to clarity so lets give examples, use cases
        - Concrete instead of abstract works
    - http://bit.ly/identitycrisispaper has case studies
    - Really good, accessible analogies work well (magic pennies to explain blockchain)
    - Being more graceful, not calling people stupid
    - Uniqueness of the way one feels and the way one presents themselves
    - Identity is about self, but in practice, it's about how we relate to others.

"It's A Pain in the Ass, But it's Well Supported" (FIdM)

Thursday 1G
Convener: Alan Karp
Notes-taker(s): Judith Bush

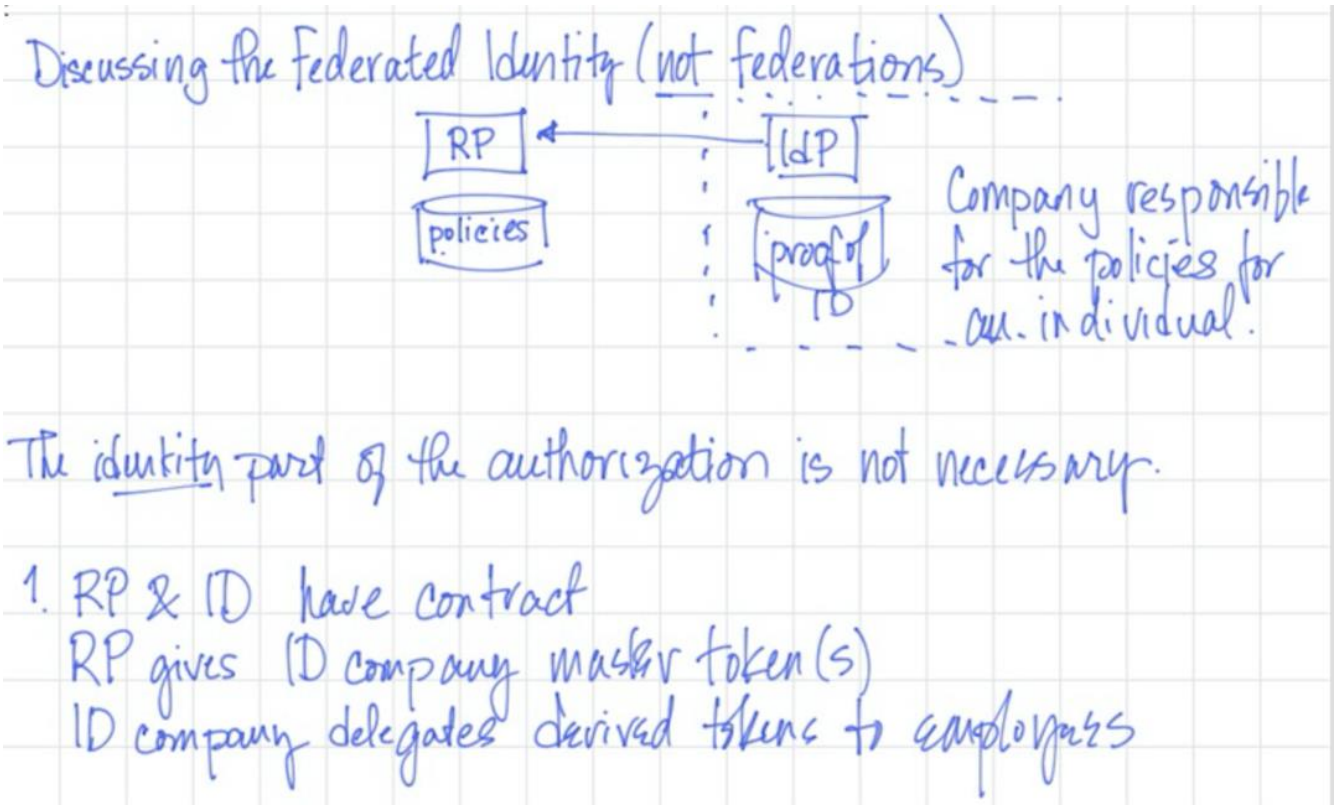
Tags for the session - technology discussed/ideas considered:

Authorization

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

Current IDP systems can control authorization at RP at service level scale by choosing to issue SAML response or not based on internal grants (eg: by assignment to groups). Finer grained authorization is the open problem, that Alan believes should be handled at IdP and communicated via tokens to RP. The RP should not need to link an identity to an access profile.

Later, Alan noted that he was conflating the above with issues of chained delegation within the domain of the IdP and that issue can be kept separate from the issue of authentication/authorization.



1. Identification
2. Authentication – proving process/person is allowed to use the
3. Authorization
4 Access

permissions granted to an identity.

Act of granting tokens & subdelegating tracks the the responsibilities.

UMA is a way to support this

UMA keeps track of responsible parties in Authz system

	User Domain	Server Domain	Before Access	At Access
Id	X		X	
AuthN	X before access			
AuthZ				
Decision		X		X

SAML only has AuthZ allow/deny ↕ IDP only Auths to RP

FINE GRAINED RAT HOLE: lets assume IF should access tokens level of granularity customer access understands —
Could only AUTHENTICATE iff IDP allows access

5/4/17

Some Sailors had access to data that the service did not.

DOD SAML diagram...

Works fine at coarse grain.
Does not work at finer.
Still avoid the rathole

NOW consider internal delegation

NOW need to address the finer grain

RFC for token exchange for the delegation "Nested JWT" proposal

Privacy Preserving Geo Location & Other "mystuff" Services

Thursday 2C
Convener: Arman Maghbouleh
Notes-taker(s): Alan Gous

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

Two use cases for looking after your things:

1. Improving privacy for geo-location tags

- Current setup involves BLE tags (Tile, Trackr), communicating to gateways (cell phones) that add geolocation info and forward to a proprietary server. Users can access the server.
- Sketched a more open, privacy-centric version:
    - Ephemeral IDs (EIDs) on BLEs
    - Gateways add geo-info cryptographically
    - Distributed Hash Table (DHT) bulletin board so gateways post EIDs and user apps query for these.
    - DHT has no ability to link users to the locations or data from things.

2. Attesting Ownership of Things

- Discussed a DHT solution for registering, transferring ownership, verifying ownership of goods (eg camera with serial number), for lost+found and deterring theft.
- Suggested interest from police services, insurance companies, pawn shops, etc

Sovrin ID Card

Thursday 2F
Convener: Steve Fulling
Notes-taker(s): Tyler Ruff

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

Sovrin ID card notes
What should it do?

It could be blank, but then what happens when we drop our cards next to each other? Which is which? Could it sync with your phone? Yes.

The idea of the card is having a low trust point, something tangible people can give to introduce themselves. It would be an intermediary between a human, their agent, and the relying party. As an RP you could scan it and it could pop up a picture of the owner. Picture doesn't have to be on the card. It could just have an RFID chip. It could be the last business card you ever have.

Someone asked: Why don't we just use token technologies? Because we're talking about a card that has a photo, what makes the card feel like yours? How do you limit the the correlation to the card.

Having key fobs and things like that does make sense. Some people that have no technology could use this as their first non-gov't identification. What requirements are there for what should be on (in?) the card?

