

IIWXX

INTERNET IDENTITY WORKSHOP 20

 identitycommons working group



Book of Proceedings

www.internetidentityworkshop.com

Collected & Compiled by
KAS NETLER, HEIDI N SAUL AND BARBARA BYERS

Notes in this book can also be found online at
http://iiw.idcommons.net/IIW_20_Notes



IIWXX

April 7, 8 and 9, 2015
Computer History Museum
Mountain View, CA

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



Contents

About IIW	3
IIW's 20 th - Retrospective and a Look Forward.....	4
From the Founders	4
What has happened over the last 10 years that you could not have imagined 10 years ago? .	5
What did you hope for that has not come to pass?	6
Looking ahead - What can you imagine/would you like to see this community/conference accomplish in the next 5 years?	7
At IIW	8
IIW 20 Session Topics	9
Tuesday April 7	13
Intimate Wearables Use Case.....	13
Trust & Consent: Consent Receipts for Personal Data Control	15
IndieWeb: Principles & Protocols to Own Your Identity / Get on the IndieWeb in Minutes ..	16
Personal Data Ownership in a Corporate World.....	18
The Emerging Field of Consent Management.....	20
VRM: Five Participating Groups ~ notes from 5 related VRM Sessions	22
PDEC - Personal Data Ecosystem Consortium - Growth & Opportunity	26
Lesson Learned: SAML and OIDC @ AWS.....	27
Distributed Capabilities - Systems for Real Time Communications	28
Fido U2F Update.....	29
Enhancing the Digital Currency Opportunity	29
New Business Models Based on Reputation (Part 1)	31
Mobile Profile Open ID Connect: Client Registration.....	32
New Pothole PICOs.....	33
IETC ACE Authentication & Authorization for Internet of Things.....	34
PDEC Call for Hot Topics / Papers	35
Local Re-Delegation with OAUTH	38
Blending Consumer Education and Enterprise Identities	39
Blockchain & Minecraft: Can Someone Tell Me About B/C @101.....	41
Notif Update - User Controlled Notifications.....	42
How the BLOCKCHAIN Can Solve All Our (identity) Problems.....	42
Wednesday April 8	43
Vectors of Trust	43
XDI Review & Demo /Personal Data Ownership in a Corporate World.....	44
SSO, Hello, and Passport: Updates to Identity in Windows	46

Clouds For Things.....	47
Can Technology Revolutionize Consumer & Citizen Activism?	47
Blockchain Tech 101 + Identity (onename)	48
What's new in PICOs + Cloud OS?	48
AWS Identity Round Table (Amazon Web Services).....	49
Privacy Issues Regarding Federated Login	50
Freedom Box Update.....	51
Fluffy are Kitties!	51
Bureaucracy & IoT (Internet of Things)	53
Workshop: best practices of profiles from 10 years of IIW	54
Defining data brokers; Use cases for disrupting data brokers; Governance/regulations	55
My Wave VRM: A Deeper Look	56
Terms we assert // Consent & User Submitted Terms.....	56
VRM In the Developing World	58
Honest(er) Ratings System: Let's Build It.....	59
OTTO = Open Trust Taxonomy for OAuth2.....	59
IIW Connectivity Between IIW's / Identity Commons	60
Identity Binding in the Extended Enterprise	61
Creating Trust at Scale in a Sharing Economy.....	62
OASIS XDI TC - open meeting	62
Put a Voter File into a Blockchain	64
A Guide for Integration of Authentication Technologies	64
UMA 101 - Everything You Always Wanted to Know About UMA but Were Afraid to Ask	65
Business Models Based on Reputation (Part 2)	65
Thursday October 30.....	66
TOS (Terms of Service) Back 2	66
Human Centric Computing/Scenario Planning of Avoiding the Compu Serve of things	67
Identity Anthology: Input & Feedback	68
My Own \$5/mo UMA Authorization Server	70
Useable PKI.....	72
API Fusion Drives	73
Enterprise Single Sign On and Social Network (mobile centric)	74
User Terms Continued	74
Digital ID Images.....	76
Implement Indie Web on your service in minutes (Indie Web Camp).....	81
Open Notice and Consent Working Group.....	81
[In] security Sessions.....	83
Architecting Future Scenarios: Digital communities that self-balance on reputation, privacy & other norms // Pen Names.....	83
Mozilla Listens to IIW	84
H.E.A.R.T. Working Group Session - UMA Security Profile	87
The Third IIW Women's Wednesday Breakfast	88
Thank You to All the Fabulous Notes-takers!.....	88
Demo Hour	89
Happy Birthday IIW!.....	Error! Bookmark not defined.
IIWXX #20 Photos by Doc & John H.	91

About IIW

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

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

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

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

The event is now in its 11th year and is Co-produced by Kaliya Hamlin, Phil Windley and Heidi Nobantu Saul. IIWXXI (#21) will be October 27 - 29, 2015 in Mountain View, California at the Computer History Museum. Super Early Bird registration is open now at: <https://iiwxxi-21.eventbrite.com>

IIW Events would not be possible without the community that gathers or the sponsors that make the gathering feasible. Sponsors of IIWXX (#20) were:

[Microsoft](#) ~ [Google](#) ~ [Gigya](#) ~ [Yubico](#) ~ [NetIQ](#) ~ [VMWare](#)
[JanRain](#) ~ [Nexus](#) ~ [Qredo](#) ~ [ForgeRock](#) ~ [Mozilla](#) ~ [IDICIA](#)

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:

IIWXXI #21 October 27, 28 and 29, 2015
IIWXXII #22 April 26, 27 and 28, 2016



"IIW is the mecca for identity and privacy innovation. It's beneficial for newbies and it's an essential collaboration forum for the stalwart pundits who nurtured this emerging field."

Mike Schwartz
CEO Gluu

IIW's 20th - Retrospective and a Look Forward

From the Founders

When IIW started there was no such thing as “internet” identity. Identity was an enterprise thing and the idea of Web sites and other Internet applications federating identity was brand new.

IIW was committed, from the start, to problems around personal identity and the issues associated with people controlling their online identity and accounts. IIW's continuing role is to provide a *neutral ground* where companies and other organizations that need to cooperate on Identity can meet and work together without NDAs and other friction.

IIW is a protocol seeding and cultivation ground. It helps move many things forward by steps over time. I remember when SCIM was just an idea on the agenda wall, a session called, "Cloud LDAP". No other conference has done more for more different code bases and causes than IIW. Over the past 10 years this has also included...

- Kim Cameron's “laws” (which are truly valuable) were hammered out at IIW, to some degree, along with Microsoft's now-dead information cards.
- OpenID may be the biggest thing, since it began with Brad Fitzpatrick handing over his code at the very first IIW in Berkeley, and has evolved much since then.
- OAuth, XDI, UMA and several of the lesser known federated social web protocols were started or work on significantly at IIW.
- Phil's picos and other approaches to IoT have benefitted from IIW.
- PDEC grew out of IIW, as did many different forms of personal data stores, lockers, clouds, vaults and services, by all those different names and more.
- Markus S. is the only person to actually build a working and useful Freedom Box, though that conversation mostly happened elsewhere, he has brought each new iteration for ‘show and tell’ and feedback.
- I credit IIW with helping enormously with VRM

IIW consciously created a ‘community’ space through arranging for and providing dinner each evening so conversations could continue and relationships developed further in a social setting. Over the past 10 years we've lost several community members whose spirit and contribution to the world were cut short early ~ Nick Givitoovsky, Bob "RL" Morgan and Eno Jackson.



“I’ve been attending IIW for many years, and it provides immense value every time. The event promotes progress in one of the most exciting and consequential realms anywhere in the world of technology, and the unconference format brings out the best in experienced identity practitioners and newbies alike.”

Eve Maler
VP Innovation & Emerging
Technology - ForgeRock

IIWXX was opened by asking participants to write down the answers to several questions and then share their answers with each other. The written responses have been transcribed below.

What has happened over the last 10 years that you could not have imagined 10 years ago?

- Geolocation
- The rise of the sharing/reputation economy
- Consumer Scoring
- Shifts in the roles of the 'Titans' (Apple, IBM, Microsoft)
- Shifts in the computer market
- The evolution of new silos based on old business principles (e.g. Facebook)
- Inter-Domain relationship sharing
- Everyone carrying around mobile devices
- Willingness to put private data in the cloud
- Audience segmentation
- Air BnB, UBER, LYFT, Task Rabbit
- The current level of cooperation/integration globally ~ not near enough, but better than I thought
- Total dominance of centralized capitalist models
- Complete suppression of pseudonymity
- So much data leakage theft / Widespread security breaches
- Twitter / Bitcoin
- That Google, Facebook et al, are shifting towards personal privacy services
- Development in mobile devices
- Personal data is so at risk
- Subscribing to music, i.e. Spotify
- Multi-dimensional information
- Proliferation of ad-tracking based on identities
- Facebook would "supersede" the Internet in various countries and cell phones would approach proxy for identity
- Still using passwords as primary auth
- Challenge for web-apps by smart phone apps
- The event – IIW – continues, the conversation continues
- Democratization of info + services via mobile/smart phones
- I'm working in an identity community
- Including legal frameworks and policy
- Laws just pushing liability around – not solving anything
- Cloud computing
- Things are the Things now
- The mainstream embrace of P2P structures (in learning, business etc...)
- OpenID AB & Connect coming together
- Selfie sticks & the implications that one selfie enough to need one
- OAuth – Internet-wide access control federation
- Personal privacy + identity has become a topic outside of IIW
- Rise of Twitter ~ global messaging
- MLS vendors adopting "PUID" = Property UniqueID, setting stage for open ecosystem in Real Estate
- General public adoption of smart phone technology
- The distributed ubiquitous surveillance network
- Idm, governance and security convergence
- Bohemian RHAPS – ID
- The emergence of REST + JSON as common sw dev patterns
- Shared signals
- PC to Mobile
- Loss of privacy
- The shift from emphasis on authentication to emphasis on authorization, largely due to OAuth2
- Social Login
- This being my first IIW, I could not have imagined being at IIW because I didn't even know it existed
- Government Agencies sharing data
- Lack of concern in younger generation regarding identity privacy
- Identity as a domain
- Assisted reality
- Monopoly of the Social Commons by Tech Corps
- Lack of concern about personal privacy by consumers
- The Maker Movement
- I never imagined that people would share their entire life on line / Excessive sharing of personal information
- That the evolution of online identity would be so slow
- That we would assent to massive privacy violations
- FIDO as a standard authentication solution
- Could not have imagined that we'd go 10 yrs and still have not widely adapted interoperable standards
- Mass surveillance with substantial public acceptance
- The embrace of the sharing economy

What did you hope for that has not come to pass?

- Advertising is still a viable business model
- No more password only auth
- SSN is still a thing
- I wish I had been coming to these earlier
- Why don't I have a VRM system? (Where is my flying car?)
- Distributed identity & social networking as opposed to walled gardens
- Digital Identity for Dummies ~ the book
- ECPA Reform
- Innovation for social change
- The distributed ubiquitous surveillance network
- Get rid of passwords
- New business models – Valuation of digital services
- Multilateral trust
- Lack of high speed data across the U.S.
- Identity Federations
- Secure communication everywhere
- That the internet would be a safe place by default
- No more passwords / End of passwords / We still have passwords!
- Most people still have not taken control of their own identity
- OAuth – fine grained access checks (?)
- More crypto to be used for privacy / security e.g. Remote voting systems
- Service providers take security seriously
- US National ID Program
- OAuth service to service communication
- Liberty Alliance Interoperability – emphasis on interop (and it won't come to pass)
- Hoped for Cow – Cow!!!
- Data 9/11
- Information Cards / Internet-wide claims (self & third party asserted)
- That we would still need this conference
- VRM to be mainstream
- Decentralized user managed social media
- Obsoleting of native applications for most tasks
- Decentralized ID – Open Linked Semantic Data
- Interoperable Identity & Data Sharing Standards
- PKI to be used everywhere for security authentication
- Hasn't Happened / Home Buyer ID, ability for homebuyers to manage own real estate identity
- Personal Health Records
- Micro payments
- Fully immersive virtual reality
- Privacy Preserving Identities
- Easy identity syncing between enterprise products
- Lack of wide consumer interest in privacy
- Global Gov w/enforcement power that does not lend itself to tyranny
- Fewer identity silos
- I had hoped for improved identity security in the US (like EU)
- Better Privacy Protection
- I had hoped inter-domain friend requests and relationships would be a standard by now
- Compliance that means something real, not just checking a box
- The rise of Facebook, Google+, linkedIN and Twitter as effective owners of our identities with the ability to terminate our digital selves for any reason feels like a failure



Looking ahead - What can you imagine/would you like to see this community/conference accomplish in the next 5 years?

- Provide authenticators that speak to privacy
- Greater personal ownership of personal data
- Actual digital data ownership
- Eliminate Passwords – Solve the “password” problem - no more passwords – fix passwords
- Passwords 80% gone
- Less least privileged access & more activity monitoring
- No password ID
- Stop bugging banks about becoming IDPS :)
- SCIM in all SaaS products
- Privacy beyond compliance
- Wider adoption of OpenID Connect
- Better controls for how my identity is used on the internet
- VRM to become dominant tech for customer/brand interaction
- Standardized PDS/personal cloud used everywhere
- Community based identity providers
- Identity/authorization is more freely, but appropriately shared. NOT the property of organizations
- Legal/policy Interoperability – Distributed “Intergovernance”
- I’d like to see privacy & security by design a reality
- Secure and convenient identity solution
- Inter-domain relationship sharing
- Privacy by design
- Usable encryption tools (useable by novice users)
- Kill Facebook
- A marketplace where convenience, privacy, security can be chosen
- Protocols are programs, downloadable and create layers of interoperability
- Viable policy + technical foundation(s) to make security and privacy tools better + easier to use
- Continued standards refinement/recommendations + use cases more clearly socialized
- UMA – Internet wide claims with central owner control
- Privacy in a connected world
- Instrumental in achieving an identity outcome that works for citizens
- Accessibility and accountability in privacy
- IoT security that is appropriately strong and complex (simple)
- Good VRM tools to help my life
- External education beyond the community – beyond our industry
- Clear set of standards
- That service providers will take (identity) security seriously
- Personally owned/controlled identities (not even service can access)
- Put the voter file into blockchain
- Open Decentralized Standard
- Improved Internet of Things security
- Get rid of my wallet
- Social Media ID proofing
- Kill indemnity – Long Live Reputation
- Ubiquitous delegated AuthZ & AuthN
- Mobile payments – no wallet
- Determine an accessible VRM solution for daily/weekly purchases, household, entertainment, business expenses
- That IIW will be full of end users – not just technology people
- Rich sharing over internet
- There will be safe spots on the internet
- Prove that free people are worth more than captive or followed ones
- UMA becoming a widespread reality for users
- Google drive fixes its sharing model
- Appropriately priced, perfectly secure hosted storage
- The singularity
- Tackle major foundational pieces toward defining privacy framework, policies
- Interoperable Identity & data sharing standard
- View privacy as identity “channel integrity”
- A consistent/seamless way to define, manage identities
- neo LOA
- Less walls around gardens, more choice, simpler to explain to end users
- IIW attendees bootstrap Products that grow into platforms
- Interoperability
- Separation of internet identities (ability to have more than one)
- Closer time gap between thought learning to beneficial products/services

At IIW ...



We do
Open
Gifting
at the
end of
each day.



A time when
anyone can
thank a
colleague for
leading a
great session,
having a
helpful
conversation,



along with
acknowledging
ongoing
contributions to
work happening
in the
community in-
between IIW



"IIW has played a vital role for the development of today's open identity standards. All the people that understand the bits and bolts and challenges are there. Thank you IIW for providing this rare space!"