1. A photo of the person
The biometric should never leave the card
2. The card should have an RFID.
It shouldn't be tamperable. We should discuss how trust-able it is. There's an enrollment process which ensures the binding is accurate. Probably involves cryptographic control. There is tech out there which makes it impossible to spoof. How do we trust that the binding is authentic?
Couldn't someone produce fake Sovrin ID cards?
The trust model validates the market fit for a card like this. Independent identity needs to move from institutional identification to independent identity proofing.

Does this card serve as an "introduction card"? It shouldn't have correlatable attributes on it. If I had one card for all my membership cards.

A chip or card reader or something like that, like the card system works today, would generate a random identifier each time it was scanned?

Paco: Digital passport gets signed by the private key of the issuer. The problem with it is you don't want to disclose all your information. YOTI lets you selectively disclose.

"When you can verify who don't need trust". When you look at a caard, you're trusting the issuer. There's two attestations from people who know you. One of them has to sign the back of a photo.

Pop-up Enterprise

Thursday 2G
Convener: Justin Richer
Notes-taker(s): Andrew Hughes and George Fletcher

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

Q: What is a pop-up Enterprise? (An enterprise infrastructure for loose conglomerations)

- Time factors
- Identifiers
- ACLs (?)
- Services
- Export / Archive

- How would a capital asset investment cycle work with a pop-up enterprise?
    -
    - Could treat capital assets as smart agents - business as a service
    - Needs to fit into a cost accounting model - calculating the inputs and designation of the assets and outputs
- Strawman - Justin is thinking about how to instantly instantiate a 'company' technology platform to allow for a group of companies or individuals to work together
- Talk about how to set up a project team's tools from SaaS providers automatically
    -
    - Use micro-billing

May need an identity component to the "pop-up" infrastructure.
-- roles and access controls require identity IAM and SSO features

Also needs auditability for addition and removal of people capability.
-- changes over time

Also useful for a "trial startup" mechanism. Build the "enterprise" infrastructure while trying an idea/product and then eventually morph it into a permanent enterprise if things go well.

Another aspect of this is to enable the Machines to be their own company and then the machine shop just "contracts" with the Machine "company" for use of the machine for x amount of work.

What's missing?
-- security as a service?

"The best team; just in time"

OTTO-ifying FastFed

Thursday 2H
Convener: Mike Schwartz
Notes-taker(s): Mike Schwartz

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

The IDP's and RP's of a federation need to agree on certain things to drive down the cost of single sign-on. This includes user claims, but may also include OAuth scopes and authentication details like acr and amr. (See OpenID Connect client metadata for a definition of these terms: http://openid.net/specs/openid-connect-registration-1_0.html#ClientMetadata)

OTTO is a set of API's and a JSON model that can be used to automate the operation of a multi-party federation (like InCommon...) The OTTO WG decided to leverage JSON-LD. There is an extensive schema already defined at https://schema.org In particular, we re-used the JSON-LD classes for

Organization and Thing quite a bit. See:
https://schema.org/Thing
https://schema.org/Organization

The advantage of JSON-LD was that it provided some linked data capabilities, but looked like "normal" JSON to developers who didn't care about these features.

On Tue, Darin McAdams presented an overview of progress in the OpenID FastFed Workig Group: http://openid.net/wg/fastfed/ You can see a spec straw man at: http://gluu.co/fast-fed-strawman

In that document, a configuration response from an IDP is proposed:

```
{
 “identity_provider”: {
 “name”: “Awesome IdP”
 “logo_uri”: “https://example.com/images/idp_logo.png”,
 “auth_protocols”: [“SAML”,”OIDC”], #In practice, only 1 protocol typically
chosen.
 “saml_metadata_uri”: “https://tenant12345.example.com/saml-metadata.xml”,
 “oidc_configuration_uri”: “https://tenant12345.example.com/oidc-configuration”,
 “token_endpoint”: “https://tenant12345.example.com/token”,
 “scim_endpoint”: “https://tenant12345.example.com/scim”,
 “supported_attributes”: {
 "schemas": ["urn:ietf:params:scim:schemas:core:2.0:User",
 "urn:ietf:params:scim:schemas:extension:enterprise:2.0:User"],
 "id",
 "userName",
 "name": {
 "familyName",
 "givenName",
 },
 "displayName",
 "emails",
 "urn:ietf:params:scim:schemas:extension:enterprise:2.0:User": {
 "employeeNumber",
 "costCenter",
 "manager": {
  "value"
  }
  }
  }
 }
```

Mike Schwartz's feedback was that perhaps OTTO's JSON-LD model could enable a more elegant expression of this information.

Current draft OTTO JSON-LD vocabulary can be found here:
- OTTO Core Vocab : http://gluu.co/otto-vocab
- OTTO OpenID Vocab : http://gluu.co/openid-vocab

OTTO Vocab defines several classes:
  Registration Authority
  Federation
  Participant
  Entity
  Metadata
  Schema

OpenID provides more specific classes:
  OpenID Provider (subclass of Entity)
  OpenID Relying Party (subclass of Entity)
  User Claim (subclass of Schema)
  Scope (subclass of Schema)
  Metadata Statement (subclass of Metadata)
  Categories (Defines values of enumeration like "OpenID Connect user claim")

An entity, like an OpenID Provider, could reference certain schema as supported by either linking to it, or providing the schema JSON-LD in the "supports" property. Of course, an array can be used to specify multiple schema objects.

Any schema object can specify certain common properties like:
  name
  description
  required (boolean)
  url
  category (to enable searches like: return all "OpenID Connect Scopes")
  sameAs

The "sameAs" property could be used to specify equivilancy. For example, an OpenID Connect Provider may use the claim "family_name", which is equivalent to "sn" in SAML. Using links enables the specific schema objects to describe what's relevent to their counter parties (like SAML2 URI, which OpenID Connect client's wouldn't care about.)

Currently OTTO has only defined a profile for OpenID Connect, but SAML is in the works. A profile for SCIM also seems like a good idea. Another advantage of using OTTO is that it is inherently extensible locally, or through the collaboration of standards groups or ecosystems.

Using OTTO to define a Fast Fed IDP response, perhaps it could look something like this:

```
{
  "entity": [{SAML IDP}, {OpenID Provider}],
  "Schema": [ {OpenID UserClaim 1},
            {OpenID UserClaim 2},
            {SCIM UserClaim 1},
            {OpenID Connect ACR},
            ...],
```

```
  "Organization": {}
}
```

The above syntax is simpler and is potentially more expressive, and more standard (by leveraging existing schema from schema.org).

Digital Life Collaborative

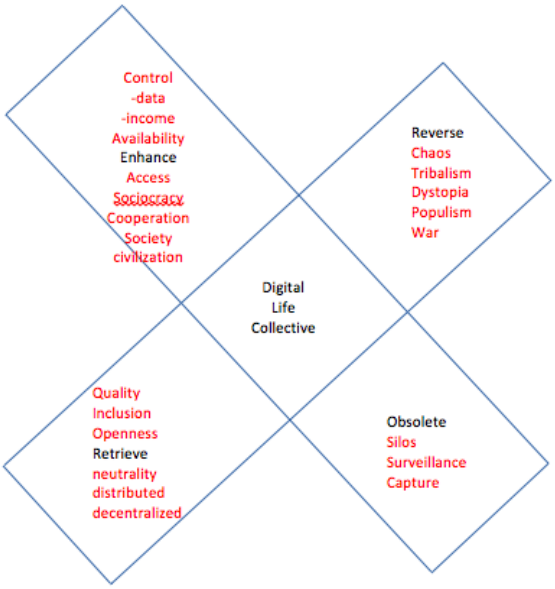
Thursday 3A
Convener: Adrian and Doc
Notes-taker(s): Sharon Franquemont and Mei Lin Fung

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

Digitallife.com and The Web We Want

I. Digital Life Collectivewww.diglife.com
   a. Please consider joining us or give us feedback. What suggestions do you have?
   b. Inspired by Phillip Sheldrake who tried various funding strategies to collectively design and actualize a web we want, the decision was to collectively fund and build this web.
      - One minute description is good and
      - Founder's prospectus clarifies it more
   c. By May 4, the Digial Life Collective has reached 135% of funding goal for starting.
   d. IIW community has the talent to build a new web as a collective, if desired
   e. Governance based on Sociocracy

2. Doc Searls' Power Point:
   - McLuhan and Identity
   - Applied McLuhan Summary:



Ehance:

- Access
- Sociocracy
- Cooperation
- Society
- Civilization
- Availability
- Control data & Income

Reverse:

- Tribalism
- Dystopia
- Populism
- War

Retrieve

- Quality
- Inclusion
- Openness
- Neutrality
- Distributed
- Decentralized

Obsolete

- Silos
- Survelillance
- Capture

3. Discussion Topics:

- New funding source: development of the crypto economics,, see white paper on, way beyond bitcon
- Members in commons, the collective
- Distributed web concepts
- How can we organize ourselves as a collective without degenerating into a dysfunctional group
- Ideal web:
    - *I want what I want when I want and where I want it.*
    - *Ubiquitous, free from surveillance, equality, control my own data*
- Governance of Digital Life Collective needs:
    - Constitution
    - Universal set of digital human rights
- Funding looking for a fourth business model
- ****New WEB must answer:
    - Why do I need it is instantaneously clear
    - Excitement, people "I want that!"
    - IMPORTANCE of visceral outcomes. Two immediate ones
        - Own my data, can make Money from that
        - Much greater Safety

The web we want www.diglife.com

I want what I want when and where I want it
I want to control and communicate those things at will if it has anything to do with me
Making something happen with identity

Usability for Identity Management

Thursday3F
Convener: Kent Seamons
Notes-taker(s): Tyler Ruff

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

Usability and Identity Management notes

Kent works in "Usable Security Research". A systems person who's gotten to do more human centric applications.
Attackers often focus on the users. SEcurity is not the primary taks but is a sendary concern. Draws upon security, HCI, social services
Security must be convenient or users will bypass it. "The more you make something, the less secure it becomes".
As security experts we can fail to design usable systems
IF it's usable and secure it's elegant

How can we measure usability? There's both qualitative and quantitative approaches. What are the risks to the users?
There's a congintive walkthrough. Think of a code review, but you walk through a scenario/use case step by step. Is this the persona approach? Could be.
Developers ask themselves what are the users going to do next? They go through screen by screen.
Need to go talk to users, not just 'step into their shoes'. Need to step back and ask yourself: Would any user want to use this?

Look at the "SUS questions" list of 10 Q's. They are the result of analyzing thousands of questions. You answer them on a 5 point scale. Agree/disagree.
Also look at the System Usability Scale (Brooke 1996) Top 15% of tools score well, but shouldn't be interpreted like any old college test.

Usability for secure email (example study of usability). BYU conducted studies with students and asked them to use various pgp tools and most tools utterly failed. 1 or 2 scored well. They've found that you can compare existing work out there and seeing how much better these systems score if you take a different usability approach.

If you don't train users, what do they think of?
You have to trust Signal because they control everything about the system. That is not a good model for long term security. Doesn't matter how secure a system is if no one will use it. The inverse is you have the appearance of safety/security but it's really not.
Signal is an improvement over SMS absolutely but it's not the end all best solution. There is an unavoidble conflict between functionality, usability and security. It's a slider, where on one end is funcionality and the other is security. People only use the functional applications.

People won't trust the perception of a single vendor which they need to trust. I

IF a UX person was in this meeting he'd say: You can't change user behavior. That's a no no. Also if you're teaching users you're dead already. But users today don't have good behavior and don't have a good understanding of security practices.

We have a very different mental model than the end user. We need a good UX guy to meld the two mental models: security focused and usability focused.

Users actually make pretty good decisions & risk analysis based on what they know. They just don't know very much.

Lessons learned:
-Hiding too many details results in a lack of trust
-Useres are concerend about the permanence of information
-Comparing separate systems has too many confounding factors
-Need careful A/B testing to understand _____ crap he changed the slide.... -___-

PICOs in Practice

Thursday 3G
Convener: Bruce Conrad
Notes-taker(s): Bruce Conrad

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

One-on-one tutorial introducing the node pico engine to Mark, Paco, and Armand, with much interest expressed and some specific projects discussed.

Interaction with Pico Labs starts at the home page: picolabs.io

Installation of the engine is done with the command

npm install -g pico-engine

We reviewed the developer user interface, and talked about rulesets that contain rules which respond to selected events sent to a particular pico on a specified channel. In response to events, rules might update the state of the pico and raise further events to be handled by the pico. Each event is evaluated in a single thread so that the programmer doesn't have to worry about critical sections.

We invite participation/questions/discussion through the Pico Labs forum and/or GitHub repository, both linked from picolabs.io

Reputation & Identity

Wednesday 4A
Convener: Sam Smith
Notes-taker(s): Dan Finlay

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

Reputation is a predictor of your future behavior.
Reputation is used to engage in a transaction.
Reputation is highly context-dependent.
When engaging in a transaction, you want to disclose the minimum necessary information to establish good reputation to the other person.
"The Principle of Least Disclosure"

Joe Andrieu: Privacy is about contextual integrity.
Nathan George said some

There is no one value of reputation, no one credit score.
Even the credit agencies get paid by banks for more context-tuned credit scores.
The value always just being the prediction of future behavior in this context.

Reflexive Reputing:
Reputable events are "Reputes"
A repute is a person (reputer) reputing a reputee.
Whoever is collecting a repute has an implicit repute going the other way.

When Amazon first released ratings, they were simply 5 stars and a comment.
Then people would just mob & vote up their friends & down their enemies.
Then they required you buy the item.
Now they let people rate reviews so that useful reviews can be prioritized to the top.

Kevin Serrano points out: A political book advocating "questionable things" could still have high ratings, because its readers are self-selecting for people who agree with it.
This is why you really want reputations as published by people ho trust.

Netflix does a good job of "Because you enjoyed…". Predicting *your future behavior*. Your likelihood of enjoying it.

Reputation algorithms themselves can have reputations.

What if Facebook had knobs that allowed you to tune the types of algorithm that forms your feed? Raise your tolerance for other views, perhaps?

Optimize your feed for the person you want to become.

Once we're in an open ecosystem, we can create incentive systems for bringing people into other ways of thinking.

You need a reputation for reputations.

Make XDI GREAT Again!