Stina Ehrensvar
CEO & Founder of Yubico



IIW 20 Session Topics

Tuesday April 7, 2015

Session 1

- Inter-Domain Relationship Sharing & Friend Requesting
- Intimate Wearables (AKA IoT)
- Trust & Consent / Consent Receipts for Personal Data Control
- Hacking Privacy Policy by Managing Politicians
- IndieWeb Principles & Protocols to OWN YOUR IDENTITY
- Personal Data Ownership in a Corporate World

Session 2

- Engaging Voters Through A Policy Management Game
- The Emerging Field of Consent Management - Next Gen UI Infrastructure Under the Hood
- VRM: Customer Needs - Definitions
- Personal Data Ecosystem Consortium - Growth and Opportunity
- Lessons Learned - SAML & OIDC @AWS
- Distributed Capabilities - Systems for Real Time Communication

Session 3

- FIDO U2F Update / What's New & Drawing Board
- Enhancing the Digital Currency Opportunity
- VRM in the Developing World
- VRM: Vendor Needs - Definitions
- (new?) Business Models Based on Reputation
- Mobile Profile OpenID Connect (Part 1 working session)

Session 4

- IoP: Net of Policies - Phil W's Personal Pot Hole (PPP)
- IETF ACE - Authentication & Authz for Internet of Things / Scenarios & Solutions
- PDEC - Call for Hot Topics / Papers (Personal Data Ecosystem Consortium)
- Mobile Profile of OpenID Connect (Part 2 working session)
- Local RE-Delegation With OATH
- Blending Education, Consumer + Enterprise Identities / Identity in the Academy (and beyond)
- Blockchain and Minecraft - Can Someone Tell Me About B/C

Session 5

- Modeling Privacy Policy in a Political Management Game
- The VRM Value Proposition (Biz Model Canvas)
- Account Chooser and Mobile Connect / What must we change?
- Notifs Update
- Get on the IndieWeb in Minutes
- How Blockchain Can Solve All Our (identity) Problems



Wednesday April 8, 2015

Session 1

- Vectors of Trust
- XDI Review and Demo
- SSO, Hello and PassPort - updates to Identity in Windows
- Cloud for Things
- Can Technology Revolutionize Consumer Citizen Activism

Session 2

- Trust Elevation
- Blockchain Tech 101 + Identity (onename)
- What's New in Pico's & Clouds?
- University Community (InCommon, Internet2, Identity Registries, API's)
- GovTrain - CluGov
- AWS Identity Round Table (Amazon Web Services)
- Privacy Issues Regarding Federated Login's

Session 3

- Freedom Box Update
- Fluffy are Kitties
- Blockchain Based Authentication
- How Do I Find Out Where I Can Be Involved in Standards & Policy
- Bureaucracy & #IoT
- Influencing Social Expectations of Online Info Services Through Ecosystem Codes of Practice
- Workshop: Best Practices of Profiles from 10 Years of IIW

Session 4

- Distributing Data Brokers
- MyWave VRM: A Deeper Look
- Terms We Assert / Consent & User Submitted Terms
- VRM In the Developing World
- Honest(er) Ratings System - Let's Build It
- OTTO = Open Trust Taxonomy OAuthz / Session #1 Charter
- IIW Connectivity Inbetween IIW / A Discussion of Identity Commons Community Looking Ahead

Lunch

- Business Models Based on Reputation Part 2
- IIW Like Events in Other Countries

Session 5

- XDI TC - Open Meeting
- Identity Binding in the Extended Enterprise
- Creating Trust At Scale - In the Sharing Economy (Why do we let strangers stay in our homes?)
- Put a Roter File into a Blockchain
- VRM: Market Maker
- A Guide for Integration of Authentication Technologies
- UMA 101 - Everything You Wanted to Know About User Managed Access But Were Afraid to Ask



Thursday April 9, 2015

Session 1

- NAPPS Update - Native Apps SSO (a working group of OIDF)
- Haman Centered Computing/Scenario Planning or Avoiding the Compuserve of Things
- TosBack 2 / Terms of Service + Privacy Policies Archiving + Analysis
- Identity Anthology - Input and Feedback

Session 2

- My OWN \$5/mo UMA Authorization Server
- This is the Year of PKI! Useable Crypto?
- API's (Fusion Drives)

Session 3

- Enterprise Single Sign-On and Social Networking *Mobile Centric*
- User Terms Continued...
- Digital ID Images - Sharing visuals that you created that clarify some issue.
- Implement IndieWeb on Your Service in Minutes

Session 4

- Open Notice + Consent Receipts Working Call-In/Working Session
- VRM FrameWork: Define the Developer Role in the VRM Framework
- [in]Security Questions

Session 5

- Meet 'Frank' The MyWave VRM Personal Assistant
- Pen Names (creative expressions) Separation of Multiple Identities Over Time
- Architecting a "best" Scenario: Digital Communities that Self-Balance on Reputation, Privacy & other Norms
- Mozilla Listens to IIW
- RISC = Risk & Incident Sharing & Coordination (working group of OI DF)
- H.E.A.R.T. Working group session - UMA security profile (Health Relationship Trust)

Tuesday April 7

Intimate Wearables Use Case

Tuesday 1D

Convener: Adrian Gropper

Notes-taker(s): Judy Clark

Tags for the session - technology discussed/ideas considered:

Tagged: [autonomy](#), [health](#), [law](#), [medical](#), [physical](#), [regulations](#)

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

See paper here: <http://hg.openid.net/heart/wiki/Post-MI Implant and Rehab>

HEART – Post-miocardial infarction and rehab use case (real use case)

- Implantable cardioverter defib
 - rhythm: fibrillation/shock, preamble, lead degradation
 - follow-up, info goes to cloud
 - trigger ← programmer (must be open source? Trust issues)
- Fitbit tracks activity, relay data, provides context, public health and research
- MD1 and MD2 (doctors who are involved)
- Cloud stuff
- Applications as relay, other functions

Everything works today. Posing questions about open-ness of the system?

- Risks
- Trust
- Control
- Regulatory (disproportionate impact, drives standardization, silos) – partners to be chosen at edge, vs enterprise?
- Standards
- Supply Chain

Hoping to learn how to push this use case through regulatory process, taking the spirit of IIW and communicate that in other parts of Adrian's work; how to communicate the issues more effectively.

Discovery of separate info channels and value. Patent law makes part of this discussion a separate set of relationships. Non-technical standardization is behavior, lack of reliability by people and institutions. Need multiple trust frameworks. Behavioral specs: what's behavioral shift that's desired, communication between doctors and patients. What are options? Having doctors identify with patients is a challenge.

This is mostly an edge use case. Ideally the system would be open source, no proprietary stuff. Could be a distributed system.

- FIDO: uses pairwise pseudonymity by default. Question about why FIDO is relevant, if main purpose is to get rid of passwords, not problem of IoT things. Federation first or Control first? Don't need to choose if we use FIDO for security. Doesn't solve federation, just authentication. "Supply chain is like a valley of risk and opportunity—all marbles roll down into valley." What Adrian wants: autonomous relationship with doctors, professionals. Q: moving around the world, will standardization change? A: example of glucose pump for fabricated pancreas. Q: who is it sharing data with? A: who is in control—patient and doctor's programmer? FIDO can include biometrics as authentication.
- Dynamic registration: OAuth central, UMA, high privacy protections?

"Metabolism as a service." Communication with your personal server (or cloud—personal or enterprise)

- Other issues:
 - you want to be able to interact with enterprise world. To do that, you have to have a couple of pieces:
 - group design is crucial
 - interface agents that deal with professional regulation as well as legal regulations

Desire to preserve autonomy, learn lessons from blockchain, introduce frameworks (UMA, other) to drive

Politics around dynamic registration.

Too much imposition of controls becomes "death panels." Balance between regulating thru FDA vs regulating by licensed professional being sued. How to best protect safety, maintain autonomy? Here's the whiteboard from the session: (Photo credit Scott Mace)

[Continue →](#) 2015 April 7 · [friends/family](#), [future](#), [history](#), [records](#), [tools](#) · [Leave a comment](#)

Trust & Consent: Consent Receipts for Personal Data Control

Tuesday 1F

Convener: Mark Lizar

Notes-taker(s): Mark Lizar

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

Introduction to the consent receipt, how a record of consent creates transparency over data control and how the use of the receipt by the individual creates trust.

We discussed consent receipt in the UMA flow, and we discussed how consent receipts facilitate user submitted terms. We focused in on how consent management terms can be submitted.

There was a lot of detail around the compliance of consent and liability issues which are compelling for organizations.

IndieWeb: Principles & Protocols to Own Your Identity / Get on the IndieWeb in Minutes

Tuesday 1H & 5H

Convener: Kevin Marks

Notes-taker(s): Darius Dunlap

Tags for the session - technology discussed/ideas considered:

#indieweb

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

Kevin started by presenting the basic concepts of Indieweb. This all exists at <http://indiewebcamp.com>, so we will provide limited notes here for context and links to useful resources with more complete information.

Back to first principles of the Web:

<http://indiewebcamp.com/Principles>

- My identity on the web is my website.
- I communicate by publishing things there
- Each of my posts pushes out from there to various places, depending on needs, purpose, post type, etc.
- Interactions on those various places also are pulled back into your own website, so that you can see, for example, "Kevin Marks liked this on Facebook".

There is also an Anti-definition: avoiding the Silos

Several companies and organizations have built something “open” that really just turns out to be alternatives to the commercial silos, but end up with many of the same problems. Most fail. See Also: <http://indiewebcamp.com/sitedeaths> [Check link]

But The Silos are Actually Interesting and Useful

Twitter, Facebook, Instagram, Google+, Flickr, etc. have real uses that people like. Your friends are there, interesting people are there, they are useful, usable, and have attractive apps that make them easy and pleasant to use. So we connect to these services and cross-post or “syndicate” things from our own website to these services as needed. For example, you post an interesting link to your website and the link and title get posted to Twitter. We call this POSSE.

POSSE Overview

This is the idea that you can “Post (on your) Own Site, Syndicate Elsewhere” Example:

I post to MySite, and the Title and Link are posted to Twitter, and the Title, link and an Excerpt are posted to Facebook. <http://indiewebcamp.com/POSSE>

PESOS

“Publish Elsewhere, Syndicate (to your) Own Site”

Because some online services provide tools that are compelling. The Instagram App, for example. If you like that service, the right thing to do is just make everything you post there syndicate back to your own website. We Call this PESOS. <http://indiewebcamp.com/PESOS>

The Glue that makes it all work

To make this all work, there are some protocols and tools that make it easy. Webmention
Webmention is a protocol that allows someone at one site to mention a
<http://indiewebcamp.com/Webmention>

Brid.gy

Brid.gy is a service that connects up the silos to webmention. It provides the round-trip of likes and mentions on Facebook and Twitter (for example) back to your own site.
<http://indiewebcamp.com/Bridgy>

IndieAuth

OAuth-based authentication using your domain as your identifier. IndieAuth goes to your domain and finds the rel="me" links, and gives you a choice of any of those which provide OAuth. What's important here is that you are logging in using your domain as an identifier and some linked OAuth provider as authentication. if you come back to login again, you don't have to remember which OAuth provider you used. Any of the ones that you have linked up properly will work.

More info:

<http://indiewebcamp.com/IndieAuth>

MicroPub

A lot of the posting mechanism is powered under the hood by Micropub, which is a defined way of posting structured data to a site.

<http://indiewebcamp.com/Micropub>

(This page is formatted oddly, with an index at the beginning, so scroll down for a huge amount of detailed info.)

How get Started

<http://indiewebify.me/>

This is a walk-through that takes you through all the steps, providing tests of each functionality and links to useful resources for getting everything working.

Where to find out more

<http://indiewebcamp.com>

IRC - #indiewebcamp on freenode

Events:

<http://indiewebcamp.com/events> — includes:

- Homebrew Website Club
- Indie Web Camp

Personal Data Ownership in a Corporate World

Tuesday 11

Convener: Annabelle Backman

Notes-taker(s): Hugh Pyle

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

[Annabelle] Want a discussion - lots of questions, but don't necessarily have any answers. We're in a corporate world: our information is handed over to companies, for storage, communication, and so on. Companies hold our data, but can we trust them with it? E.g. facebook, google. Let's look at alternatives - e.g. "home box" type solutions, then somehow maybe facebook (etc.) integrate with it? How would we make that manageable by the consumer? Then, even if we solve those problems: how do we get the hosting companies to care about these private-cloud solutions?

[Patrick, Eric] There's a question of how to get people to care about privacy. It's an uphill challenge. Can we give users a reason why they should *own* their data? Value or convenience

[Annabelle, Didier] Q: in EU it seems the government is more involved in privacy issues; does that reflect a difference in public feelings? Maybe not; concerns about privacy in US post-Snowden seem to be at least as important. In France example, there's a history >40years of state regulations in this area.

[Hugh, Bob] Apple has an interesting stance here, "we don't want to see your data" & commercial model from hardware. But: it's different to say "we don't want" versus "prevent", or to protect PII when it's in the system; see the prominent iCloud hacks. Does the EULA say "don't store private info"?

[Hugh, Annabel, Eric]

Q: Are there any very-decentralized options versus that war between the big cloud operators? Or: does decentralization matter? Are we trying to address a problem that doesn't exist?

Companies are typically better stewards of data than the user. But there are questions around data ownership & sovereignty & control that the user gets.

With a platform with cloud storage & end-to-end encryption: *confidentiality* is one thing we can do easily under the user's control, but the *availability* guarantees are hard for an end-user.

How do you be sure you can trust that entity? How guarantee that you have any greater control over my data than another third party?

[David, Annabel, John]

Question over control of the data. What mechanisms for personal control of that data? (David's embarking on a project where that's critical but don't have a solution yet).

Define "control"? => "consent to share" (or use) (or purpose)

When someone has access to your data you're no longer in control. Radio Shack promised won't share your data for marketing, but look what they did. The fact they had access to that data implies someone else probably will gain access to it, even if gov't or a creditor. To be in control, encrypt it at the source. Separating "store" from "share" can help that. But, to share => you have ability to view in the clear.

As soon as you share something - even if using a distributed platform... trust that your friend doesn't share it onward. This moves the problem from the "cold & dry code of the computer" onto the "warm wet code of human relationships".

[John, Eric, Judith]

Authentication on that control? Often authenticate the user who's sharing their data, but maybe can't be sure your friend is really your friend when we do the sharing. That sounds like DRM which is almost exclusively an enterprise thing.

The UMA group is working on protocols may make it possible more generally.

[Judith, Annabel, Steve]

We've been talking about personal data as data that originate with the person. What about more disconnected data of mine, : e.g. the records of my power use? Lots of data originates from my *actions* but as soon as it originates it's out of my control. Do the same issues apply?

Arguably not solely your data; e.g. amazon's order data this data is *theirs and yours* (you brought a product, they sold it). Tied to you. Anonymization? Third-party?

[William, David, Andrew]

People are "creeped out" by ad tracking. Curious if there's a line between creepy and ok. That line varies on context. It only becomes creepy when tat data shows up in a context you didn't expect e.g.: snapchat more persistent or more widely shared after hack.

[Judith, Hugh, Bill, Eric]

Some opportunity for stores of personal data where the user is the aggregator, e.g. health/fitness data from multiple devices.

Bill's interested in potential abuses at the intersection of health and housing data. Is someone using my personal data in my best interest?

VRM community should talk about "fiduciary first"; looking for a framework where policy supports shares *in my best interest*

Does that imply a legislation or regulatory framework? For real-estate cases, the FTC established some disclosure laws; conflicts of interest are rampant though.

[Andrew, Annabel, Hugh, Eric, Christie, Dave]

There's a necessary shift in social norms. Changed expectations. In the case of gov't surveillance: some behaviors have changed around metadata.

Have we actually changed our actions? The general public doesn't care or understand.

Some signs say yes. Goog encrypts the backbone now. Lots of software vendors are taking security very seriously. In Canada there's a noticeable shift in the legislative environment now that people are more aware of the attacks.

It's less of an anonymous web these days, your footprints are exposed, is there a downside to that? Certainly there are public effects of not having the expected level of privacy. Society closes in on itself. The outliers have to be brought in. People don't take risks.

One positive change that came out of the internet: people found shared interests.. Requires privacy, vs. social pressure.

See the Colbert/Snowden interview, framed as "do you care that the government has your dick pics": yes, people care. Another useful framing is that it's not about 80% of a population (& then outliers), it's about 80% of your life. There's lots of very normal privacy. Parents' conversations with their kids about dating are not public.

Worry that NSA has Congress' dick-pics (they do).

[Annabelle, John, Hugh, Didier]

Once you share something with a third party unencrypted, it's out of your control at that point.

Interested in privacy-by-design concept, where apps protect users from themselves. Some apps – redphone / signal / textsecure – encrypted by default, don't need to think about the mechanics of

security, it just works. We know how to do that, right? - at least the tech, if not getting deployment to ubiquity. That needs work in the UX.

Not a tech problem, it's a business-model problem for these apps. They don't want your data; the other apps are based on your data.

There's a non-profit building a browser extension that uses blockchain tech to do MITM-proof encryption on any web site.

There are legit reasons for content provider to have the metadata: without that, they can't do usage restrictions – abuse, fraud, harassment investigations? Arguably: those are "quality controls" so they need some insight into the content. If it's all encrypted, how to do the quality control?

[Andrew, John, Kazue, Eric, Annabel, Christie]

One of the hard problems that will take a diverse community is: working on social norms, identifying what is best practice. What if there is actually a *code of conduct* that orgs could sign up to and be accountable for? A "goodness policy" on the internet?

Corporate behaviour: part of Apple/Google is trust over years of operation & living up to their stated values. (As well as the monetization aspects).

Is the identity monetized? When the data becomes the product. "classism": you can purchase that privacy if you can afford it, but the alternatives are freemium providers who will sell your data. Somehow you have to pay for the platform, otherwise the business is not sustainable; but many startup models externalize that. Free services; defer monetization with VC money to build scale. But free has to fail eventually.

The Emerging Field of Consent Management

Tuesday 2D

Convener: Ken K.

Notes-taker(s): Eric J.

Tags for the session - technology discussed/ideas considered:

PrivacyLens, Consent

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

Links

<https://work.iamtestbed.internet2.edu/drupal/>

<https://work.iamtestbed.internet2.edu/confluence/display/YCW/Yourtown+Community+Wiki+and+Service+Portal>

<https://spaces.internet2.edu/display/scalepriv/Scalable+Privacy>

Notes Consent is not understandable; you only find out what information is being shared, not why. Consent for Google does not say "yes" or "no", it's continue/cancel, which is a different thought process. It is because they want to get the user through the flow, not because they don't want users to know about the privacy details.

Has optional as well as required attributes that are releasable

Shows value that the user gets for each privacy element

Consent revocation as a major flow

Unfortunately, most apps are not granular based on privacy elements released

[Paul] I saw that there are two kinds of attributes; capabilities, and information – should there be a separation?

Determining the minimum required entitlements required.

It's really hard to get more granular than type of attribute, but even the specific attributes that they access or need, but it's a goal.

[Eve] It feels like consent dialogs are not the question I want [technical things], but I want a different question: "You want goal X right? How much are you willing to let pass?"

[Paul] The UI doesn't tell me the consequences of not releasing

General agreement that a better UI would not focus on attribute release, but more on what you get for it. But that's also of an app design issue, and it's common that apps get it wrong.

[Eve] Non-correlating IDs alone are not enough; some scenarios like sharing need a correlating ID.

Example – New Zealand ID

There are only 2-3 types of attributes that may need meta-attributes. One example is name. Since there often isn't a name field stored by the IDP as opposed to first/last name, etc.

Applications don't care what group a person is in – example – A may want to care whether you are a manager or not.

With revocation, consent suppression becomes really easy.