Thursday 4F
Convener: Markus Sabadello
Notes-taker(s): Markus Sabadello

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

We went over 2 projects currently underway that use Sovrin and the XDI protocol:

1. CULedger (http://www.culedger.com/) uses XDI for negotiating agreements and executing transactions between credit unions for the purpose of moving money, loan participation, and other financial use cases.

2. DiMe (https://github.com/HIIT/dime-server) is a personal data store project in Finland that will use Sovrin and XDI to establish link contracts and exchange data between personal data stores.

Anonymous Claims Authentication – Requirements and Sequences

Thursday 4G
Session Leader: Nat Sakimura, Nomura Research Institute, (@_nat_en)
Notes-taker(s): Nat Sakimura

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

Participants: Andrew Hughes, Sarah Squire, John Bradley, Carla Roncato, ..

Abstract
People talk a lot about such concepts like "anonymous", "verifiable claim", "claim authentication", etc. While it is a nice sounding words, it is not clear if they are speaking of the same thing when they use these words. It may as well be talking past each other.

In this session, these concepts were first defined to allow some precise discussion. Then, 12 abstract requirements for "Anonymous Claims Authentication" were built. For clarity, “Anonymous Claims Authentication” means “Claims Authentication in systems where anonymity is desired”. Finally, these requirements were examined against a possible implementation to check that these are indeed achievable.

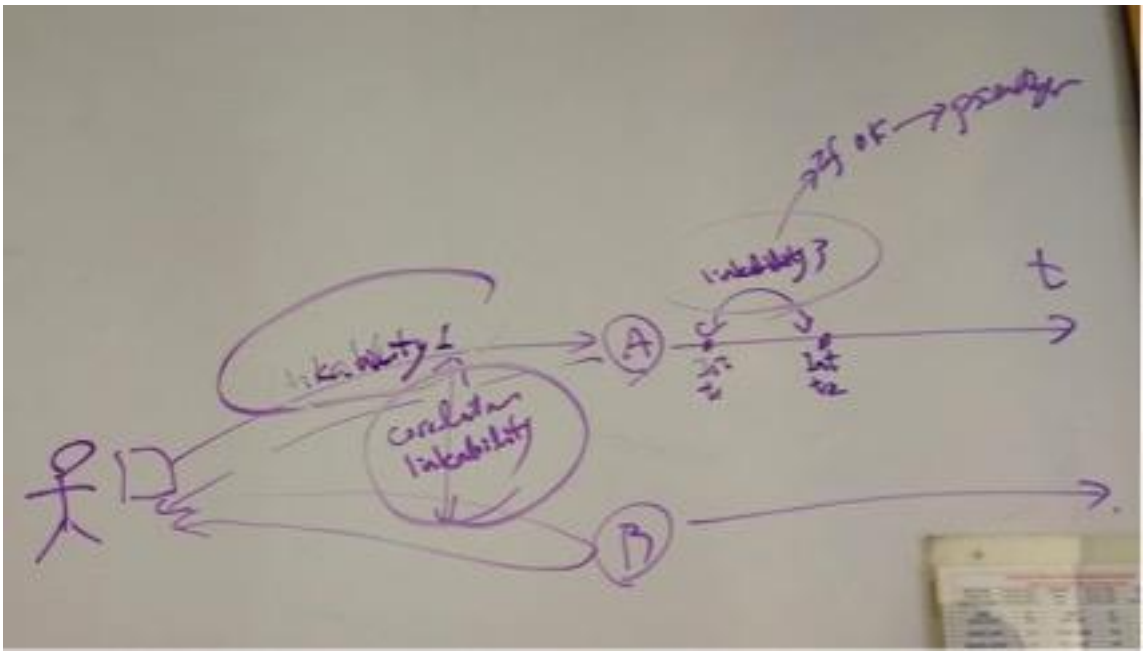
1. Defining concepts
At the beginning of the session, the following concepts were examined:

- anonymous
- claims authentication / verifiable claim

To define these concepts, the following model was introduced.

The first step is the user registration at the IdP. IdP must verify the claims related to the user upon registration so that it can attest the claims later.

Then the IdP creates claims set re: user (called authenticated identity) by user authenticating the user. Such authenticate identity is presented to the RPs. Such process is depicted in the following figure.



Here, through the ***user authentication*** by ***IdP*** (Identity Provider, claims issuer. The party that attests that the claims values are accurate to his knowledge), various "sets of claims" called ***authenticated identities*** are formed. These authenticated identities are presented to the ***relying parties***, ***RP***, (e.g., web sites, depicted as A and B in the above figure) to access services offered by those relying parties based on the value of the ***claims*** included in the ***authenticated identity***. There is a concept of time-lines depicted in the above diagram. When the user visits A at time t, then an authenticated identity denoted I_{At} is presented. For example, for t=1 and 2, then two distinct authenticated identities, I_{A1} and I_{A2} are presented respectively. Similarly, when the user visits B at t, I_{Bt} are presented.

Def: **Entity-Identity linkable**
In a system S, if A can link the user to I_{At}, then S is said to be entity-identity linkable for A.

Def: **Inter—RP linkable**
In a system S, if A can find out that I_{Ax} and I_{By} belongs to the same user, then S is said to be Inter-RP linkable.

Def: **Inter-temporal linkable**
In a system S, if A can find out that I_{Ax} and I_{Ay} belongs to the same user, then S is said to be inter-temporal linkable.

Then, with these linkability concepts, the participants examined what is meant by pseudonymous and anonymous when we usually refer to them. They agreed that when we say "pseudonymous", we usually mean RP-pseudonymous as follows.

Def: **RP-Pseudonymous**
If it is not Entity-identity linkable nor Inter-RP linkable, the system S is said to be RP-pseudonymous.

Similarly, when we say "anonymous authentication" etc., the "anonymous" usually is talking about "RP-anonymous" as follows.

Def: **RP-Anonymous**
If it is not Entity-identity linkable nor Inter-RP linkable nor Inter-temporal linkable by RPs, the system S is said to be RP-anonymous.

Def: **IdP-Anonymous**
If it is not Entity-identity linkable nor Inter-RP linkable nor Inter-temporal linkable by IdPs, the system S is said to be RP-anonymous.

Then, it was examined if it is possible for the RP to verify or authenticate the claims, i.e., to evaluate that the value is accurate to the desired probability, if S was IdP-Anonymous as well. It was agreed that it is not possible as there would be no party attesting the accuracy of the values of claims anymore.

As the result, the participants agreed that by "anonymous claims authentication" or "anonymous but verifiable claims", we actually mean RP-anonymous authenticated identities (clams set).

2. Requirements for RP-anonymous verifiable claims system
Then, the participants discussed what would be the requirements for RP-anonymous verifiable claims system. We started off from the 8 requirements that Nat prepared beforehand. These are prepared from what he has been hearing as requirements for such systems from various people so it is not using the concept defined above, but the participants mentally translated these in the above terms and verified that they are sensible.

1. RP MUST not be able to link two authenticated identities.
2. RP MUST be able to evaluate the level of assurance of the claims received.
3. IdP MUST be able to authenticate the entity at a required level of assurance.
4. IdP MUST be able to attest the accuracy of the claims value at a level of assurance.
5. IdP MUST not be able to determine where the assertion is being presented to.
6. RP MUST be able to determine if the assertion is forged.
7. RP MUST request only the minimum necessary claims.
8. IdP MUST provide only the requested claims.