VRM: Five Participating Groups ~ notes from 5 related VRM Sessions

Tuesday 2F: Customer Needs

Tuesday 3F: Vendor Needs

Wednesday 5H: Market Maker

Thursday 4G: Framework Developer

Convener: Nitin B.

Notes-taker(s): Lionel W.

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

URL:

<https://docs.google.com/document/d/1o6EJ19u4zWPCyeF6g5KCpObYrTTD5XdJAE2Mww7hUB4>

VRM: Five participant groups

- **Developers**
- **Vendors**
- **Customer**
- **Market makers**
- **Policy makers**

VENDORS NEED:

Privacy
Control of Data
Ability to Scale
Assert Terms
Access to Support
Portability
Rules of Engagement
Autonomy
Ease of Use
Utility (Usefulness)
Ability to cast intent
Data Control

VENDORS WANT:

Survival
Real valid gestures (know a customer is real)
Qualified
Context
Severability (when a customer leaves, rejects the product)

NS: The data they have is worth money

Companies are making money from it

It is only fair that the customers get compensated:

DS: I don't like the compensation model. - My data is not worth money. - It is beyond that.

If someone gets my data I am going to sue them.

NS: Today companies are chasing shadows, or data exhaust. - At least people should get financial recognition that they are participating. - This plays to people's sense of fairness.

People are not being treated fairly today: this is a good marketing message.

DS: This feels like socially unacceptable behavior.

"It's not fair that you are reaching into my pants unexpectedly; compensate me".

KD: Generational issue here. <25 year olds do not feel violated like that. The people >40 yrs old feel privacy as a loss of rights. The emerging generation only knows this life of ultra-connectedness, where they cannot do business without giving data away. They never knew a world where data could be kept private. These younger people are looking for reciprocal rewards for participating in the data ecosystems.

AG: Two things to add to the list.

- Ease of Use
- Usefulness

These are critical to customer experience.

NB: Ability to cast intent.

DS: Add data control

MH: it's not either/or: either we give data or we get something, or we don't have privacy if we share information. Compare with physical space, and that "markets are conversations". In a physical market, we hand over money and get a physical object. Think about a "Farmer's Market" transaction. The experience is visceral and real, with transparency about every aspect of the transaction. online, the 3rd parties are invisible and not apparent.

Add: Transaction Visibility (Transparency)

JL: I prefer transparency. It's not just about the transaction.

KD: Currency. Selling data for money? But data itself is a kind of currency. We are willing to exchange services for data. The digital citizen has assets accrued from birth that are liquid and exchangeable. The insight capability information itself is a form of value or currency. Data is a kind of currency that is linked to value. A personal health record accessed in an emergency room to speed triage and treatment is value.

NSp: Currency is a tricky metaphor, since currency markets have daily fluctuating values in a currency exchange valuation marketplace.

MH: I decide the value of my own data, I decide if I am getting a good deal in this trade. It is the autonomy that enables this.

D: I might say, in facebook I am happy revealing A, B, C but not D, E. On the other hand other people might decide different things.

NS: The seller, being the data owner, has to be motivated to offer their data. If it facilitates the sale, it has value.

JS: Dave Birch, identity guru, "Identity is the New Money"; rather than individual bits of data, think of the data, as a whole, constituting an identity. Avoid an atomic view.

KD: Let's say, I am offered a glass of red wine, that might be 10 Euro, but I actually wanted water for 2 Euro. I want a 2 Euro value but am forced to take the 10 Euro object. This often happens--where I am forced to accept a higher value object, since the lower cost item is not available.

NB: The customer needs to participate in the choice making. Choice is highly driven by context.

LW: for example, Transaction visibility: let's ask, Is there a UX making visible the value exchange and information-in-use. We can ask this question of, for example, ATIMI software

NSp: The answer is "yes." ATIMI makes visible the use of data.

LW: Look to the use of the framework that we are writing. Investors and tool purchasers are looking to use the information. Inform those readers, define the critical categories, and then show how each line fits.

JC: A tangent: where we are going together, as people, is trying to express our needs, inner and outer directions, and combined. The SRI values and lifestyles program expresses that. What we are trying to do as customers, having customer needs, is expressing these needs. On the ecosystem side of things, we are just trying to get work done, that works for us. In this scheme of things, the work we do around the VRM framework, puts us down 'in the weeds' and we lose the visibility into this larger teleological issue.

NB: Is it scalable for the individual, as it is already scalable for the enterprise?

JC: We have a conversation with the world that lifts us up.

JS: Usefulness is a great word; utility is even better.

MH: Usability is helpful; it embraces design as well, and whether the meaning matches the intention. Utility means whether it matches overall means.

AG: I see usability as cross-site, portability, and the cadence of usefulness. If I use it once a year, that is not as useful as something that I need three times a day. Let's push VRM from once-a-month to once-a-day.

NS: We need to make the list shorter. Some items are blindingly obvious--what is not needed to be useful, easy to use? Why state things that are universal?

NB: We do need to itemize the specifics, even for obvious things.

C: Centricity is important. Patient-centered, customer-centered; who is in the center?

NB: The customer is in the center of the visual.

D: The list feels like, "how to explain to the enterprise how they should be thinking about this in terms of their customers." It should be, "what an individual wants."

AG: I want to get rid of the wallet. To replace it with my other digital gadgets. To the extent that VRM is the payment. In the case of healthcare, it is only the insurance company that has visibility to your

payments across doctors, hospital, pharmacy, etc. In the same way, my wallet is the only thing that knows when I opened it to pay people.

DS: The wallet represents a portfolio of capacities for operating in the world.

AG: It might take 5 years to get rid of my wallet and use, instead, my phone or an implant. Apple pay is a big step in that direction. Today, when I go jogging, I do not have to carry my wallet. Apple pay increases my privacy by introducing paywise pseudonymity into the transaction. It's a big step up without a step down. This is why UM is so important. It allows policy-based decisions. Another example, my password file is replaced by an UMA authorization server.

JS: Dan Miller calls this strong passive authentication. Passive, meaning "I don't have to think about it."

DS: You need your keys, wallet, phone

KD: and lipstick

LW: This is a small set of necessary tokens: key, wallet, phone, lipstick... Customers want this set to be reduced or made smaller.

KD: The smartphone is part of this 'token reduction' journey. It is the revolution of ubiquitous screens.

AG: Add to this list, FIDO token. (Fast ID online). It is useless. If it can authenticate me, I have physical control over it. This could be implanted in my skin and would not reduce my privacy, and could replace some tokens. If you accept the FIDO spec, I can implant.

CUSTOMERS WANT

DS: Scale. I want to be able to change my address once, and have every silo and enterprise pick up that address change. I want to save my time on issues like that. That is what scale means. Customers want scale across all their vendors, e.g. auto body shops.

NB: Customers want scale with all these four other parties: the Policy maker, market maker, vendor and developer.

SB: Advertisers talk about one to one, but they don't really want one to one

NB: They are scared of that, there is liability behind it

SB: Exactly. They mean, by one-to-one, that they want demographics and 'buckets' of like minded and like-acting people.

CB: Choice.

NB: Choice in the interactions that you have with the four other parties: the Policy maker, market maker, vendor and developer.

DS: Substitutability

KD: Opt out from organization

MH: Autonomy

KD: Identity

DSan: Intrinsic motivation: autonomy, mastery and purpose by Daniel Pink.

NS: Sounds like Maslow.

DD: I want the other parties to work on my own terms

XX: I want economy. Save me money.

MH: Cost effective. Accessibility. ($\frac{1}{3}$ of the population has disabilities.)

XX: The conundrum that I keep coming back to is that, customers want to be educated but they don't even know that they want to be educated.

XX: They don't want to be educated. Whenever you are selling something, you show people that others are buying that exact thing.

NSp: Our generation does not want to be sold, we want to feel that it was our own idea.

NS: My generation also was like that.

XX: We all have insurance.

D: What about we buyers pulling our buying power together?

NB: That goes back to scale, joining together is a kind of scale.

PDEC - Personal Data Ecosystem Consortium - Growth & Opportunity

Tuesday 2G

Convener: Dean L & Kaliya

Notes-taker(s): Kaliya

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

Kaliya shared some of the history of the Organization. Starting in 2010 several companies were talking about people and data and a one day invitation only event was hosted after Phil Windley's Kynetx conference that Spring.

Kaliya and Drummond talked about founding an organization together - Drummond got the Startup bug and she decided to found it by herself anyways in the fall of 2010. The first companies joined by the Summer of 2011 and it has grown to 50 companies. Following the Spring 2014 IIW Kaliya decided to work her partner William Dyson to found the Leola Group and starting in the Summer of 2014 she asked Dean Landsman to join her in leading the organization as the Director of Communication.

The organization is now working on getting its formal governance clear and developing bylaws to become its own organization.

Dean is working on updating the slides

The session review this slide deck _____url coming_____

The contrast between the organization and just protocol focused effort is that we care about taking a stand about how the data can be used.

We are going to be working with our members to request for compliance.

Lesson Learned: SAML and OIDC @ AWS

Tuesday 2H

Convener: Shon Shah

Notes-taker(s): Nick S.

Tags for the session - technology discussed/ideas considered: AWS, OIDC, SAML

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

Background

- At AWS, Shon worked on IAM, Cognito, Directory Service
- User for IAM is AWS admin.
- Cognito targets mobile app developers.
 - Manages data storage, sync, as well as identity layer.
 - Built-in support for features like guest sign-in.
 - Supports social IdP's like Facebook, Google.
- Directory service targets AD admins, OS and app admins.
 - Directory service supports both cloud and connected (on-prem, VPN-based) installation modes.
 - Directory service is not AD on the backend (actually Samba 4).
 - Requests coming in for directory service to offer SAML/OIDC endpoints (not currently available).

AWS IAM

- Early on, AWS IAM offered federation through custom code (to allow customer's AD users to access AWS services).
 - Limited adoption.
- Nov 2013, added SAML support.
 - Can associate a trusted SAML IdP with your AWS account.
- Good adoption with addition of SAML support.

Cognito

- Started with custom solution that supported Google, FB, IWA
- In Oct 2014, added OIDC support
 - As of now, customers are using 42 unique IdP's. Big win for adding standards support.

Lessons Learned

- Standards matter.
- Self-confirmation certification for OIDC compliance is a big win -- not scalable for implementer to verify compatibility with different providers themselves.
- Problem -- long-lived tokens on SP side in AWS IAM (e.g. what if user is fired).
 - As a result, set the lifetime on the SP side to 1 hour
 - Usability problem -- hard to make this work in a way that is very transparent to the user.
 - Need a revocation mechanism (currently under development at AWS).
 - Spec work underway to offer this in OIDC.
 - Granularity of revocation is important -- at role level or principal level?
- Can start small, iterate only if needed.
 - IAM supports IdP-init only.
- What about CLI access to AWS IAM?
 - Looked at enhanced client profile.
 - Few IdP's support it.
- API and CLI access almost as important as console access.

Comments - OIDC in production at MIT, to allow access to apps built by students.

Distributed Capabilities - Systems for Real Time Communications

Tuesday 21

Convener: Matt Schutte

Notes-taker(s): Matt S

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

Distributed Capabilities

- Designation + authorization
- Webkeys
- OAuth puts cap in the header allows multi-audience tokens
- Redirectory
- Exerciser allows talking to the correct endpoint

Fido U2F Update

Tuesday 3A

Convener: John H, Jerrod

Notes-taker(s): John H.

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

Here is a link to the slide deck: <https://docs.google.com/presentation/d/1WHPAnjSBbZpJ-2kvP8HFfMjclA5TFgh0KnCQHzK-OuM/edit?usp=sharing>.

Please check it out to make sure the sharing options are permitting access, I have set them, but always good to double check.

During the presentation, Yubico shared our experiences with the U2F deployment from our perspective:

- Oct 21 2014 Google enabled U2F for all Google accounts through their 2SV security settings
- #1 Amazon seller for electronics for several weeks, 10's of thousands sold to date
- Support calls have been non-existent with all calls usually related to misunderstanding various protocols (i.e. Lastpass use of OTP and Google use of U2F)
- We asked for a volunteer who had a Gmail account using 2SV. Bill Welch came up and within a minute had U2F enabled his gmail account and registered multiple Security Keys.
- We asked for protocol feedback and that Yubico's goal is to create an open U2F ecosystem that benefits all

Next step is upgrading U2F to FIDO 2.0 which Microsoft announced in another session will be released with Windows 10. This will broaden the ecosystem dramatically.

Enhancing the Digital Currency Opportunity

Tuesday 3C

Convener: Paul Dravis

Notes-taker(s): Paul D.

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

History of Currency – Changes are driven by man's changing needs and changing technology.

Outsider's view- concerns about Mt. Gox, Silk Road, regulatory uncertainty, price volatility, too much jargon, etc.

To increase market acceptance will likely require better messaging (telling the story in a simple and clear manner), better metrics (how to measure the growth of the market) and meaningful uses cases (real world uses – not theoretical).

Customers, prospects and investors seek solutions that are 1) faster, 2) better, 3) cheaper than alternatives.

Inertia is a barrier to market acceptance.

There are over 180 global currencies – not all are stable.

There is a broad set of global (cross boarder) opportunities digital trade opportunities to pursue – many are outside of financial services.

The market is still at a very early stage of development and remains confusing to many people and there is still controversy about the potential value of solutions.

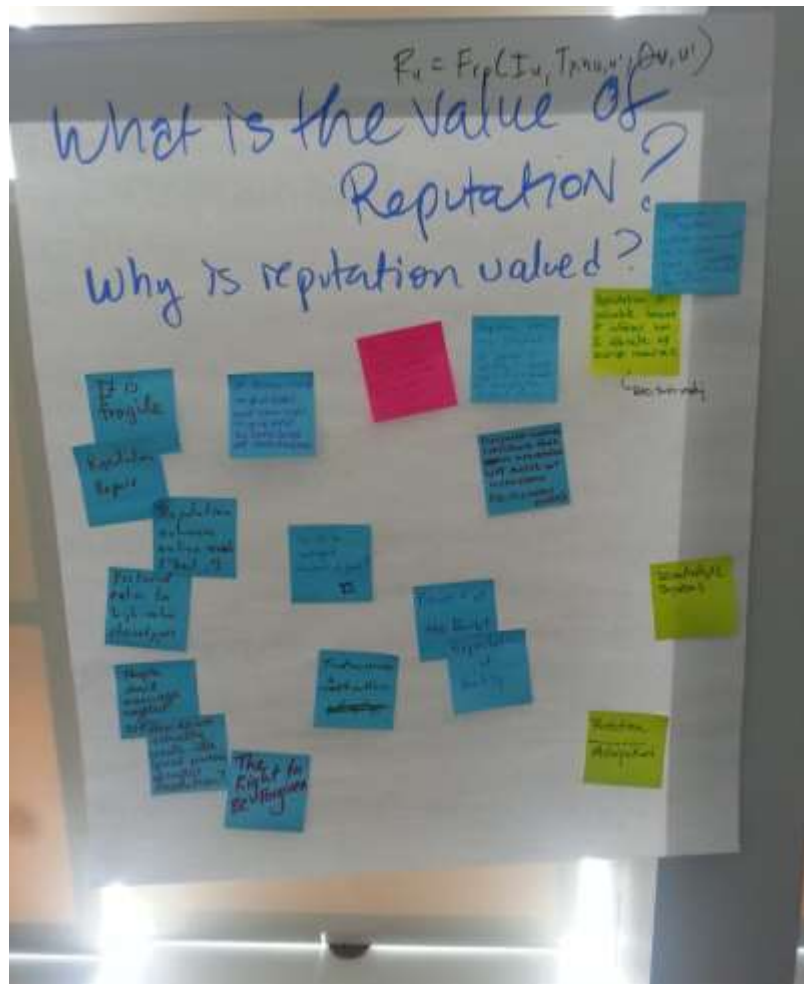
More resources for consideration are available at www.dtexpress.co

Additional Notes:

- Inertia by consumers may be a significant barrier to market acceptance on new solutions.
- There are many are outside of financial services in pursuing digital trade opportunities to pursue
- There are over 180 global currencies – not all are stable.
- The market is still at a very early stage of development and remains confusing to many people and there is still controversy about the potential value of solutions.
- Outsider's view – there are concerns about Mt. Gox, Silk Road, regulatory uncertainty, price volatility, too much jargon, etc.
- History of Currency – Changes are driven by man's changing needs and changing technology.
- To increase market acceptance will likely require better messaging (telling the story in a simple and clear manner), better metrics (how to measure the growth of the market) and meaningful uses cases (real world uses – not theoretical).
- Customers, prospects and investors seek solutions that are 1) faster, 2) better, 3) cheaper than alternatives to incumbent platforms.

Notes-taker(s): Heather Vescent

https://www.dropbox.com/s/mlguusqdd4sm4es/Reputation_BusinessModel_part2_IIWApril2015.m4a?dl=0



Mobile Profile Open ID Connect: Client Registration

Tuesday 3H

Convener: Torsten Lodderstedt

Notes-taker(s): Torsten

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

Software Statement: authz —> audience Signature algorithm: RSA (?) ISS (registry) —> in turn need to obtain key material redirect-uri (sector id) display name homepage / TOS, etc Kind of credentials / scopes	claims (not supported yet in dyn reg) grant types, response types allowed cars software id jti registry tos version (kantara?)
--	---

Questions: Does every instance of a native app need to register?

New Pothole PICOs

Tuesday 4A

Convener: Phil Britt

Notes-taker(s): Judy C

Tags for the session - technology discussed/ideas considered:

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

PICOs: persistent compute object, could have utility beyond storage, can form relationships with other things/people around it. May have own URL/address, QR code, etc. Has attributes, can certify ownership.

Mirror Worlds (don't look at title page) – written before the web. Idea to create models of the world that help with decision making. Phil's blog post about potholes: you have a device that tells you about it. When you see the hole, you'll see info about it as well, like how long it's been there, how many neighbors have reported it, when it'd due to be fixed (an identity). Computation and data about that identity gives context.

Easier to imagine each potholes, with street, infrastructure below street, having a unique identity that can help us know more about the world. For Internet of Things, we usually think about stuff that has computers, but models

Where is pothole, or a person or other PICO-enabled entity located physically? There's a neighborhood relationship, also jurisdictions. All jurisdictions are certified, two-way relationship with possible issue tag, can be accumulated on a map. Physical measure of when it makes sense for me to go out based on, say, number and severity of potholes, location en route to my destination, etc.

If you're having a conversation about policy? NewGov is now tracking hashtags, geotagging issues and putting them on politicians' maps. NewGov uses Twitter firehose for hashtag source material. Collaborative in four dimensions: 1. FTP (didactic), 2. WWW (collaborative), 3. Internet of things, 4. Internet of policy.

Higher level: a person may have attributes that include jurisdiction and issues that they care about. Querying the PICO will return the attributes. We are effective policy influencers.

IETC ACE Authentication & Authorization for Internet of Things

Tuesday 4C

Convener: Thomas, Eve, Erik, Hannes

Notes-taker(s): Eve M.

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

The goals of the session were:

- Get feedback on this draft: <http://tools.ietf.org/html/draft-maler-ace-oauth-uma-00> **Hannes also presented this slide deck:** <http://www.ietf.org/proceedings/92/slides/slides-92-ace-9.pptx> (Here is a supplementary IETF #92 presentation that talks about IoT architecture and security: <http://www.tschofenig.priv.at/wp/?p=1084>)
- Interest people in getting involved in the IETF ACE (Authentication and Authorization for Constrained Environments) group: <http://datatracker.ietf.org/wg/ace/charter/> (To this end, we collected the names and email addresses of nine people, and we'll be sharing them with each other and asking them to get involved.)
- Gather ideas for adapting OAuth and UMA for responding to the authorization challenges identified by the ACE group.

In the session, we discussed the following topics:

- Having access to multiple authorization servers is of interest. A cloud AS is desired for "sharing" functions, and a local AS is desired for "backup" and privacy functions.
- Local token introspection is of interest. However, if the resource owner has revoked access in the meantime, there may be "entitlement latency", which in some use cases could be a severe problem.
- "Fail open" scenarios are of more interest in IoT scenarios than web scenarios, which typically prize strong security. If a car dies on the highway because an access token has expired, it's a big problem!
- A system design view of challenges is especially important in IoT, where, e.g., physical security and life-and-limb considerations tend to come into play.
- The question of federated login comes up depending on use case. We examined a "door lock" scenario. If the person is an employee vs. a consumer, they will expect different login options.
- Thomas presented a new draft, "Fluffy": https://datatracker.ietf.org/doc/draft-hardjono-ace-fluffy/?include_text=1 This is a lighter-weight way of distributing keying material than Kerberos, which would be valuable in IoT scenarios

PDEC Call for Hot Topics / Papers

Tuesday 4D

Convener: Dean Landsman

Notes-taker(s): Dean Landsman

Tags for the session - technology discussed/ideas considered:

PDEC, White Papers, Hot topics

PDEC discussion on ideas on relevant White Papers related with Personal Data

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

SESSION SUMMARY ~ The objective of the session was to help define a set of topics to develop for PDEC (on Personal Data) in order to convey knowledge and awareness on this broad and critical topic. Further, to do so as a way to try to identify future business opportunities in the community and add to the ongoing discussion.

The session was very fluent and many issues were raised and discussed during its course.

The main conclusion of the session was that the group would gather in the future on a regular basis – hopefully a weekly basis, virtually or physically – with the objective to identify first what are the hot topics in the area (via research using tools such as Buzzfeed’s Analytics Topic Generator or similar mechanisms) with the aim to develop very short and easy to read articles (such as, for example, “Data Brokers at a glance”) that could produce immediate impact on the community by raising awareness on facts that are happening in this area and that are actually “pain points” or critical business issues to members of PDEC and also to the IIW Community at large.

SESSION NOTES ~ PDEC intends to organize meetings, conferences, and increased activity on its website.. This session was a step toward identifying topic areas that would be of interest to PDEC members, and also that would be of value to the Personal Data Ecosystem.

LaVonne Reimer (PDEC member and participant in the PDE Governance Committee) has been working on a White **Paper** for PDC to publish, exploring ways to facilitate the exchange of information among companies in order to deal with identity problems and to enhance usability.

PDEC is building a glossary of terms defining a common language. It is the belief of PDEC that this is an important step for its members and also for the Community at large.

“We are looking for subjects... and will continue to do so with outreach over the coming months.

Lionel Wolberger (of PDEC member company Emmett Global) offered suggestion: In addition to white papers, how about something else? Short, three paragraph overviews of Personal Data topic areas, offered to the membership to read and then discuss. (see more on this below as it was gone into in further detail).

Dean Landsman (PDEC Communications Director) suggests that we need white papers that can be used as the base for a discussion. Also need to build out discussion on topics and issues of concern to PDEC members and of note in the Personal Data Ecosystem. The white papers can and should stimulate discussion and also help state PDEC’s position and view on these topics. Personal Data is a highly charged arena, with all the breaches of late and the increasing awareness that Google, Amazon,

the NSA and others (advertisers and marketers) use cookies and data mining to acquire and in many cases sell the Personal Data of individuals. Often this is done, yet unknown to those whose data is being acquired.

LaVonne replies that the aim of this Working Group is to be a group of doers instead of thinkers.... Dean suggests a possible **paper**: What kind of labs could we develop? People here at IIW have many ideas that could be put in place in such labs...In IIW there is a good mixture of people from academia and from industry with different goals that together could make very interesting projects.

Lavonne: Topic suggestion -- Blackboxes vs. Open Systems

A white **paper** clarifying Personal Data Ecosystem definitions....

Dean notes that once we have a good **glossary** we can facilitate conveying the information and products to be created for the end user.

What is the "End User" of which we speak? In first instance, End User should be the average consumer.

PDEC has great potential as publisher of papers based on projects that work and are related to Personal Data, Privacy Policy, Identity Verification, Trust frameworks separate from associations such as IPP.

In this case, customers of PDEC are businesses....

Small businesses are a blurred point between user data and commercial data.

Let us see how Personal Data can be used for creating new businesses such as Using Real Estate as a use case for Personal Data. This is a system that implies such much Personal Data that is information used to take decisions on Mortgage, lending, etc.

What is the difference between Personal Data Manager, Personal Data Store, Vault, etc.

From a consumer perspective, they can get information from this which will increase their awareness of how their data is being used.

How do PDEC and Customer Commons (who work together very well and always hold a joint dinner the night before IIW) differentiate, and how does each's publications differ? Customer Commons is for geared for the consumer. In the case of PDEC the feeling is that it is essential to speak the language of the enterprise to engage them. Similar to Customer Commons, we want to empower the individual to allow them to engage enterprises. (VRM!)

The above arose from a discussion of whether PDEC's topics and white paper would represent individuals, end users. This brought up considerations of what Customer Commons' mission is, and how PDEC and Customer Commons are complementary, and supportive of each other.

From a business perspective the centrality of personal data starts to become a problem in terms of glossary, definition, and clarity amongst the various players in enterprise (and others in the wilds of commerce) as rules and roles become unclear due to the lack of a body offering standards, etc.

Our (PDEC's) role is to set industry standards and develop a glossary...

There presently is no existing authoritative paper on empowering the user. Much VRM discussion centers around this but not specifically in reference to Personal Data.

There is no research or proof indicating whether there is a marketplace for privacy... people don't care (?)...this is about control... but in order for apps to be useful, you need to give some information... but you should provide this data with control. Privacy is a loaded term; it can mean various things to many people.

Dean stated that PDEC is looking into developing a "Good Housekeeping" litmus test for determining levels of compliance, respecting Personal Data and business activity with regard to such data.

Dean would love to put a **paper** that could be a request for compliance areas... if a company or entity requests a user's email address (or anything else), what do they do with it? Why do they need (want) it?

Does it affect end users and is it a value for enterprise objectives? If so, what is the benefit or value to the consumer(s) who have provided this data?

Another topic: How the emerging eco-system can clear these issues by itself – is this where compliance comes into play, or is a standard by which companies can be measured a better idea?

Oscar Manso (the Alexandra Institute, Denmark) raises the question that maybe privacy should be legally enforced such as in Europe, as a topic for discussion. How do standards differ across nations and continents? But here in USA it seems impossible to follow such approach of governmental enforcement. But is this what NSTIC is meant to do, or a variation on the theme?

Kaliya (Identity Woman/LeolaGroup, founder of PDEC) then mentioned that one of the great things about IIW is the mix between European and American companies.... An interesting **paper** would be to find a way to bridge both cultures to enhance privacy. And to get this done without harming businesses.

Karen Lewison (CEO, Pomcor) is working on a **paper** on the privacy instantiations of authentication...

Privacy is a tough word... that should be a word that would really need to be defined...

Other possible topic areas: Can an identity provider know where are you going in your transactions? There is no clear answer to that question.... Some people want to have that privacy and some other want the IdP to trace those transactions in order to avoid fraud...

Who controls that metadata as it goes further?

Another idea for white **papers**... What if we did a series of many shorter offerings on the PDEC site, Personal Data zeitgeist topics as suggested via tools similar to Buzzfeed Analytics. These could be easily researched via the web and serve as an alternative to working on longer form papers... so let's search for what Personal Data terms trend via Buzzfeed Analytics. So in addition to us solving the issue content let's also look what topics are already in the wild, in various stages of discussion and perception.

Kallia thinks that this is really smart in terms of what is doable and also is easily accomplished.

A good start would be to use terms such as Data Brokers, Personal Data Systems at a glance, etc ...

Dean suggests that this should be more of a discussion and share group that should collaborate weekly on a virtual or physical basis. PDEC will have Committees devoted to various areas of growth and operation. This is a good mandate for a committee.

Bill Wendell (RealEstateCafe) points that if you want to change somebody you don't change it by connecting via his/her head but on a personal and emotional level. We should approach this with a view of solving problems. Are the "victims" or people in some sort of pain, with regard to uses of their Personal Data? What is happening that is causing pain? How to alleviate the pain? These reproblem areas where PDEC can find solutions, and PDEC members can make these things happen.

A very interesting article Bill proposed: "Real Estate is making life hell for home owners."

The session could have gone on much longer but we all had other sessions of interest to attend. For the IIW participants attending the session and for PDC, it was a very productive session.

Local Re-Delegation with OAUTH

Tuesday 4G

Convener: Alan Karp

Notes-taker(s): Alan Karp

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

The Problem: Alice gets an access token authorizing her to access a protected resource. She wishes to give Bob an access token with reduced scope to access the same protected resource. There are two RFCs, but both have expired without being adopted. They both work by having Alice present her access token to the Authorization Service, which returns the sub-scope token that Alice can pass to Bob. Alice would like to avoid the round trip to the AS and be able to generate the delegation token when she can't reach the AS.

Proposal: The basic idea is to generate the delegation token by hashing the original token. Say that Alice has an OAuth bearer token T1. Under this proposal, she can create a separately revocable token with the same scope by hashing, $T2 = H(T1)$. The AS can validate T2 by hashing T1.

We need some additional metadata to make the proposal practical. First, the AS has lots of tokens, so we should tell it which token to hash. We can do that by having T1 associated with a label unique among all the AS's tokens, call it L1. Now we have $T2 = L1 \ H(T1)$. (Blank denotes string concatenation.) If we want to produce a subscope token, we can list the permissions being delegated. For example, if T1 has Read/Write/Append permissions, we can delegate Read/Append permission with $T2 = L1 \ [R,A] \ H([R,A] \ T1)$.

It's obvious that the proposal is incomplete, but the consensus from the session was that it might work. One important contribution of the group was to correct a mistake I had made. I had assumed that the Resource Server could validate the delegated tokens, but the group pointed out that only the AS had sufficient information to do that. (Of course, the AS and RS could be tightly coupled.) I would have been in a lot of trouble had I gone ahead with my original idea.

Thanks for the free consulting folks. Your check is in the mail.

Blending Consumer Education and Enterprise Identities

Tuesday 4H

Convener: Alec, Scott David

Notes-taker(s): Scott D.

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

Alec.shuldiner@autodesk.com led the discussion

Universities unique – non-commercial

This can solve problems including identity.

Bringing together of education and consumer. What are the points of intersection?

Many problems here are “wide”, but not deep in addressing many highly orthogonal identity challenges. How can the general solutions address the specific.

Need “mass customization” concept of identity and data usage.

Question of bringing together marketing and distribution function with the engineering of products. Engineering company comes to realization that needs to engage more closely with the consumer.

Data strategy and policy – When have big piles of data, but unstructured and unarchitected at present.

When academics and others are talking about solutions, sounds good from the individual level. But from a corporate perspective, recognize that have big challenges among businesses. Not an “academic” question.

Comment: Would like to understand and generalize role of industry and academics and other non-profits.

Interoperability and shared infrastructure – but agenda are not shared, so see challenges.

Identification of challenges is non-uniform.

Important to start with consideration of the person as having a multiplicity of personas

Start with the classic customer//vendor relationship of a software vendor for example. Added direct sales to the relationship with the customer, but still don’t know the customer directly (there was an intermediation in the supply chain).

Then create a consumer business (as distinguished from an enterprise business). (education is a third line of business). Each had different terms.

For example, if education, may have had “for free” model.

Consumer market was different. Higher volumes. But B2B markets not grow as quickly as B2C markets. Exponential growth in C2C is a challenge to the model.

So have multiple distribution channels to contend with

Can also have licensed professionals (such as medical), that adds to the complexity of the potential challenges.

Individuals have personas, but not being accommodated in the architecture of the distribution channels. Branding issues.

Like healthcare challenge of patient matching. People have expectations about being matched across healthcare situations, but not being met. The conferences on healthcare not meeting with adoption, because they require “total surveillance” approach.

If had a regulated environment with infinite money. Banks are not able to get this together.

It is a problem of “de-duplication” of data.

Suggest that they chat with VRM folks about the efficacy of putting the individual at the center.

Most entities do account matching and manual processes to remove duplication.

Individual wants a single interface and a single identity in the system. This is a problem.

It is possible to let the customer solve the problem through account reconciliation. Like when a mobile carrier and fixed telco carrier combine, they have multiple accounts for a single person. Put the onus on the customer to help resolve the challenges.

From university perspective, maybe a solution is to not care about the duplication of identity. Do we care if we have multiple identities.

Where is the line between desirable pseudonymity and undesirable multiple identities. In common is a way to federated identity.

UW has apps being built with different expectations of data supplied by users. When want to have “hands off” of the data, so not have responsibility for the data.

Two terms – “coercive” and “secret” In general when institutions try to solve the problem, there are “coercive.” In that want to manage it.

When institution gets into situation when there is opacity on the processes, there is a relationship problem with the customer.

It is a supply chain problem. The enterprise customer wants to maintain the relationship. So maintain opacity. When it is more automated, there is more opacity. It is a desire of “simplex” versus “duplex.”

Like same problem that Adobe went through when they became a cloud company. Using a “named user” model – like Adobe. Have a “login” name, through a named user. This will change the shape of the problem.

Identity broker concept introduced. Identity broker can be “triple blind.” Identity providers, service providers and infrastructure in between that doesn’t know who you are. If you postulate that, does it solve the problem?

It is a question of persona control. Change inadvertent pseudanamy to intentional pseudanamy.

Another solution is to blend the accounts. How can that be blended using external service. They want context and business logic.

Outsourcing the challenge is possible, but challenge in regulated industries (HIPPA, etc.).

Could create incentives for the channel.

Not an atomized problem. Must consider in the larger context.

May not be about the individual, it is about the use of the information in the channel.

Don't solve the problem too much, because may get "creepy"

Blockchain & Minecraft: Can Someone Tell Me About B/C @101

Tuesday 4J

Convener: James L

Notes-taker(s):

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

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

The Bitcoin blockchain is a database with several unique features:

- A new node in the Bitcoin network can run the software and download a full verified copy of the current and historical state of the database from other "full nodes" in the network. The database updates with a new "block" of verified transactions approximately every ten minutes.
- Access to the database is restricted by cryptography using ECDSA signatures.
- Consensus regarding the state of the block chain is achieved in a decentralized manner using proof of work i.e. hashcash, removing the need for trusted third parties/ central authorities to maintain the integrity of the database. Limited-supply "tokens" or "coins" are used to incentivize computers aka "miners" to perform the proof of work calculations aka "mining."

Notif Update - User Controlled Notifications

Tuesday 5I

Convener: Jim F.

Notes-taker(s): Jim F.

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

The Notif Update session had about 10 attendees, and mostly went through my slide deck at: http://www.slideshare.net/jim_fenton/notifs-update

Followed by a short demo of my prototype implementation.

How the BLOCKCHAIN Can Solve All Our (identity) Problems

Tuesday 5J

Convener: John Light

Notes-taker(s):

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

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

The block chain can function as a distributed key-value store that can be used to map globally unique, human-readable identifiers e.g. domain names to public keys, replacing the need for centralized IDPs, name registrars, certificate authorities, etc. The block chain can thus be used to create end-to-end encrypted, man-in-the-middle-proof communications channels between users on the Internet.

Wednesday April 8

Vectors of Trust

Wednesday 1A

Convener: Justin R., Steve O.

Notes-taker(s): Oscar Manso

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

This work started at an Internet Society meeting last Fall, and spun up an IETF non-wg list. To review the list archive and/or subscribe, see <https://www.ietf.org/mailman/listinfo/vot>

	<u>Identity Proofing</u>	<u>Credential</u>
<u>Zero</u>	Anonymous	Session
<u>Low</u>	Pseudonymous-Self	User/pwd
<u>Medium</u>	- (Some minimum auth)	
<u>High</u>		

In terms of credential assurance, vendors will like to be able to add their own flavors to signify their difference

In order to transfer these values across the wire to the RP the proposition is to send a vector of values:

[I2:C3]

[I0:C3] -> This one can be very appropriate for the health sector

You need to be able to verify where is this identity information coming from because otherwise you are in trouble...