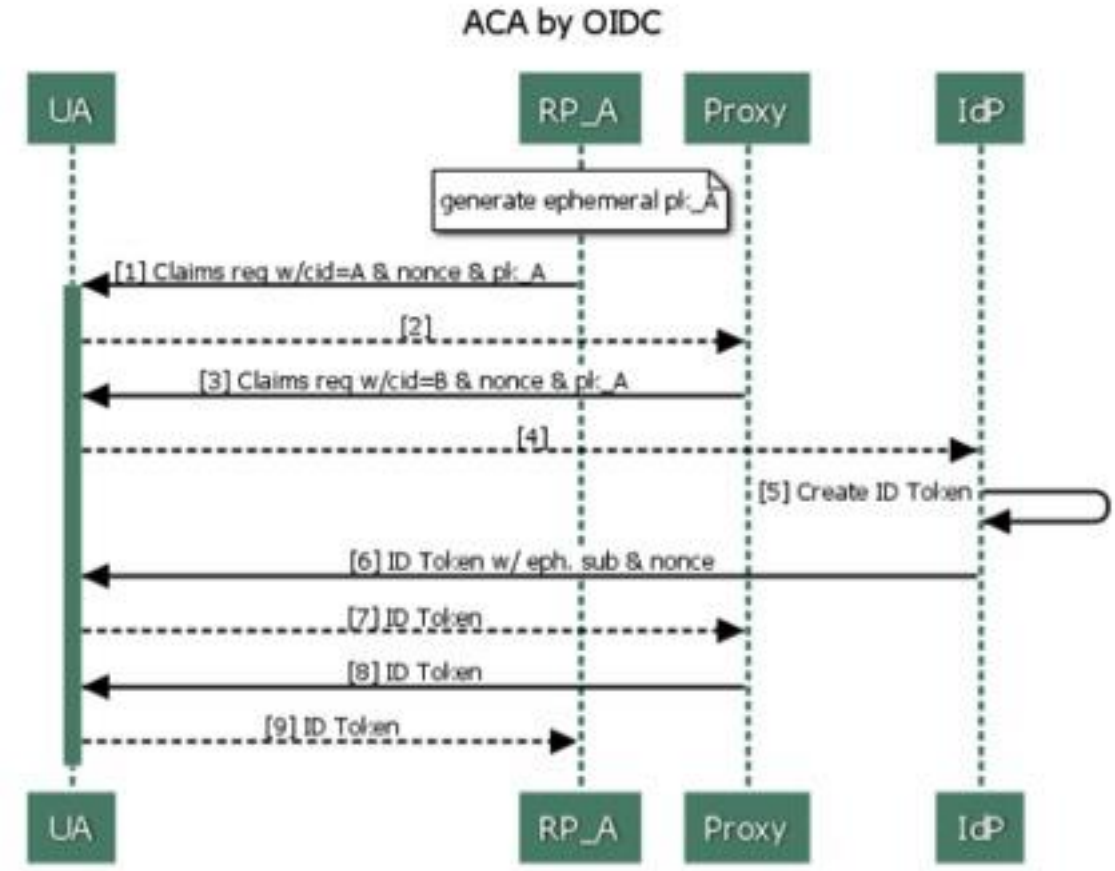
In addition, the participants came up with the following additional requirements.

9. Observers MUST NOT be able to link entities to identities (i.e., the system MUST NOT be Entity-Identity Linkable.)
10. Claims MUST be opaque to observers.

11. Authenticated Identities MUST BE non-transferable (Collusion resistant)
12. The system MUST be timing-correlation resistant so that colluding IdP and RP cannot compare the logs to find out retrospectively who went to what RP.

It is probably a good idea to re-state these in terms of the concept defined in the section 1, but as the time was running out and we wanted to join the closing circle, we proceeded to the next task.

3. Reality check – can it be achieved?
Finally, the participants checked if it can be achieved by briefly inspecting the sequence diagram that Nat has prepared, where Proxy in his mind was a self-issued provider so that there is no IdP-Proxy collusion issues. John pointed out that OpenYOLO can also be used. (Note: It is assumed that device finger-printing precautions are taken by the UA. Otherwise it is only RP-pseudonymous at best.)



Participants quickly verified that it seems to be satisfying the requirements 1 to 8.
Requirements 9 and 10 seems to be achievable through channel encryption and request/response encryption.
Requirement 11 can be achieved by setting nonce=token binding ID.
Requirement 12 can be tricky. It probably requires random wait at the proxy as well as large enough traffic to the RP. Alternatively, an operating scheme that ensures IdP-RP collusion can be introduced.

Finally, it was noted especially by John that system like this while often demanded by governments are not really useful. Specifically, the requirement 5 is irrelevant most of the time since the user trusts

the IdP. Otherwise, why does the user use IdP?. Sarah pointed out that the free choice is not always available to the user and thus it is important from the government perspective to be able to do this.

To close the meeting, Nat thanked the participants that as an editor of ISO standard related to this topic: *ISO/IEC 27551 Requirements for attribute-based unlinkable entity authentication* and that this session was very useful for him. Sarah asked what would be the use of such standard and Nat conjectured that perhaps vendors could self-attest or third party attested that they are compliant to such a standard. Participants agreed that it would be a good opportunity for an identity professional to get a revenue opportunity.

Sharing Systems Leadership

Thursday 4H
Convener: Kaliya
Notes-taker(s): Kaliya

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

Kaliya presented about a detailed report she has written to articulate how to engage in systems leadership in identity systems.

This is the introduction. Kaliya is working on a revised short version of the over 100 page report. If you would like to read it please contact her kaliya (at) identitywoman.net

Today's systems for digital identity are frustrating for people, businesses, civil society and governments. This report outlines at three phased, systems leadership approach, that the federal government can use to catalyze transformational change in identity systems. At this critical time the government cannot shirk its responsibility to ensure that these systems actually work and improve. As they are functioning today these systems are vectors of cybersecurity vulnerability. In addition the Homeland Security Enterprise depends on a smooth functioning scalable set of IdM and privacy systems. The government must nurture change to help the systems we all interact with daily become more efficient and more secure.

There is no single "answer" to solve the challenge of identity, there is only process that present a paths to get there. Starting with a pre-determined outcome will guarantee failure. While one can't have a pre-determined outcome, one can start with a clear intention, such as, *The new/resulting system work better for everyone*. Precise clarity about potential solutions and helpful actions the government can take within the communities of diverse stakeholders will only come in time and with the cultivation of strong networked relationships.

There is a real opportunity to take a leadership approach based on systems **"Systems Leadership"**. An article in the Stanford Social Innovation Review, *The Dawn of System Leadership*, co-authored by Peter Senge articulates three core capabilities that systems leaders develop in order to foster collective leadership. The author found this article after the report was basically complete and discovered that the three core capabilities it outlines map directly to the phases of this report. The first is the ability to *see the larger system*. The second capability involves *fostering reflection and more generative conversations*. The third centers on *shifting the collective focus from reactive problem solving to co-creating the future*.

If one starts with a small yet diverse representative group and then nurtures a community of stakeholders who understand each other and are motivated to work together by shared concern about the issues and challenges, the effort is likely to succeed. So *the way* in which the government seeks to catalyze change in this field is important. This is both because of the broad nature of identity affects literally everything and the sensitivity of the general public to government involvement in identity systems.

The report includes details on how a government agency can take a three phased approach to relate to people and build relationships and the processes and methods that might be used in each. Before getting to the details of the phases the report provides a review of complex systems and the reasons why identity itself is complex.

Phase One focuses on primarily on Naming and Reframing the challenges while identifying and inviting stakeholders to participate. As it progresses some sense-making (understanding the system) will be done by the stakeholders through the development of a series of field guides of key concepts. By the end of this Phase a core stakeholder group will have formed and will be in alignment about the challenges/issues and how to proceed to Phase Two.

Phase Two focuses on more intensive community building amongst stakeholder communities while they work together to figure out how the systems work today as they begin exploring visions/possibility of how it could work in the future. This would include uncovering

- What key elements are missing?
- What do people really care about relative to privacy stances of the actual available technology options?
- What do businesses need to support confidence in documents (physical and digital)?
- What regulations might need changes or updates to support new digital systems?
- What new laws would help create and enhance the functioning of the overall identity system and protect all of its stakeholders?

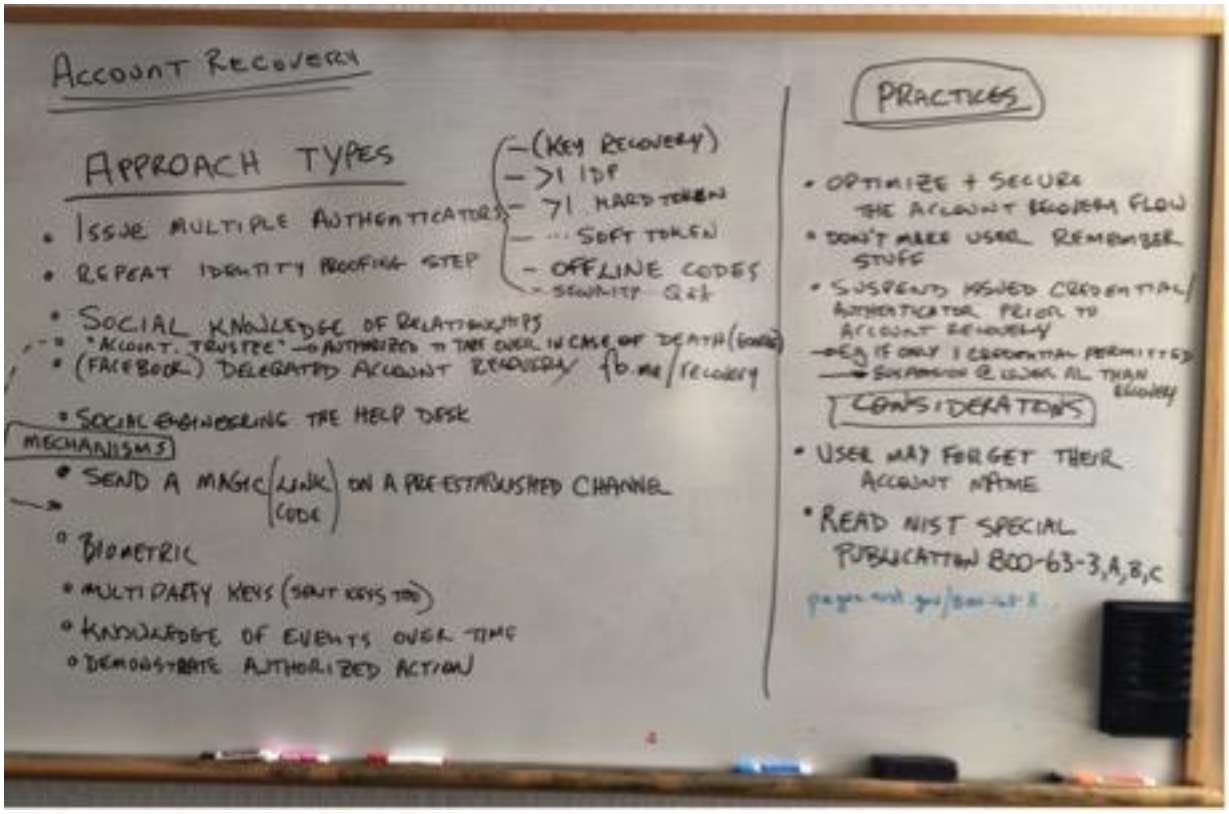
There are a lot of challenging questions and a wide range of stakeholder's who hold different perspectives and world views. Phase Two offers a variety of potential Mapping methods and related processes for gaining collective insight and taking collective action. This Phase will build collective will for joint stakeholder action to work together in improving the system.

Phase Three focuses on intensive collaborative action to catalyze system changes and co-create the future. It builds on Phase Two and many of the collective action methods will be appropriate to do the work of this phase. The Conclusion gives an overview of the document, shares research questions that arise from it and recommends initial steps to begin implementing the vision outlined in this report.

Account Recovery Systems

Thursday 5F
Convener: Andrew Hughes
Notes-taker(s): Andrew Hughes

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



OAuth JAR Working Session

Thursday 5G
Convener: Nat Sakimura, Nomura Research Institute, (@_nat_en)
Notes-taker(s): Nat Sakimura

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

Abstract
Four remaining points that came up during the IETF last call for OAuth JAR was discussed. The opinion of the participants were to partly revert the query parameter requirements to the WGLC version, add clarification on the semantics of request_uri, define a authorization server endpoint for accepting request objects, and add JWT parameters in the OAuth request parameter IANA registry.

Meeting Notes
This session was to discuss how to close the loose end of soon to become RFC OAuth JAR.
Those points were:
Plausibility of removal of query parameter parameters in the authorization request;
Simplification and concretization of request_uri location and clarification that it is at the discretion of the authorization server that where that location can be.
Clarification that request_uri does not have to be URL, but it can be URN.
Registration of JWT parameter values like iss, exp, etc. for the OAuth Authorization Request IANA registry.

1. Plausibility of removal of query parameter parameters in the authorization request;
In the IETF LC, a comment came in that the duplication of the values in parameter and in the request object was a waste and having unprotected values are a security risk. To accommodate the comment, all query parameters were removed.
Subsequently, a comment from Brian came in that client_id and scope is really useful in the query parameter for deployments for a couple of reasons:
The authorization server can use them as the switch to change the processing logics before parsing the potentially encrypted token.
Load Balancer etc can use the parameters to switch the backend server based on it. It cannot look inside of the JWT (especially when it is encrypted.)
The group decided that bringing client_id and scope would be a very good idea.

2. Simplification and concretization of request_uri location and clarification that it is at the discretion of the authorization server that where that location can be.
Brian pointed out that in many implementations the authorization server cannot make a query to the external network to fetch a potentially arbitrary content as it will cause a DoS if the content was very large, etc. The support of request_uri is very complex and he would not like to implement it.