In terms of credentials assurance for mobile devices there are three main elements to take into account:

Strength of auth method + Credential secure against malware + credential is protected against physical capture of the device

Justin suggests that if this is done at such a high level, this type of definition may explode and may make not sense for many type of credentials... that said, if this information can be conveyed at a higher level, that could be very interesting....

Another category that has been suggested to include is environment. But environment in respect to what? If it is in respect to the IdP, this can be considered as quite static and therefore, can be conveyed in a different manner...

Another environment more dynamic is the Auth Context, how was the authentication being presented? Another approach to look at all this is to define it as a set of attributes for everything... this may explode too much... everybody will be looking for their own attribute and their special definition...Justin feels that we should end up with between 2 and 5 vectors...

Another proposition is to consider the values linked to the attributes in a more fluid manner but then, the result may not make any sense at all for the Relying Party...

Should we have a mechanism for an attribute bundle to allow for particular cases?

Jim indicates that there is an Executive Order 13681 released in October 17, 2014 that aims to improve the security of consumer financial transactions:

<https://www.federalregister.gov/articles/2014/10/23/2014-25439/improving-the-security-of-consumer-financial-transactions>

The distinctions defined need to be meaningful otherwise that won't make sense.

Level of Assurance can be split into two parts:

+ Level of Strength (of authentication)

+ Level of Confidence (of attributes)

He proposes three levels of strength...

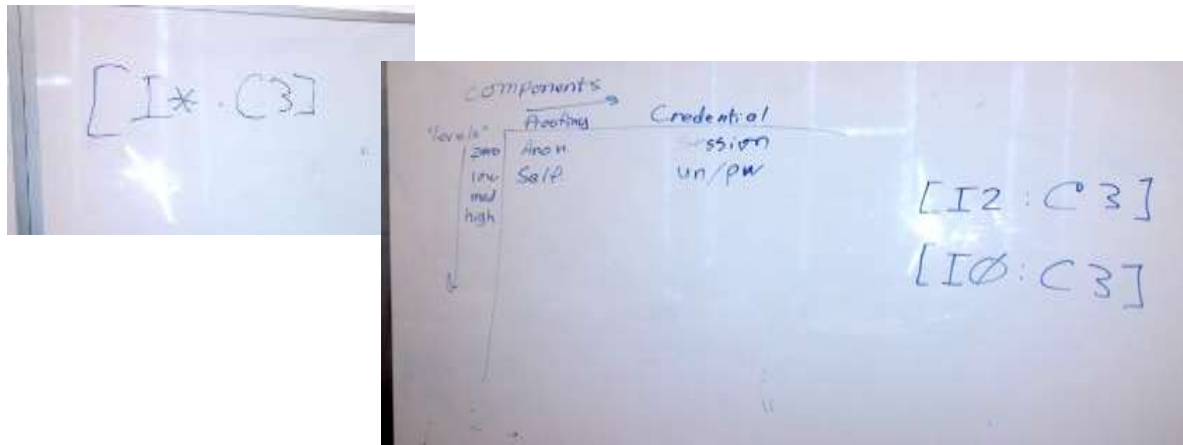
Eve also introduces that this is a communication problem for consumers in the context of UMA... and consumers could not understand more than three levels...

Another point is that if we define a static system to start with we may be thinking on a more dynamic system that could evolve in the future...

--

Jim Fenton presented his proposed approach, slides at

http://www.slideshare.net/jim_fenton/loa-alternatives-a-modest-proposal



XDI Review & Demo /Personal Data Ownership in a Corporate World

Wednesday 1D

Convener: Markus Sabadello

Notes-taker(s): Hugh Pyle

Tags for the session - technology discussed/ideas considered: XDI Names

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

People: identified with '=' identifier. The Leola "nymble" registry uses +nym=markus (etc). Then: Organizations (name begins with '+'). Finally, Things (prefix is '*').

Some more discussion of names (global forms, local forms) & registry & their scope, context, and semantics. (The subject of names is way too big to handle this session but XDI designed to describe those context & relationships.) Drummond enumerated the six contexts

- two authority-types: = and +. Only for privacy purposes.
- two instance-types. *:unordered-list. @: ordered-list.
- two classes: hashtag (#friend etc), used by the community; dollar-sign (\$and \$or \$not \$msg \$if \$uri), used by the XDI Itself.

xdi2: Java implementation (<http://xdi2.org>)

Tools: parser, signatures, discovery

discovery: the registry resolves =name to an authority URI (someone running an XDI service that hosts the graph for this name). Then it'll query the authority & get (e.g.) public keys for signature.

Support multiple registries. But the registry is just how to find the name. Graphs themselves just interoperate. Point from one to the other. Also pseudonym thing ("wrapper") that hides the underlying name from you, you only see the pseudonym in the result.

Signature things: just a convention, not deeply assumed into the XDI language itself. Over time there will be a data dictionary defining common names for the standard things, e.g. cryptosystems, signatures, and so on.

Some higher-level tools. See the list of demos, <http://xdi2.org/demos.html>. Things that can be useful as functional building-blocks for the application layer.

Link contract: permissioning steps. e.g pizza demo: provide my address without typing it in, by instead making a link contract that describes that the pizza site is allowed to connect to my personal cloud for the purpose of reading my address. The "forever address-book" thing. Ongoing connection, revocable. Unlike OpenID Connect where attributes are transferred once; this creates a permanent connection (will also persist if you move your graph from one place to another, as long as I maintain the link contract, its UUID doesn't change).

q: what about the problem domain of reverse-id - verifying identity of a phone caller from amex when they ask for all your personal information to authenticate. Routine scam model.

Cloud cards similar, connections between individuals. Webpage that shows some of my profile information.

q: relationship with uma? some discussions. OAuth about access to a single resource. UMA for one place where I manage my permissions in different service providers, with all the people I want to give permission to. Could relate directly with the link-contract mechanism.

q: blockchain - use case for peer-to-peer assertions about things at a moment in time. How would that with XDI? Things that could be done there.

SSO, Hello, and Passport: Updates to Identity in Windows

Wednesday 1E

Convener: Eric Jia

Notes-taker(s): Nick Sawadsky

Tags for the session - technology discussed/ideas considered:

Windows 10, Fido, OAuth, Passport, Windows Hello, Azure

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

Principles

- Passwords bad
- Help user navigate through their multiple identities

Started out trying to solve own identity problem

Windows 8 added ability to login in to Windows with consumer identity

Enterprises didn't like it - consumer data flowing into enterprise laptop, and vice versa

Windows 10 - update Windows to work with enterprises

- Users can login with consumer identity or Azure AD

How do we handle the fact that user can have two different identities?

- Don't hide it, surface it

How do we deal with the fact that users use their personal device at work?

Even though logged in with Azure, should still be able to sign in to one of your other accounts

Application could conceivably leverage the fact that you are signed in on both home and work accounts

Passport, Fido and universal authentication - replace passwords completely, using public and private infrastructure

- Relies on local user gesture and a key store
- Log in with biometric (or fallback to PIN)
 - Unlocks the key store ("Fido container")

Windows Hello: The biometrics that support Passport

- Iris
- Fingerprint
- PIN (could be a simple 4-digit PIN, or a complex password)
- Pluggable architecture for biometrics

How Passport works:

- Hardware element: the secure container (a TPM). Stores keys for the different services you use.
 - Fido spec allows for a software-based container, and Windows 10 will support it as a fallback.
- Local user gesture

Not every action you do in an application requires you to unlock the container

Any third party site, if they implement the Fido specifications, will support this

System to allow sign in with both Azure AD and consumer account

- App requests token through broker
- Broker launches the native plugin identity provider (could be Azure, could be Facebook)
- Plugin returns a token to the broker, which returns it to the app
- Similarities to NAPPS
- Broker caches token for IdP so that it can be reused by other application

Clouds For Things

Wednesday 1G

Convener: Doc Searls

Notes-taker(s): Matt S.

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

Link to audio file of session:

<https://soundcloud.com/matthew-schutte-1/iw-session-clouds-of-things>

Can Technology Revolutionize Consumer & Citizen Activism?

Wednesday 1H

Convener: Paul Dravis

Notes-taker(s): Paul D.

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

- Can technology truly help consumers/ citizens what they seek to engage with corporate, government and NGO entities.
- Can technology based solutions provide leverage when confronting the inertia and scale (both dollars and staffing) on corporate, government and NGO entities?
- Models to consider emulating included Craigslist and crowdfunding (Kickstarter, etc.)
- There was interest in exploring the potential for sustainable (rather than non-profit) models.
- Solutions should be issue and problem driven. (Policy may be an outcome, but likely not the starting point).
- Issues and problems should be clearly identified with a finite focus - rather than thematic.
- Solutions must be seamless and provide a positive user experience. User experience includes both the application interface as well providing messaging and outcomes that build and reinforce positive momentum.
- There have many failures in addressing this market need. These failures likely offer some “lessons learned” which include both the potential and limitations of technology in “Revolutionizing Consumer/Citizen Activism.”

Blockchain Tech 101 + Identity (onename)

Wednesday 2C

Convener: Muneeb Ali

Notes-taker(s): Muneeb Ali

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

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

This talk gave a brief introduction to Blockchain and Bitcoin. It explained how blockchain is a global ledger that doesn't rely on any trusted party and how this ledger can be used to build decentralized identity. Phil had a great description of the blockchain:

"The world is full of directories, registries, and ledgers—mappings from keys to values. We have traditionally relied on some central authority (whoever owns the ledger) to ensure its consistency and availability. Blockchain is a global-scale, practical ledger system that demonstrates consistency and availability without a central authority or owner. This is why blockchain matters." -- Phil Windley

The talk also introduced the work that Onename is doing. Onename is a registrar on top of a decentralized identity system built on the blockchain. Onename provides a web interface for users to register themselves and get a decentralized identity. Users are in complete control of their identity and data. To date, close to 30,000 users have registered themselves.

What's new in PICOs + Cloud OS?

Wednesday 2D

Convener: Phil Windley

Notes-taker(s): Phil Windley

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

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

These blog posts constitute the bulk of what was discussed:

http://www.windley.com/archives/2015/04/the_end_of_kynetx_and_a_new_beginning.shtml

http://www.windley.com/archives/2015/04/whats_new_with_krl.shtml

AWS Identity Round Table (Amazon Web Services)

Wednesday 2H

Convener: Bob Kinney

Notes-taker(s): Bob Kinney

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

We discussed the various product teams represented

- Login with Amazon (LWA) - <http://login.amazon.com>
 - Use Amazon as an Identity Provider
 - Integrates with Amazon Payments for "Login and Pay"
- AWS Identity and Access Management (IAM) - <http://aws.amazon.com/iam/>
 - Create and define policies for what resources are accessible for users
- Secure Token Service
 - Create temporary credentials for accessing other AWS services
- Amazon Cognito - <http://aws.amazon.com/cognito/>
 - Mobile identity + data sync
 - Users can transition from "guest" to authenticated users
 - Multiple authentication methods supported
- AWS Directory Service - <http://aws.amazon.com/directoryservice/>
 - Managed Active Directory (AD) in the cloud, based on Samba 4
 - Can link to on premise AD
 - Federated access to other AWS services (WorkDocs, WorkSpaces)

There was a spirited discussion on Amazon's (not AWS's) lack of MFA or 2nd factor authentication. This is something that is on the road map, but no time table can be committed at this time.

We also discussed various other channels for information exchange:

- AWS Summits - <http://aws.amazon.com/summits/>
 - Free to the public, locations world wide
- AWS Pop-up Loft - <http://aws.amazon.com/start-ups/loft/>
 - Loft area for Start Ups
 - "Ask the experts"
 - Workshops with engineers and solutions architects
- AWS re:Invent - <http://reinvent.aws.events.com/>
 - Yearly user conference in Las Vegas
 - Previous years talks on YouTube - <https://www.youtube.com/user/AmazonWebServices/Cloud>

Privacy Issues Regarding Federated Login

Wednesday 2J

Convener: Jonas Lindstrom

Notes-taker(s): Berit S.

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

Privacy preserving authentication, UProve, OpenID Connect, local storage of credentials, attribute based credentials, Jonas gave a presentation based on the following slides:

<http://jonaslindstrom.dk/slides/iw-2015.pdf>

He explained how the use of an IdP could be replaced by an Identity Proxy, which provides the user with a certificate signing that this person has these credentials at this IdP. The user can then use this certificate directly with the SP, without involving the IdP. This setup also allows for the use of pseudonyms.

The question: Does OpenID Connect protect the login history from the IdP? Was discussed, since this would solve part of the problem, the presented solution is aimed at solving. (answered after the session – the answer is no, the OpenID Connect protocol does give the IdP information about where and when the user logs in)

There was an emphasis on the local storage of credentials – meaning that the user cannot be tracked
The identity proxy uses Microsoft UProve to only present part of her identity

Link to demo: <http://ec2-54-171-208-102.eu-west-1.compute.amazonaws.com/AmazingServiceProvider/index.aspx>

Advantages for SP: Don't have to store user info + user just needs to check a box to provide info to the service provider giving a better user experience.

Freedom Box Update

Wednesday 3A

Convener: Markus Sabadello

Notes-taker(s): Markus

Tags for the session - technology discussed/ideas considered:

#freedombox Tagged: [Cross-platform software](#), [Debian](#), [FreedomBox](#), [Prototype](#), [Python](#), [Software](#), [Technology/Internet](#)

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



We looked at the latest FreedomBox "Danube Edition" and found that it looked super sexy and "like an Apple product", as one of the participants put it.

Functions include:

1. "Known" personal blogging service (support for IndieWeb protocols)
2. "OwnCloud" for personal file storage
3. "RemoteStorage" for Unhosted applications
4. XDI and RDF
5. Tor, VPN
6. etc.

Besides looking at the tech, we also discussed business and marketing opportunities.

Notes from Judy C

Markus gave an update on his development of [Freedombox prototypes](#). Nice design, updated hardware—especially compared to the freedombox from four years ago.

Work needed: UI in python, packaging software in Debian.

[Continue →](#) 2015 April 8 · [future](#), [records](#), [tools](#) · [Leave a comment](#)

Fluffy are Kitties!

Wednesday 3c

Convener: Sarah S & Justin R

Notes-taker(s): William Kim

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

Inverse of 'Kittens are Fluffy' sessions held at previous IIW's

As opposed to someone using their corporate identity to express potentially controversial opinions not representative of the company but still linked to the company since the person uses their corporate account, what happens when someone, e.g. Secretary of State, uses personal channels of communication to do their professional work?

Discussion was mainly in the context of corporate email and calendar.

Talked about challenges of trying to manage personal and work contexts on mobile devices.

Calendar, separating work and personal spaces as different accounts or different identities

Crossover of personal to work, and vice versa

You own your identity, but when you get fired, you lose your corporate identity

What about sensitive information in textual content of the calendar events?

Free/busy calendar information cross over

DLP voodoo magic solution? Protect corporate-specific calendar information within the firewall – once user is fired or quits, no longer has access

What about offline or remote access?

Having access to corporate calendar only on the network leads some to forsake using it at all.

Corporate email policy around email retentions. Personal workarounds to archiving email, i.e. run own mail server.

ENFORCEMENT (or loose nature of it) is what allows this kind of situation to happen. Mostly self-enforcement: “Don’t be an idiot”.

Email is still viewed as ‘technology’

Sunshine laws/transparency vs. Classified/Confidential information

Data retention for liability or to mitigate liability

Defining a ‘record’ for technology

Self-enforcement (“Don’t be an idiot model”) is a practical solution response to a complicated policy system that may not be understood or tractable otherwise. No policy system is perfect though.

Software systems (email and calendar), and hardware systems (BYOD)

Software/hardware stack on client device Vs. Server

Weird BYOD stuff kinda acquiesced by corporations, but Cloud is a different story.

Isolation of environments using VMs, user experience issues?

NDA’s with a customer while using Gmail

Using paid service transfers some liability? As opposed to free service or hosting your own service

American view of identity is highly fragmented? Expectations to act certain ways in certain contexts. “Roles”

Socio-normative controls

What are the consequences? Why is there no real crackdown? Because expectations are still emerging.

Where to shape the privacy bubble around people and around digital identities

Alignment to privacy expectations, in corporate sense NDAs/IPRs, but perfect alignment not desired.

We still want whistleblowers and whatnot.

Bureaucracy & IoT (Internet of Things)

Wednesday 3G

Convener: Phil Windley

Notes-taker(s): Dave Sanford

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

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

Phil started with review of the 'Utopia of Rules' book by David Graeber:

Bureaucracies create perfect places that throw out imperfect people, because they won't follow the rules. Bureaucracies create structure and efficiency using rules and regulations. This is not limited to government, but includes typically any organization that creates hierarchy and rules.

Phil indicated that he wanted to stay away from partisan policy discussions and indicated that political parties as well as all or most organizations are pushing some kind of bureaucracy and some may be objectively better than others.

Relationships are based on queues, reciprocity, even for trivial relationships. In power relationships, this occurs only or primarily in one direction (e.g. slaves need to know everything they can about their master in order to survive, however the master does not need to know much or anything about the slave). Much of business involves more nuanced "interpretive labor", to influence you need to think about who the party you are trying to influence is and what they want.

Alternatively if you simply hit them over the head to enforce your will – most of this communication becomes immaterial. It is in this sense that David Graeber believes that all bureaucracy is literally based on force. Business and Government in this model are in collusion. Businesses use the available force of government to enforce its goals. We as unforced individuals outside bureaucracy and force have the capacity to cooperate – but to do so we have to take the effort to understand each other mutually. The implicit or explicit threat of force is required whenever individuals bypass cooperation, often because the work to cooperate and understand is too much work.