Nat pointed out that
It is at the authorization server's discretion to decide the permissible locations of request_uri. It could constrain it to be within the authorization server itself as well.
While it will be more complex for the implementations since it now cannot be stateless, many customers (esp. banks) actually prefer it.

Some discussion ensued and it was agreed that defining an endpoint at the AS to accept the request object to give out the request URI would be a good idea. The result of discussion has the impact on two specs.
JAR: Make it explicit that it is at the discretion of the AS where the request_uri can be.
JAR: Create an AS endpoint to accept the request object and return the request_uri.
FAPI: in the mean time, have the request object endpoint duplicated in it as the deadline for FAPI is way shorter than for JAR.

3. Clarification that request_uri does not have to be URL, but it can be URN
It was authors' intent that when it is indicated as URI, then it does not have to be URL but it can also be URN. However, there has been much feedback asking "why does it have to be URL" from multiple directions.
It was agreed that it is a good idea to mention that the fact.

4. Registration of JWT parameter values like iss, exp, etc. for the OAuth Authorization Request IANA registry
Brian argued that JWT parameters need to be registered by this spec. at IANA sometimes ago.
Nat's response was that the comment came in too late and we are past IANA review that if we do it, we need to get back to the WG level.
However, as the result of the discussion in item 2., it is now clear that it will get back to the WGLC, so they can now be added.

Will Nationalism, Populism, Isolationalism Kill Identity Exchange? How to prevent the reification of Stateism?

Thursday 5H
Convener: Kaliya
Notes-taker(s): Kaliya

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

This was a wide-ranging discussion.
Books to READ - Seeing like a state.
https://en.wikipedia.org/wiki/Seeing_Like_a_State
https://books.google.com/books?id=PqcPCgsr2u0C&pg=PA11#v=onepage&q&f=false

We have built a vast book keeping system.

Some issues we are dealing with is when states go bad. How do we prevent their systems from being used for evil.

How do people without states actually get identity?
People NEED identity as attested by person, place, thing.

States define what is and isn't legal.

There can be offenses at the point of use - or the point of trade (such as no adds).

This could even be about moving certain types of data across boarders - but then they are also watching to see what is happening…

A VERY INVASIVE SYSTEM -… the cuddly police state is emerging.
We had a world that was local and distributed and now there is all this finding and sorting.

Two interesting state developments.
With the AD-Tech and Identity requirements in the EU.
The browsing in the US of EU citizens.

Recent rulings (I asked which ones but no one knew the name of the case) The United States said that data stored abroad by US companies is still subject to US law.

As populism grows/rises and states seek to reify themselves.

So with the US Travel ban on people from various countries could we see some kind of equivalent digital travel ban? ~ Exchanging attributes about certain people is

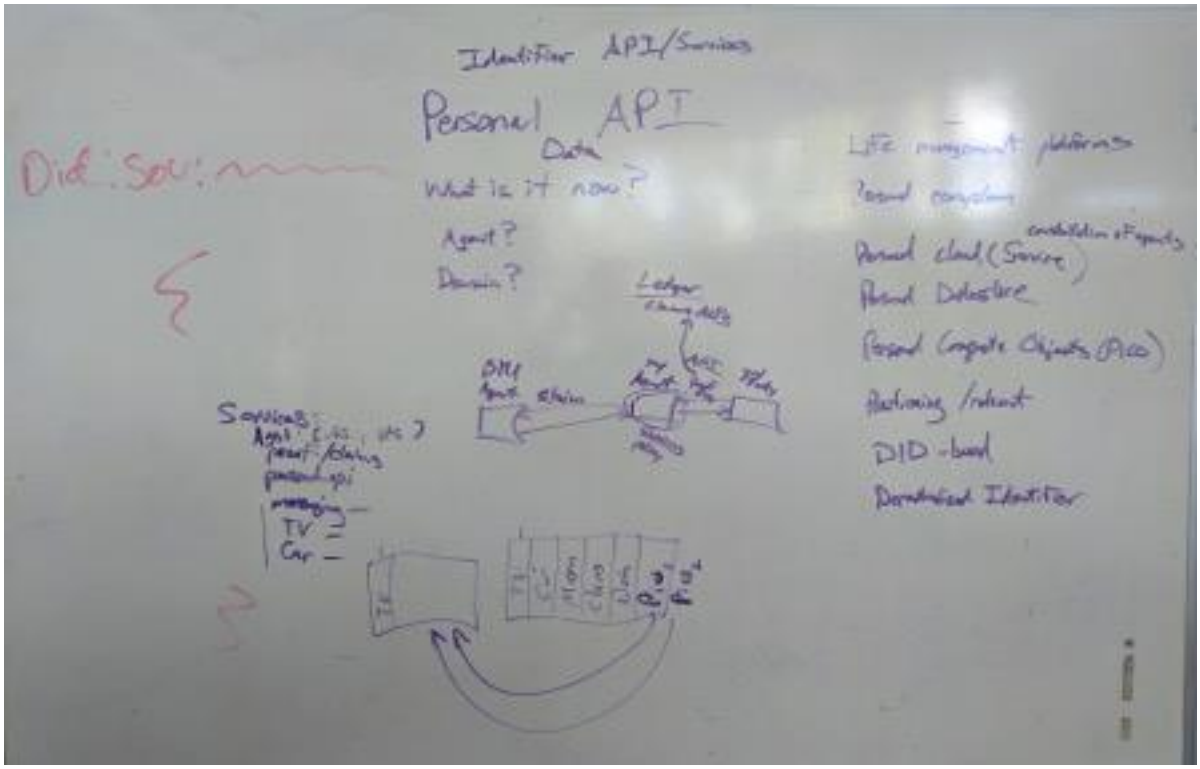
Ideas from Mei-Lin
We are still on the equivalent of the Louis and Clark expedition to the digital frontier.

The revolutionary war happened because of Mad King George and how people were treated.
It also happened because of the vast open frontier that people had to go .
With Identity we are on this new frontier.

Personal API

Thursday 5J
Convener: Matthew Hailstone
Notes-taker(s): Matthew Hailstone

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



Thank You to All the Fabulous Notes-takers!

There were 92 distinct sessions called and held. We received notes and/or white board shots for 79 of these sessions.

And welcome to our new Facilitation Team Member and Notes Wrangler Extraordinaire ~ Simone!

Photo credit #IIW @Nobantu

Demo Hour

IIWXXIV #24 Community Sharing / DEMO LIST
Wednesday May 3, 2017

Thanks to our Demo Hour Sponsor

1. **Serverless Sign In with Blockstack Auth:** Ryan Shea, Co-Founder of Blockstack
   URL: https://blockstack.org/
   We are pleased to demo Blockstack Auth - an authentication system that will allow users to sign in to websites without relying on any third parties or remote servers, Verifiable Claims Ecosystem.

2. **A Peer-to-Peer Trust Protocol:** Jon Nash
   URL: https://fiatdata.org
   A distributed, open source solution to identity confirmation.

3. **Consent-Informed Attribute Release (CAR):** Ken Klingenstein
   URL: https://spaces.internet2.edu/display/ScalableConsent/Scalable+Consent+Home
   We demo "Consent-Informed Attribute Release," an open system that enables user choice about release of their personal information-- or use of scopes, e.g "view family photos"--on a per-relying party basis. It can play with SAML and OAUTH/OIDC and is mobile and browser independent.