Phil indicated that one of the cases of force over cooperation in the Internet space is the 'contract of adhesion'. All of our talks on relationships in the VRM space are predicated on all parties having to be in "interpretative relationships". Vendors often think they are in a relationship with customers, but they want the benefits without doing the work that is required. To be fair to vendors, they may really want to understand and respond to customers – but in many environments that appears to them to be not cost effective.

Phil cited another book "Seeing Like a State"; which indicated that early census was to determine the soldiers (young men) and tax base available to support war. Doc cited Corey Doctorow's review of the Graeber book as saying that everyone knows that rules are not uniformly applied; bureaucracies are supposed to be meritocracies, but everyone knows that is false.

The conversation moved back to VRM and goals of less violence i.e. less reliance on contracts of adhesion – Doc quoted his long standing assertion that free customers are worth more. Nittan asserted that current business models want caged customers because their bureaucratic model is all about independently minimizing the costs of Acquisition, Retention and Efficiency.

Doc argued that there is more that can be had by moving past this static bureaucratic view of the one road to profits and that a one-way relationship erodes trust, and therefore profits over time. We are emotionally attached to our stuff (reference to George Carlin skit). In an Internet of Our Stuff – that matters. With my shirt it is just me and the shirt once I’ve purchased it. With Fitbit – that organization is still in the on-going relationship after the sale. If we take the current model, all my connected stuff will be partially owned by a wide variety of bureaucratic entities which will continue to want to define and limit how I use it. Vehicle-to-vehicle mechanisms (like airplane collision avoidance systems (TCAS) for cars) may provide great safety benefits – but they also may decide where I can drive, stop my car, etc.

There followed some discussion of what is the ability and what are the precursors for information technology to build non-bureaucratic systems. Nittan quoted Peter Drucker as saying that “all knowledge work is volunteer” in the sense that management will in general not understand the nature of the work that the workers do. There is some movement by bureaucratic organizations to return to Frederick Winslow Taylor’s “defined outcome work” of measuring acquisition, retention and efficiency – because they know how to control it and do not have to have the costs of the relationship with workers. They are trying to move from unstructured data coming in from customers to defined outcomes. When a business has defined and rewards the outcome they are expecting from the worker (e.g. in a call center), they may simply not care who is sitting in the seat.

Conversation continued about the origins of the Internet – is it a fluke? Some discussion indicating that defined outcomes are not necessarily bad – the key question being, ‘Who gets to define the outcome?’ We can envision a world that looks like the original Internet, but we don’t know how to build it in this society.

Doc asserted that Phil’s and other systems being developed by IIW community members are non-hierarchical and that with block chain we have non-hierarchical ways to manage a directory. Audio is available for this session.

Workshop: best practices of profiles from 10 years of IIW

Wednesday 3J

Convener: Kevin Mark, Christopher Allen

Notes-taker(s): Judy C

Tags for the session - technology discussed/ideas considered:

Tagged: [digital identity](#), [iiw](#), [internet identity](#), [persona](#)

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

20 Events, 10 Years *Happy anniversary and congratulations* to the Internet Identity

Workshop crew! The event being held at the Computer History Museum in Mountain View, CA is the 20th in the series, over the course of 10 years. There are a lot of new folks here, as well as a solid group of ongoing coders and explorers.

We’re talking about the sessions to come. I’ll be posting from various sessions over the next three days.

[Continue →](#) 2015 April 7 · [event](#), [future](#), [tools](#) · [Leave a comment](#)

Defining data brokers; Use cases for disrupting data brokers; Governance/regulations

Wednesday 4C

Convener: LaVonne Reimer

Notes-taker(s): LaVonne R.

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

Possible definition (from Adrian): A data broker is anyone who has my data but doesn't allow me to sign in and see it. i.e., someone who has my data but with whom I have no relationship.

Recent FTC report on data brokers list 3 kinds:

Marketing/Ads data brokers

Risk/Fraud prevention data brokers

People Search

Is data brokerage an activity or a kind of company?

Major areas of concern include:

- Repurposing of Data (collected for a seemingly innocuous purpose, then sold and used elsewhere to profile with adverse impact)
- Whether or not consumers want transparency or control (or both)
- No disincentives for brokers and minimal barrier to entry
- Little to no transparency; no standard of ethics

Is there any interest in setting up a working group to compile a data broker code of conduct?

ISO cloud service rules depend on service provider control policies. For example, Amazon isn't considered a broker in those rules, but companies that use Amazon may be.

FCRA was created for the purpose of regulating uses of data and disclosures by granters of consumer credit. Allows for a process to see data and challenge it. Regulates the purposes for use like hiring decisions, insurance, offers of credit. The evolution of big data and modern data technologies is leaving new gaps in coverage in addition to the longer-term gap for uses of consumer credit info about the owner or team in small businesses.

Suggestion that a person could be allowed to approve every transaction involving the use of their data. Question about whether or not this scalable. Disagreement. At least it would be good to provide consent receipts.

How can data subjects push for data transparency?

How can data subjects control their own data?

It might be good to analyze what brokers do well and ways to promote doing those things while doing good; Potential for new data brokers to differentiate on compliance with code of conduct

Discussion of the problem with the government selecting a particular company's service, but granting that company an unfair advantage which they use to self-promote and market. Example is the SBA's requirement that business's use their DUNS number when applying for grants or loans. Gives Dun & Bradstreet an unfair advantage in marketing to new businesses. Those parts of the company could be separated. CPNI and FCC regulations over the telecom industry do something similar by not allowing regulated entities like telcos to cross pollinate data from the regulated side to their marketing arms. Started on discussion of use cases but ran out of time. Participants signed up to engage in crafting a code of conduct.

My Wave VRM: A Deeper Look

Wednesday 4D

Convener: James Ladd

Notes-taker(s):

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

MyWave Personal Assistant works with the information in your personal cloud and the services of the MyWave platform to assist you in meaningful ways. Showcase of the features of the platform which are available to all through the MyWave API.

For additional information:

<http://mywave.me> & <https://www.youtube.com/watch?v=TA2y4Ysckvs>

Terms we assert // Consent & User Submitted Terms

Wednesday 4F

Convener: Doc, Mark Lizar & Mary Hodder

Notes-taker(s): Mary H & Mark L

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

Main site on [Open Notice](#), also on the wiki at [Kantara Initiative Working Group](#).

Eve: Justin was sketching out a kind of technical specs, but it's not in our requirements yet. RESTful API in JSON format, with register-able endpoint, lodged in a protected way, OAuth-protected resources. You could do interesting things with a collection of these. Looks like this will be implemented about version .8; we're at .6.

Justin: UMA and OAuth cases are subset of larger usage cases of Consent Receipts.

Mark: has a spreadsheet of the many jurisdictional requirements for where consent needs to be implemented.

me: look at higher level, design for that. Implement details at jurisdictional level.

Mark: want to design for international user base.

Steve, Internet Society: We have no funds for this, not looking to make this happen. Also need to see requirements.

Mark: any requirements from Justin for technical model? Justin: much of it: pick a name, write it down, move to next stage. There will be errors in .7. Doesn't yet tell us what to do. Mark likes slash and burn. Justin: define data model in terms of values and structures (what needs to be where), map actions upon objects into API.

Justin: version numbers don't mean anything, they're not real milestones. Publish what we have as 0.7.0, update to 0.7.1, refine in 0.7.2. Next milestones with particular targets is point to switch to next version.

Desire to map to ISO standards and definitions (particularly [ISO 29100](#), European Standards). Three stakeholders: people, organizations and regulators (enforcement). Is there a form of universal consent receipts yet? There's a common set, but needs work. Third party sharing is one

complicating factor. In trust networks, you need to list 3rd parties, can manage data in that context. Mark: dynamic consent. Justin: consent needs to be an API.

Adrian et al.: a special term I dream of in medical area: don't ask me for consent unless you first give me my own data under my own control of my own authorization server. Only then will I consider other uses. There are two kinds: voluntary consent vs coercive consent. We must be informed to give voluntary consent, else it's not an enforceable contract. Looking for ways of keeping vendors honest. If we can force them to expose this UMA alternative, even if only 1% use it, the process keeps them honest. Mark: there are good companies. Joe: this is a form of a trust framework. Adrian: unless we force shutdown of the "dark network" of medical info, we won't be able to export through a public API. Very different from utility co's green button (which is a public API).

Justin: UMA is a proper subset of this. There's a lot of conceptual and machinery overlap. There are lots of other things that are unrelated to UMA. Withdrawal of consent receipts will go nowhere because they're not asking for it. Also, there are multiple security mechanisms that need to be combined. Removal of authorization doesn't necessarily stop the data flow.

Adrian: you can't have informed consent on distribution of entire records; you don't know what uses will exist for that data in years to come.

Mark showed a draft Scale of Assurance and how that maps to Consent Receipt.

***** Marks's Notes *****

Great Requirements

restful api for registering receipts

json format

receipt an abstract model

json presentation that you can see

technical requirements around re-use and viewing of the receipt

aggregation of receipts

Add the definitions and the fields, and the format to v.07

define the data model

core object of what represents a consent receipts

translate that into json mode

map action upon the object into an api

restful where possible.

0.7.0

0.7.1 - add stuff

Adrian - comment —> Don ask me for any consent - unless i get access to data that is usable. - if not the capacity for consent is not possible.

coercive consents = no consent

simple trust framework

don't ask for my data unless you give me access to data **AND**

We launched the new opennotice.org website - where people can sign up and get a consent receipt.

<http://opennotice.org/>

Also, we worked on the roadmap:

<https://kantarinitiative.org/confluence/display/infosharing/Consent+Receipt+Road+Map>

And we captured these notes below here:

<https://kantarinitiative.org/confluence/pages/viewpage.action?pageId=73728074>

VRM In the Developing World

Wednesday 4G

Convener: Sean Bohan

Notes-taker(s): Judy C

Tags for the session - technology discussed/ideas considered: [basic needs](#), [context](#), [Environment](#), [intent-casting](#), [Management](#), [resource flow](#), [signals](#), [Vendor Relationship Management](#)

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

Sean B's inquiry into what (if any) value VRM has for people in the rest of the world. Issues include:

- Maslow
- Addressing needs
- Sustainability
- May not appeal to people who have basic sustainability established
- Public distribution of basic needs (water, cooking or heating oil)
- Subsidies do not empower customers
- Not vendors (gov, etc.)
- OLA = Uber in India (cash) – signal

—

- Signals
- Optimization
- On-demand
- Auction/transaction
- SituationalContextual
- Opportunity space
- “Drafting”
- Choda, Ezee Tap – India
- Senior citizens
- Partnerships
- Tech Women (USAid)
- Inside.com

—

- Dangerous to presume
- Every country/province is different
- Cultural context
- Give the weather (predictive planning), movement of animals; situational awareness
- Corruption (!?!)
- Notifications (search of the future)
- Connections – boots on the ground, enabling civil society
- Informal economy – resource flow
- Crime (potential/remediation)
- Problems at scale

—

- Intelligent curation (content policy)

Honest(er) Ratings System: Let's Build It

Wednesday 4H

Convener: Matt Schutte

Notes-taker(s): Matt S.

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

Audio file for session: <https://soundcloud.com/matthew-schutte-1/honester-ratings-systems>

OTTO = Open Trust Taxonomy for OAuth2

Wednesday 4I

Convener: Mike Schwartz

Notes-taker(s): Mike S.

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

Mike gave an overview of multi-party SAML federations, like InCommon <http://www.incommon.org>. These federations provide a central authority that vets participants (either IDPs or SPs), and publish metadata in XML to distribute key material and attributes of the entities. For example, see and look at some of the entries (like okstate.edu) <http://md.incommon.org/InCommon/InCommon-metadata.xml>

In addition to publishing metadata, federations standardize the legal and technical policies and procedures to drive down the cost of integration. For example, InCommon has standardized on the eduPerson schema for user attributes.

No such standard exists to centralize trust management for OAuth2 entities. And in addition there are more types of entities in OAuth2. Where SAML just had IDPs and SPs, OAuth2 has OpenID Connect OPs, OpenID Connect Clients, UMA Authorization Servers, UMA Resource Servers, and UMA Clients.

OAuth2 also has more schema: in addition to user claims, there are scopes (both OpenID Connect & UMA). And the opportunities exists to also standardize ACRs for authentication and perhaps other technical schema.

Gluu had published an early implementation of OAuth2 federation, which can be found at: <http://ox.gluu.org/doku.php?id=oxauth:federation>. After discussing this with the higher education federation in Ireland, they expressed some interest to extend their Jagger federation tool to support OAuth2. See Jagger website at: <http://www.gluu.co/jag>

Mike had presented this idea previously at IIW in the fall 2014, and after talking about it for a few years, it seems like the time is right to start a working group at Kantara to start work. The conversation then turned to the scope of the standard. What would be the metadata, endpoints, schema seemed clearly in scope. Perhaps also what mechanisms would be in place for distribution or replication of the metadata.

With regard to endpoints, Roland expressed some concern about the size of federation metadata in SAML, and suggested endpoints that enabled querying the federation metadata by providing the entityid. Perhaps an endpoint that allowed querying the metadata by type (for example, return a list of all the OPs)? An endpoint for "Join"? "discovery" (webfinger? .well-known/otto-configuration) and to get a list of federations hosted by the federation provider. To form the Kantara Working Group, we need to submit the Charter, and get support from three or more Kantara members. Roland and Judy may be interested to get support from their organizations.

IIW Connectivity Between IIW's / Identity Commons

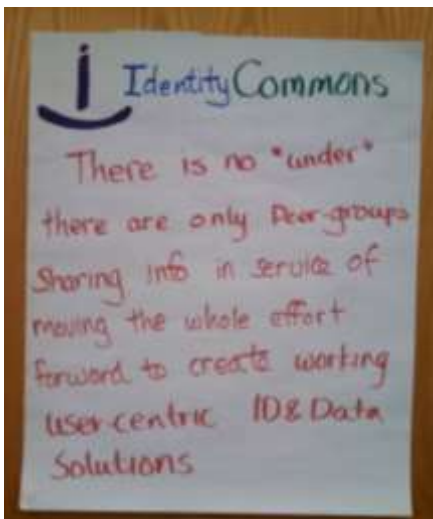
Wednesday 4J

Convener: Kaliya & Mary Ruddy

Notes-taker(s): Kaliya

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

Identity Commons - Provides lightweight community infrastructure to connect and continue conversations and work. There is no "under" there are only peer-groups (of various sizes and shapes) sharing information in service of moving the whole effort forward to create working user-centric ID and Data Solutions.



Loosely affiliated group of Identity Projects

- IIW
- PDEC
- Digital Death
- OSIS
- ProjectVRM
- NymRights
- XDI

We talked about growing the community of groups that are participating actively. Including:

- UMA
- Consent Management
- Customer Commons
- Identity North
- European Workshop for Trust and Identity
- the Australia's - Identity South?
- FIDO

A new group was started by LaVonne focused on breaking the brokers at the end of Day 2.

We have monthly calls the first Wednesday of the month at 12:15 Eastern 9:15am Pacific. We are going to update the site to be responsive design abd are thinking about an events section that would include:

- | | |
|--|---|
| <ul style="list-style-type: none">• Identity Summit• Cloud Identity Summit• Digital Enlightenment Forum• European Identity Conference | <ul style="list-style-type: none">• ID360• Identity North• European Workshop for Trust and Identity |
|--|---|



Identity Binding in the Extended Enterprise

Wednesday 5C

Convener: William Kim

Notes-taker(s): Justin R.

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

There are multiple IdPs and RPs, and in a full mesh they connect to each other in different ways.

One IdP per RP

Multiple RPs per IdP (the common way to think about it)

Multiple IdPs per RP (this is what we're after)

User has accounts at multiple IdPs, uses both at one RP

Binding is opt-in and explicitly defined by the user.

- the user says "This is me. These are my identities."
- privacy-preserving

User logs in to IBS with multiple accounts simultaneously

RP queries the IBS to ask if it has seen the user by any other name

Code is: <http://github.com/idbind/idbind>

This has been done with RPs many times (Stack Exchange), this service externalizes that

How do users decide which identities go to which RPs? (idbind project only has single list)

What about unbinding?

[Demo of open source code]

What's out of scope of project: how do RPs use this information? Some basic thought experiments to do it.

Big UX question: how do you present IdP and federated identity information to a user in a way that makes any sense?

Next major dev task is to make a simple RP to consume the information

This approach keeps the authentication context of the IdP directly with the RP

Not all IdPs are created equally, different IdPs have different security context

Creating Trust at Scale in a Sharing Economy

Wednesday 5D

Convener: Matt Muller

Notes-taker(s):

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

TOPIC:

Creating trust at scale in the sharing economy

Why do we let complete strangers stay in our homes?

QUESTION 1

What trust problems are organizations legitimately attempting to solve through the collection and use of identity and reputation data?

QUESTION 2

What are the most important aspects of reputation and identity to leverage in the sharing economy, which will allow organizations to maximize contextual benefit and minimize discrimination?

QUESTION 3

At present, the main way we quantify reputation is through one-dimensional, numeric ratings. How can we add more context to this system?

Session Organizers



Matt Muller, Privacy Manager, Inflection

mmuller@inflection.com

Jestlan Hopkins, Lead Privacy Researcher, Inflection

jestlan@inflection.com

OASIS XDI TC - open meeting

Wednesday 5F

Convener: Drummond Reed

Notes-taker(s): Drummond Reed

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

XDI TC Minutes

Following are the minutes of the official meeting of the XDI TC held at the Internet Identity Workshop at the Computer History Museum in Mountain View, CA on:

Date: Wednesday, 8 April 2015 USA / Time: 03:30AM - 4:30PM Pacific Time

ATTENDING

Drummond Reed Les Chasen Joseph Boyle Markus Sabadello	Phil Windley Kaliya Hamlin William Dyson Amanda Navarro
---	--

REGRETS

Peter Davis

GUESTS

Mark Weinstein

Review of the XDI Core Spec

The session began with a walk-through of the latest draft of XDI Core 1.0—Working Draft 04:
<http://xdi.org/xdi-spec-docbook/xdi/xdi-core-1.0/xdi-core-1.0-wd04.xml>

Drummond used the tables and examples in the spec to explain the key features of XDI to the guests.

The TC then turned its attention to the ABNF section. One remaining open issue is the syntax for a local name, as shown in the following lines:

```
external-ref = local-ref / uri-ref
local-ref   = "(" xdi-name ")"
uri-ref     = "(" absolute-uri ")"
absolute-uri = uri-scheme ":" 1*uri-char
uri-scheme  = ALPHA *( ALPHA / DIGIT / "+" / "-" / "." )
xdi-name    = global-name / local-name
global-name = name-char *( name-char / "_" / "-" / "." )
local-name  = "_" / "-" / "." *( name-char / "_" / "-" / "." )
```

Drummond clarified that the purpose of local-ref is to allow relative URIs, and that this provides a very clean way for XDI addresses to reference both absolute and relative URIs as defined by RFC 3986.

The discussion then turned to local-name rule and two related issues:

1. Should there be a local-name rule at all, or should all local names be covered by the local-ref rule?
2. If there is a local-name rule, what character(s) should be used for the leading character?

On the latter question, the consensus among the attendees was to use the underscore character as the leading character for local names.

However there was no consensus about the first question, i.e., should we even have two ways to express an XDI arc identifier whose scope is local and not global. For example:

```
+example.company=(example.person)
+example.company=_example.person
```

We ran out of time to continue discussing the issue so we will have to return to it on the next call.

XDI Messaging and XDI Bindings

Although Markus has continued to make progress on XDI Messaging 1.0 WD03 and XDI Bindings 1.0 WD03, we did not have time to review them. The most recent drafts he is working on are:

<http://xdi.org/xdi-spec-docbook/xdi/xdi-messaging-1.0/xdi-messaging-1.0-wd03.xml>
<http://xdi.org/xdi-spec-docbook/xdi/xdi-bindings-1.0/xdi-bindings-1.0-wd03.xml>

NEXT CALL The next regular meeting will be in our usual time slot, 9-10:30AM PT on Friday April 17.

Put a Voter File into a Blockchain

Wednesday 5G

Convener: Nick Carducci

Notes-taker(s): Nick C.

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

The voter registration list is the contract between a citizen and his or her government delivering them their voting rights. Their voting rights are binding for primary and general elections through this voter file, but they should also be used as evidence for advisory opinions of the actions of their elected officials.

A Guide for Integration of Authentication Technologies

Wednesday 5I

Convener: Oscar Manso

Notes-taker(s): Jonas L.

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

Authentication methods, biometrics ~ The session was about a method to compare different authentication methods

Sample case:

Virtual shop - wants to sell products from a very broad price range. Want to use different permission types depending on how much money the product costs (normal, high, unlimited).

Authentication methods are described using four groups of factors:

Context factors: Context, type of proof, applicable device

Usability factors: Complexity, responsiveness, disability discrimination

Cost factors: Implementation, deployment, user cost

Security factors: Identity assurance (how certain can you be that a user is he says who he is), credential assurance (how likely is it that the credentials can be forged), availability, revocation, renovation, privacy

Comparison of face recognition, OTP and PK systems. See tables in slide (<http://jonaslindstrom.dk/slides/iiv-oscar-manso-2015.pdf>)

Now the methodology is to list the requirements you need in your use case and compare them to the factors.

This method is used on the sample case: For each of the three levels, we define requirements to the authentication methods that are needed. One conclusion is that face recognition can not be used, because they cannot be used in a public setting.

Discussion:

A discussion on how level of assurance and other factors relies heavily on the concrete deployment as opposed to general technologies.

Outbound and inbound factors should be taken into account.

Cost factors should be put in concrete values, possibly in a range.

There was some input about similar works. One was Vectors-of-trust.

Mike Schwartz provided a couple of links on similar work:

<http://research.microsoft.com/pubs/161585/QuestToReplacePasswords.pdf>

https://prezi.com/v_h5sj0_9enx/who-are-you-from-meat-to-electrons-and-back-again/?utm_campaign=share&utm_medium=copy

https://www.youtube.com/watch?v=0w4HismSMRE&list=PLK58Vrtd56-UXsh0fFLcXW_HIGPnryOYp&index=12

UMA 101 - Everything You Always Wanted to Know About UMA but Were Afraid to Ask

Wednesday 5J

Convener: Eve Maler

Notes-taker(s): Eve Maler

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

UMA = User Managed Access

MIT KIT webinar slides from March 5th

2015: <http://kit.mit.edu/sites/default/files/documents/Eve%20Maler%20MIT%20KIT%20webinar%202015-03-05.pdf>

Recording: <http://www.dropbox.com/s/zjg7gjsmsvgpo8d/MIT-KIT-Webinar-20150305-Maler.arf?dl=0>

Business Models Based on Reputation (Part 2)

Wednesday Lunch F

Convener: Heather Vescent

Notes-taker(s): Matt S.

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

Audio file for session:

<https://soundcloud.com/matthew-schutte-1/reputation-business-models>

Thursday October 30

TOS (Terms of Service) Back 2

Thursday 1F

Convener: Steve Olshansky

Notes-taker(s): Jim F.

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

Terms of Service, Privacy Policies Link:

<https://tid.isoc.org/confluence/display/TOSBACK2/ToSBack2+Home>

The Internet Society has collaborated with the Electronic Frontier Foundation (EFF) on TOSBack2, for collecting and providing a platform for analyzing differences in Terms of Service and Privacy Policies. Steve showed a video demonstrating the TOS audit web interface.

Currently hosted in an underpowered, not really production-ready host at EFF; need to find a permanent home. Also need a long-term funding model so it will last (hosting and maintenance, etc.). But also making it production-ready. Volunteer effort, but need clueful volunteers and can't depend on them to get the effort bootstrapped.

This started at the WSJ Data Transparency weekend (2012), browser plugin to tell you if the terms and conditions have changed.

Some discussion about how to present this to consumers. Use machine learning? But every policy is a "unique snowflake".

Some surprise that the tool shown isn't more HTML-aware. There's a lot of research being done on human assistance tools so should try to leverage some of that.

We're moving to an app-based world, so a browser plugin isn't really sufficient.

Perhaps use law students to provide review and commentary about policy changes?

Discussion of possible tie-in to privacy icons (various efforts: perhaps as many as 20 projects?)

But writers of terms of service and privacy policies often don't want to be transparent.

How to handle ToS changes in apps? Perhaps through the app store?

Common Terms (commonterms.net) - effort to make terms and conditions more accessible. Check out the documentary: **Terms and Conditions May Apply**

Human Centric Computing/Scenario Planning of Avoiding the Compu Serve of things

Thursday 1G

Convener: Dave Sanford

Notes-taker(s): Matt Schutte

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

<https://youtu.be/l67SSiguAeU>

This discussion was focused primarily on how to structure interactions in a system where the holders of digital resources make use of reputation histories to:

- 1) assist them in determining who to interact with and how to engage them and
- 2) to serve as an enforcement mechanism that enables members of the community to "have faith" that, in general, agreements will be held to while
- 3) enabling members of the "digitally networked community" to disagree with one another on virtually any topic, including whether a specific action should be interpreted as an inappropriate violation of privacy or of an agreement or an acceptable deviation from the text of that agreement and enable them to nonetheless leverage one another's insights to make their own navigation of the community and its resources easier and more relevant.

We also briefly explored "pen names" and the concept of expiration dates for data, but the majority of the group concluded rather quickly that we are very unlikely (in the future) to be able to rely on a "deleting of the data" and will instead have to handle issues of redemption and of forgetting histories by using social norms to establish and enforce policies surrounding such issues.

That drove us back to the larger discussion of how to exert such pressure while also enabling disobedience to such norms when they are willing to "wear the consequences" (and enabling the larger community to adapt to such disobedience by strengthening the amount of reputation that they might require or by increasing the consequences for violating such norms).

If you are interested in working on mapping out these flows in greater detail or in actually building some of the underlying infrastructure to enable such "self-adapting social structures," please reach out to Matthew Schutte at: matt@caLabs.org

Identity Anthology: Input & Feedback

Thursday 1H

Convener: Kaliya H

Notes-taker(s): Kaliya

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

Cambria 12 Kaliya has been bouncing around ideas for an identity anthology - she outlined what she had and got input and feedback to improve it.

Book sections outlined: "The" Words

Identity * Trust * Reputation * Privacy * Security * Federation Framework * Ecosystem

Pre Identity Gang Papers: ASN Paper
 Accountable Net

Identity Gang Formation

- Cluetrain Manifesto
- Andre Durand's talk
- DIDW Meeting Doc etc.
- Dick Hardt's ID 2.0 talk
- Phil's Posts
- Johannes early Venn
- The Lexicon

Kim's Laws of Identity + Responses

- 4 More Laws - Fen
- Verifiable Minimal UnLinkable - Ben Laurie
- Axioms of Identity - Bob

IDGang Ideas + Posts

- On the absurdity of owning one's ID - Bob
- Law of Relational Symmetry - bob
- Limited Liability Persona - Bob
- Identity Oracles - Bob
- Identity Spectrum - Kaliya
- Onion Diagrams - Johannes
- Claims and Attribute - Kim

Ideas that inform Identity

- Context and Identity
- Signaling Theory
- Contextual Privacy
- Social Protocols
- What is trust?

Papers and Posts

- The trouble with Trust and the Case for Accountability Frameworks
- At a Crossroads: Personhood and Digital identity in the Information Society
- Properties of Identity

Identity and Relationships

- A Relationship Layer of the Web
- Gender and Drop Down Menus
- Designing a Better Drop Down Menu for Gender
- Disalienation: Why Gender is a text field on Diaspora
- Nym Rights and issues - Kunta Kinte

Personal Data Concepts and Principles

- Vendor Relationship Management
- The Support Economy
- Exploring Privacy
- Lumascap of Display Advertising
- My Digital FootPrint
- WEF Reports + Diagrams
- The Paradox of Choice
- Visions and Principles for the Personal Data Ecosystem
- PDX Principles
- User as a Point of Integration

Privacy Frame

- Ann Covukian's Take
- Daniel Solove's Work
 - Taxonomy of Privacy
 - Model Regime of Privacy
 - Understanding Privacy
 - Future Reputation
 - Nothing to Hide

Evolution of FIPPS

- 1974 Presidential Commission, 1980 OECD, 2000 FTC, 2010 NSTIC

Bill of Rights

- Social Network Users Bill of Rights
- Social Media Users Have these Rights
- A Bill of Privacy Rights for Social Network Users
- A Declaration of Health Data Rights
- The New Deal on Data
- The Properties of Identity
- The Bill of Rights for users of social web
- The Data Bill of Rights

Core Systems Thinking Works

- Visa the Original Trust Framework
- Life Organizes around Identity
- Intervening in Systems

Feedback from the Session

- add in -> Jeff Jonas - Talk from the last DIDW - space/time travel data

Anil John's work

- Look up Archives of Identity Gang

Paul T's work

- Mary Ruddy

- Eve Mahler

Identity and Government Section

- In local National and International Efforts
- IBM and the Holocaust
- CoIntelPro
- Right to be forgotten
- EU Constitutional things including MyData MesInfo
- DMCA

Technologies Section

- OpenID
- OAuth Eran's posts
- CardSpace/InfoCards
- Mozilla Persona
- Hailstorm

Movies

- We Live in Public
- GATTACA
- Sunshine of the Spotless Mind
- Black Mirror

Fiction

- TrueName
- TheCircle

My Own \$5/mo UMA Authorization Server

Thursday 2E

Convener: Adrian Gropper

Notes-taker(s): Eve Maler

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

The HEART WG is potentially relevant for this conversation.
MITREid Connect is potentially relevant for this conversation.

Adrian does privacy advocacy. "Ownership of data" is a fraught term that he generally tries to avoid. But ownership of the authorization for access to data is conceivable. Here's an attempted definition: "There is no privacy policy." (Because there is nobody to have it with!) An UMA Authorization Server can be a Build, Run, or Outsource (Buy) proposition. Building your own AS makes ownership of authorization for access to data possible!

These are all still compatible, no matter which path you take, or even if you switch paths. Think of the example of email servers -- same thing. Dynamic registration of clients has to be handled and watched carefully in each of these paths.

In the HIE (Health Information Exchange) work Adrian has done, typically at the US state level, and the UMA work he's done, he's dreamed of being his "own HIE". The goal is "an HIE of One". How could this community build a reference implementation for this vision? Imagine, e.g., a Freedom Box for an HIE of One.

Alan K, when at HP Labs, had done some personal cloud appliance experiments, with the WebKey technology. They used self-signed certificates and DNS name registration. The appliance would re-register whenever needed. They worried that latency would be a problem, but it wasn't. It was possible to get a free certificate that could generate other certificates.

Hardware:

- HP MyPersonalCloud appliance
 - Self-signed certificates: \$0
 - DNS name registration: \$15/year
 - WebKeys
 - No fixed IP address
 - Open source
 - Plug into router and email address in and out

Virtual hardware:

- OpenPDS (from MIT Media Lab, Sandy Pentland's lab)

Service:

- MITREid Connect (includes UMA)
- DigitalOcean (?) - Droplet

Phil suggests the idea of a cPanel, which is a control panel that could be installed on behalf of an individual ISP subscriber at a hosted domain. A Droplet isn't cPanel compatible, but the basic idea is the same. You would just need a credit card and then you could share a compiled Droplet. The only problem is that DigitalOcean won't do this for under \$10/month.

However, a Droplet gets you only 512Mb of RAM, which is pretty constrained. Could a \$40/mo virtual machine be worthwhile for a household? But then that changes the "ownership" equation. Spring is, unfortunately, very RAM-hungry.

Part of the HP business model was that if you bought a PC and support contract, then that would cover the cost of the cloud. Could that work here? With Apple HealthKit, maybe so -- or if you don't trust them, maybe not. :-) Right now, we have Prodigy, CompuServe, AOL, and SMTP -- we just have to get them all to speak SMTP!

Adrian's vision is that he wants to have, on his business card, the one string that lets him register his authorization server when he goes to a new doctor's practice etc., and then the only other possible thing on top would be a consent receipt. No messaging service or anything else would be required, other than compatibility with UMA.

Eve notes that there is more than just technical compatibility here. The systems have to work together, and interop and conformance help with this, but trust frameworks need to come into play here. It's not just institutions that impose on people; people impose their constraints on institutions and doctors too. E.g., people don't like seedy doctor's offices and want to know their data in a resource server is being treated securely. It's a "TOFU" (trust on first use) type of decision, built up from bilateral interaction.

The HP model nicely allowed for an application to be used directly by the requester with perfect compatibility. With the RESTful model, however, the URL (resource) pretty much assumes that the client needs to learn the API in question. The cool thing is that a marginally smart UMA client that knows the API in question can do trust elevation and get busy getting access.

A mobile device is really going to have to be involved if we want people to be comfortable using the interfaces to these authorization servers.

The important thing about ownership of the authorization for access to data ("There is no privacy policy" needed because there's nobody to have it with) is that it's absolutely necessary for true user-managed access (lowercase) of health data. The cool thing is that there seem to be a number of hardware and software options for building it in the not too distant future. The sticking point is that others in the ecosystem will have to come to accept dealing with an individual's chosen authorization server. If those other ecosystem players start speaking the FHIR (Fast Healthcare Interoperability Resources) API, then we can start really cooking with gas.

Useable PKI

Thursday 2F

Convener: Steve Olshansky

Notes-taker(s): Andrew Hughes

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

PKI is 20 years old, ongoing frustrations about lack of adoption

- Consumer adoption has to be zero effort from their perspective - i.e. having the right value proposition for the tech
 - Also need to demonstrate that their lives would be better in some way with crypto
- Key management is still a problem
- Tech experts tend to overestimate the value or purpose of crypto
- There may be value in use of certificates for digital signatures/protection
- In Denmark, everyone has an eID (public/private keys) that they can use for real life purposes. But it would not have happened without the Government doing it for their own purpose.
- Need to find a better mid-way solution for key management, maybe cloud-based/enterprise run, that is 'better' than today but not necessarily perfect
- Why not just blockchain it all?
- Lots of discussion about encrypted communications
- What are the issues with PKI that need fixing?
 - Nothing is really, truly interoperable
 - There are some security flaws that are addressed over time
- What is the problem that needs to be solved?
 - It is hard to get end-user applications up and running
 - Maybe it's a user-education problem?
 - How do we get herd immunity?
- Expectation management is needed
 - Fear of loss of keys equals loss of access to my stuff
 - To make it ubiquitous, it probably needs to be adopted by a mass-market producer. e.g. Unix only became ubiquitous when Apple picked it up
- Keybase.io
 - Key issuer model - can accommodate all kinds of different key models
- Blockchain
 - A secure data store with distributed copies of the ledger
 - Blockchain creates the notion of 'ownership'
 - Can create the ability to prove and protect ownership over any data object - global registry

- PGP keys can be stored in the profile which means that the username can be considered trustable to the same level as the key
- onename.com/ryanshea
 - Built on OpenName protocol
- Service providers
 - Provide services to fill many of the stated needs (encrypted email exchange, encrypted file sharing, etc)
 - Issue is do you trust the service provider
 - keybase.io is moving to a desktop model to enable the ability to detach from the servers and do local processing
- Need to look to correlated/corroborated sources
- The onetime.com setup ceremonies seem to take effort & is that too much to expect?
 - The 'runtime' operations - does it take effort to validate that the communication is trusted? Apps still need to be built - but it's easy to design and build.
- U2F seems to be moving in the right direction
- Seems that removing the CA / central infrastructure wherever possible (for peer to peer at least)

API Fusion Drives

Thursday 2G

Convener: Craig Burton

Notes-taker(s): Matt Schutte

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

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

API's (Fusion Drives) <https://youtu.be/Mqmei4BqFqI>

This was an introduction to how API's work, making use of an API from NPR to walk us through the structure of an Application Programming Interface, the requests that are made, the structure of the data coming back and an example of how that structured data might be modified so that it is presented in a more human friendly or aesthetically pleasing format.