4. **uPort - Ethereum based digital identity platform:** Christian Lundkvist, Pelle Braendgaard, Rouven Heck
   URL: https://www.uport.me/
   We will demo the mobile application with a decentralized Ethereum application. uPort is building a global, unified, self-sovereign identity platform. On uPort, users and businesses create their identity and control their data, while securely authenticating to the world around them.

5. **digi.me -current PC/Mac, iOS and Android version application:** Jim Pasquale & Julian Ranger
   URL: http://digi.me for product & http://digi.me/video for vision
   Demo shows what users can do when they own and control their own data on their own devices(s), simply by "get it", see it", share it" for social, health, and financial data fully curated from multiple sources. Sharing
   data through Consent Access feature, flashbacks perspectives on social interactions with likes and comments, and universal search, customizable widgets for building collections, creating journals.

6. **MessageGuard:** Kent Seamons
   URL: http://messageguard.io/
   MessageGuard is a browser plugin for secure webmail. It has received high usability scores in the lab. It has a pluggable key management scheme. We recently compared PGP, IBE, and passwords. MessageGuard is the first usable PGP in a lab study, and scored almost as high as IBE.

7. **Cirrus Identity/Invitation Service for Sponsored Accounts:** Dedra Chamberlin, CEO
   URL: http://www.cirrusidentity.com/invitation/
   Cirrus Identity's Invitation Service - the convenience of social login for "guest" users, with the security of access control. Easily integrated with your SAML SSO! Enterprise accounts for guest users is a pain. Solution: secure social login from @cirrusidentity-all guests authorized by internal sponsors. Pre-built email flows.

8. **Vidently/Pre-OAuth Entity Trust (POET) - A mechanism for 3rd party application endorsement/trust:** Alan Viars
   URL: http://github.com/transparenthealth/poet &
   https://github.com/transparenthealth/python-poetri
   Pre-OAuth Entity Trust (POET) is a mechanism for 3rd party application endorsement and trust. It's based on JWT. Although it was designed for consumer-based health care applications functioning as OAuth2 clients, POET can be applied broadly in non-health and non-OAuth situations.

9. **Token Bound OpenID Connect SSO:** Brian Campbell
   URL: https://www.ietf.org/mail-archive/web/unbearable/current/msg01332.html
   Token Binding enables long-lived, uniquely identifiable TLS bindings spanning multiple TLS connections. Cookies and tokens can be cryptographically bound to the TLS layer, preventing token export and replay attacks. Demo will show a token bound OIDC login and resulting session.

10. **YubiKeys & Evolving the use of hardware backed identity:** Chris Streeks
    URL: https://www.yubico.com
    Yubico is the co-creator of the FIDO U2F open standard and the inventor of the YubiKey. We will provide a brief demonstration of an OAuth 2.0 flow using YubiKeys and FIDO U2F as the authentication mechanism. We'll also update you on the latest news regarding 2FA adoption and the FIDO ecosystem.

11. **Yoti:** Bruce Nash and Paco Garcia
    URL: https://www.yoti.com
    Yoti is your ID, on your phone. It helps you prove who you are to companies and people, online and in person. It takes 90 seconds to create your digital identity, which you can use to log into websites using your face, instantly know who you're talking to online and prove your age.

12. **TruSphere mobile app sign up / sign in without passwords:** Omar Shafie
    TruSphere's login technology enables a mobile app to sign up and authenticate its users without passwords. A sample Android app will be shown. The software tech is built atop unique asymmetric cryptographic keys, JWTs, and OAuth 2.0. No special hardware required.

13. **Auth0 - :** Jared Hanson, Chief Architect
    URL: https://auth0.com
    Auth0 is an extensible identity management platform that allows authentication and authorization to be easily added to consumer and enterprise applications. Supports industry standards including OpenID Connect, OAuth, and SAML

14. **Picos Everywhere:** Bruce Conrad
    URL: https://picolabs.io
    Extending the world wide web with persistent compute objects,supporting the Internet of Things while preserving personal freedom with an open-source pico engine that belongs to no one; everyone can use it and anyone can improve it.

15. **The Data Beyond Login:** Robert Burgess
    URL: http://www.gigyamedia.com/
    A discussion of CIAM authentication flow and progressive profiling.

16. **HIE of One Self-Sovereign Identity Container:** Adrian Gropper
    We demonstrate how a licensed physician writes a prescription into a patient-sovereign health record. Both the physician and the patient use self-sovereign blockchain IDs (uPort) and both have health record code running in their identity container.

The IIWXXIV Demo List can also be found here
http://iiw.idcommons.net/IIW_24_Demo%27s

Photo Credit @tomwihttheweath
Demo time at #iiw

Photo Credit #IIW @Nobantu

IIWXXIV #24 Photos

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

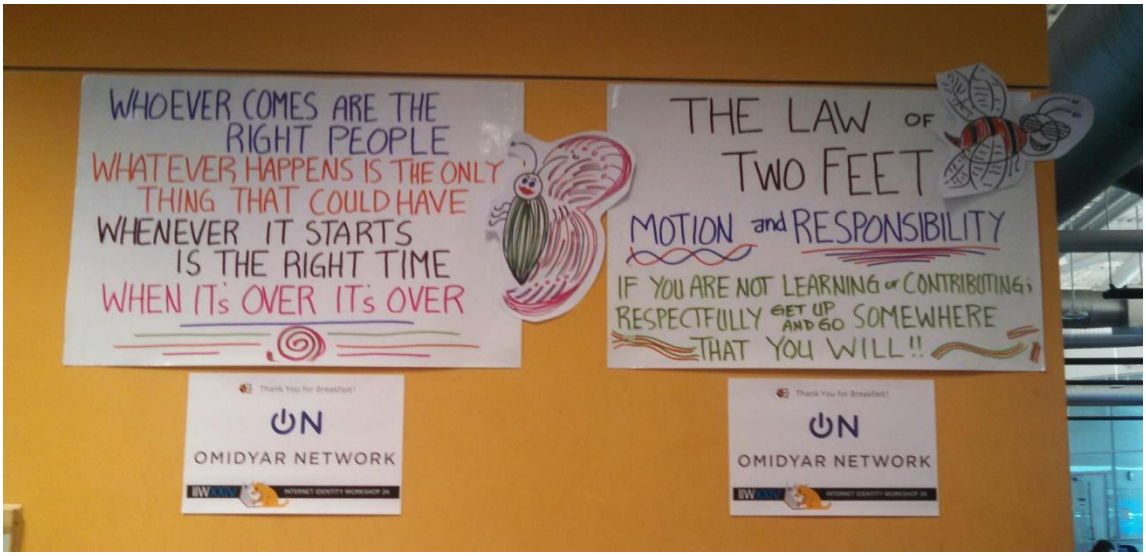


Photo credit #IIW @Nobantu

Photo Credit @justing_richer
Life on the interned, with… #iiw

See YOU
October 17 - 19, 2017

for
IIWXXV

Register here
https://iiw25-oct2017.eventbrite.com

for the 25th
Internet Identity Workshop!

www.InternetIdentityWorkshop.com