Enterprise Single Sign On and Social Network (mobile centric)

Thursday 3D

Convener: Matt Voger

Notes-taker(s): Matt Voger

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

A demo was presented the Yada protocol to the group showing an identity located on a mobile device being used to authenticate with different systems and how those systems could disseminate friend requests and friendship between each other.

The bulk of the discussion was related to the explanation of the Yada protocol and how it can enable to global social graph aka distributed social network.

The group determined that possible industries for this technology include healthcare and the transfer of patient medical history.

Challenges included creating policy to determine what information is share with which relationships. This was accepted as an action item for development.

Another concern was enterprise identities for employees being accessible able the employment ends. The solution to this would be to make the identity only accessible though VPN.

It was finally determined by the group that if the policy implementation were satisfactory that the Yada protocol could be a viable solution in distributed identity environments, including healthcare.

User Terms Continued

Thursday 3F

Convener: Doc, Mark, Mary

Notes-taker(s):

Tags for the session - technology discussed/ideas considered: #UMA #OAuth #VRM

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

If terms materially change, with no additional consent asked, there are not compliant. There is an opportunity to withdraw, but also to submit our terms to them.

Value from personal data control with terms and PDstores or other repositories we control is there. USTs could be submitted with UMA or from other PDSs.

USTs

Time Purpose Ads/ Tracking

What about gag rules where they say you can't talk about the terms (common in Health TOUs)?

Customer Commons terms are better than company's terms.. and could also really help. And individual terms are from the other side.

Need lawyer, human and machine readable terms.

Technical requirements for Consent Receipts:

1. Restful APIs registering Consent Receipts
2. CR -> abstract data model using Json data model
3. Protected so you can see it -- needs security

Cases for CRs:

UMA

OAuth

VRM companies

Define data model:

Core object: values & structures

Define consent receipt in that form

Translate into json mode

Map actions onto api (restful where possible)

Use ISO definitions and other standard descriptors

Work with other orgs like TOS/Back and dump repository etc.

Digital ID Images

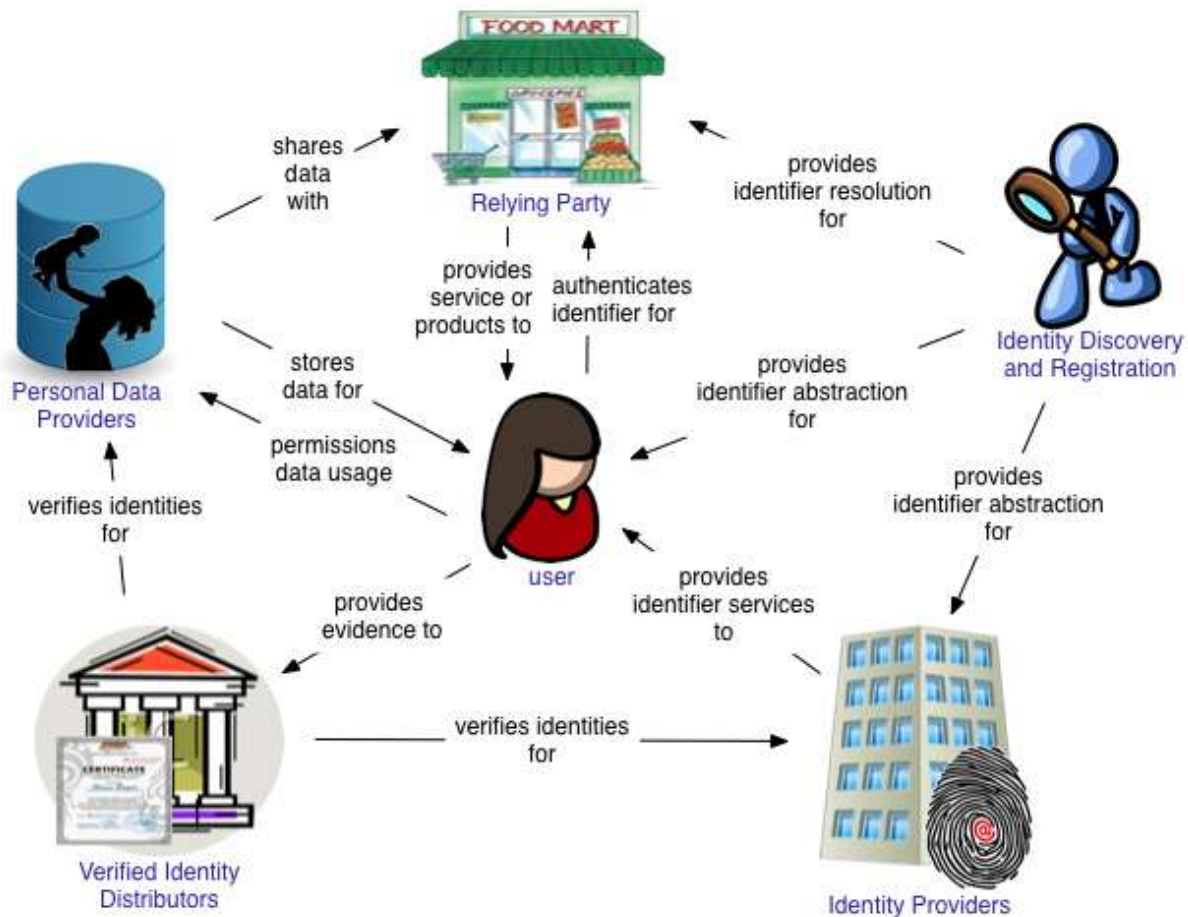
Thursday 3H

Convener: David Kelts

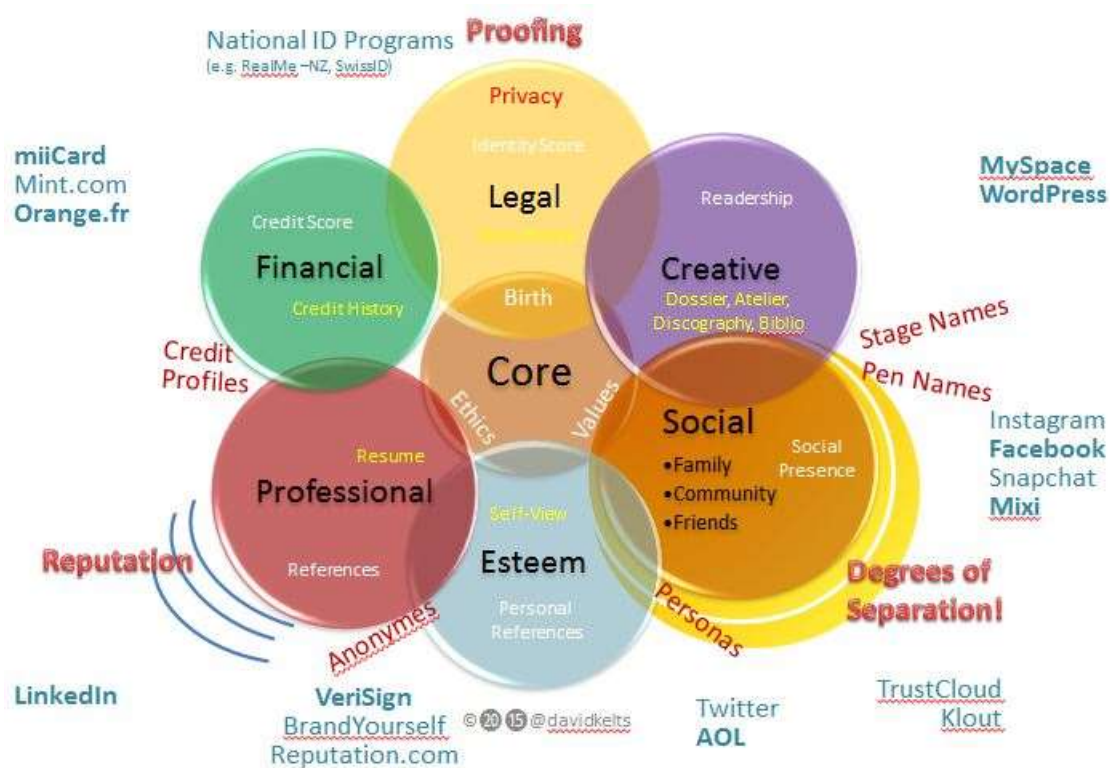
Notes-taker(s):

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

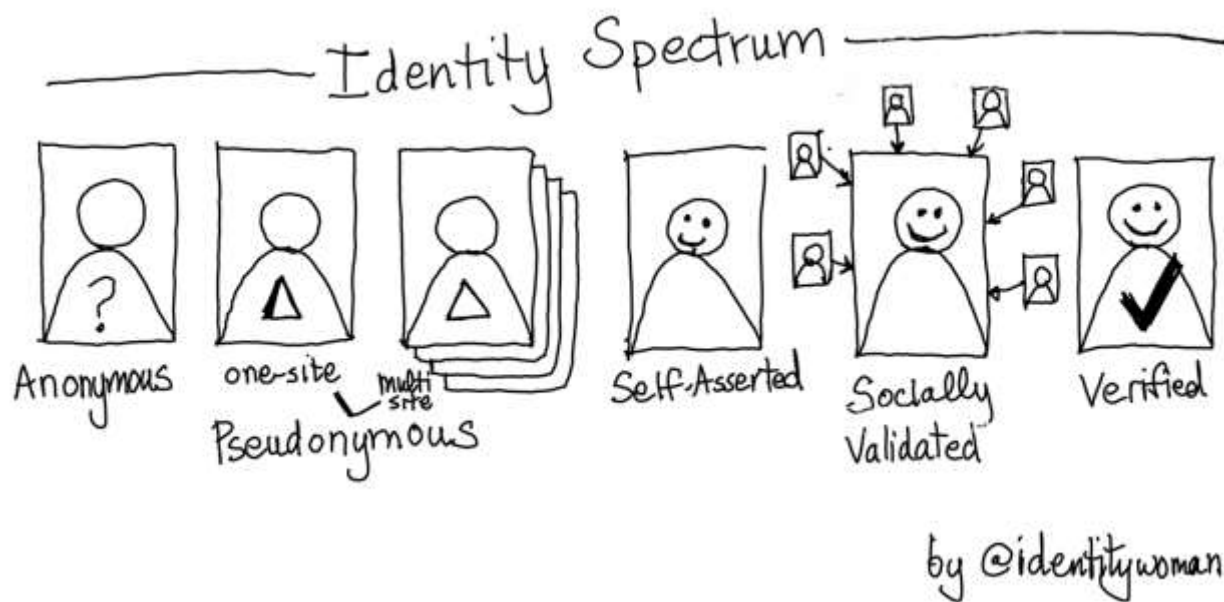
Visuals that helped us create clarity on some Identity Topic



Phil Windley – What is an Identity Ecosystem






David Kelts – Domains of Human Identity, into which we’ve organized our systems (and should)

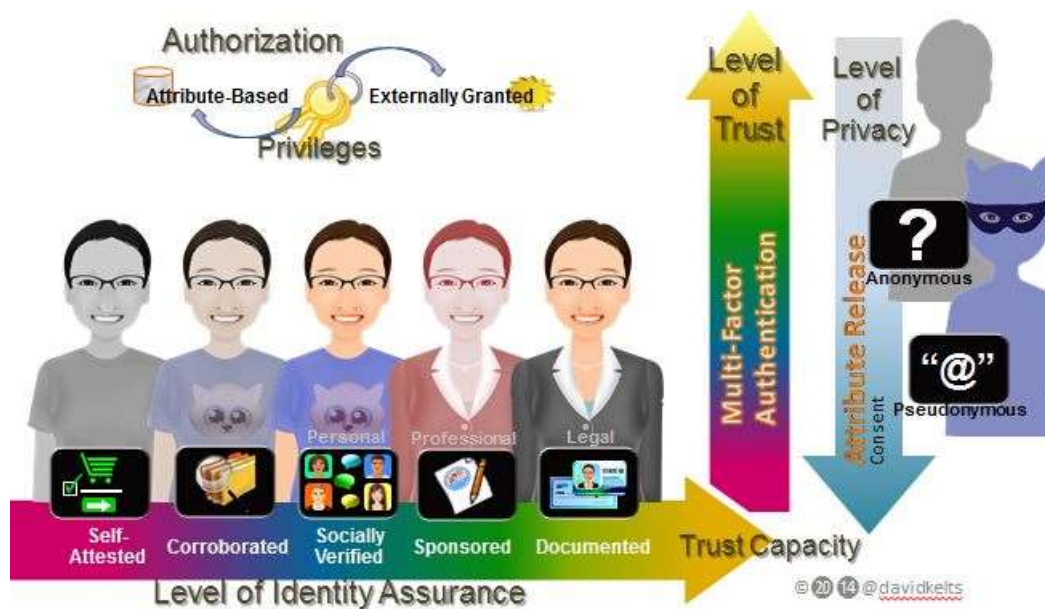


Kaliya – Identity Spectrum

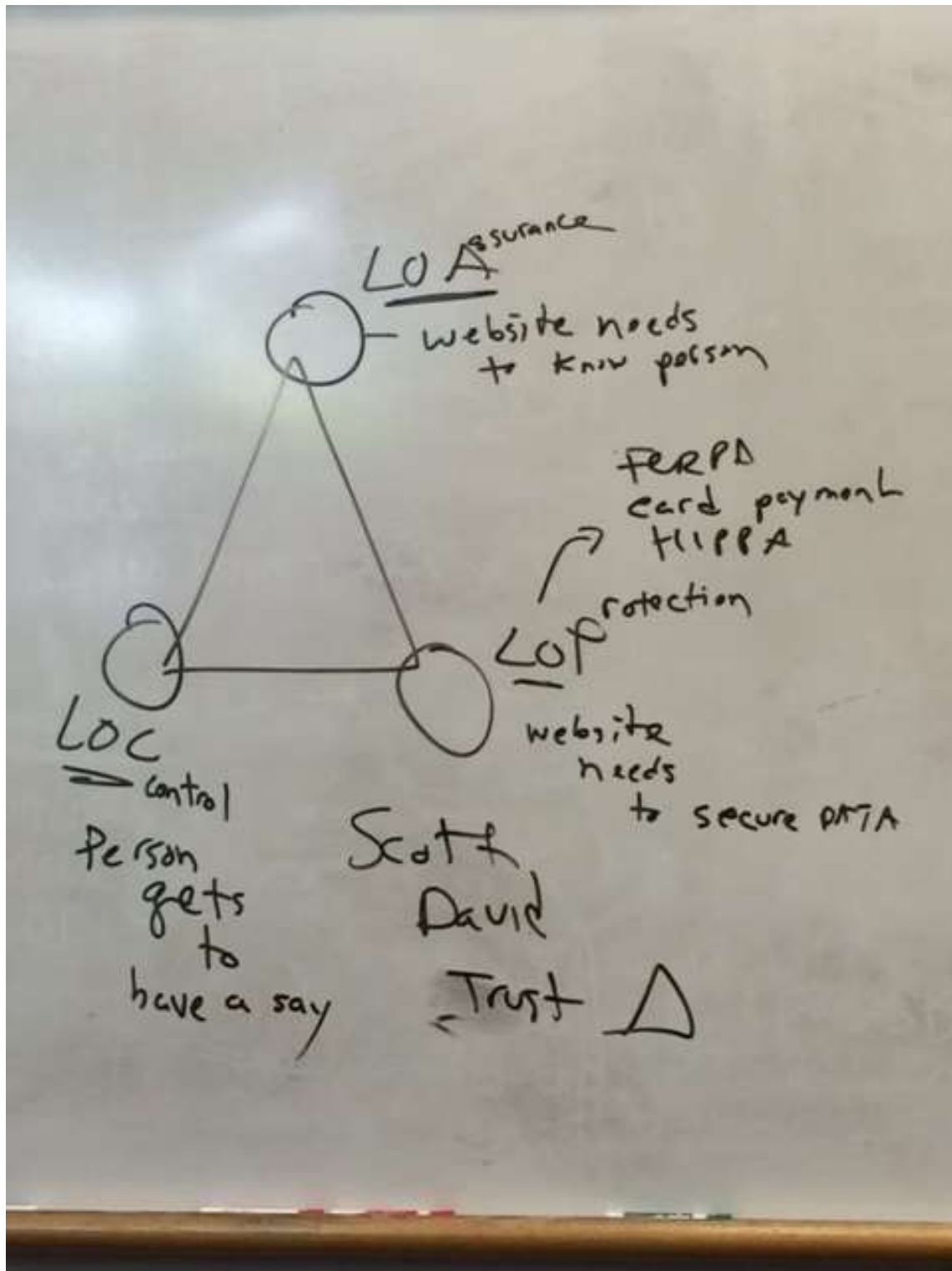
	1	2	3	4
same unique user	yes			
user was proofed	no	remote or in person	remote or in person	in person
verified name provided	no	no	yes	yes
authn strength	weak	a bit stronger	stronger still	really strong
crypto key possession		optional	soft tokens	hard token

-  simple cross-session correlation
-  identity proofability
-  real-world identity mapping
-  cryptographic token strength

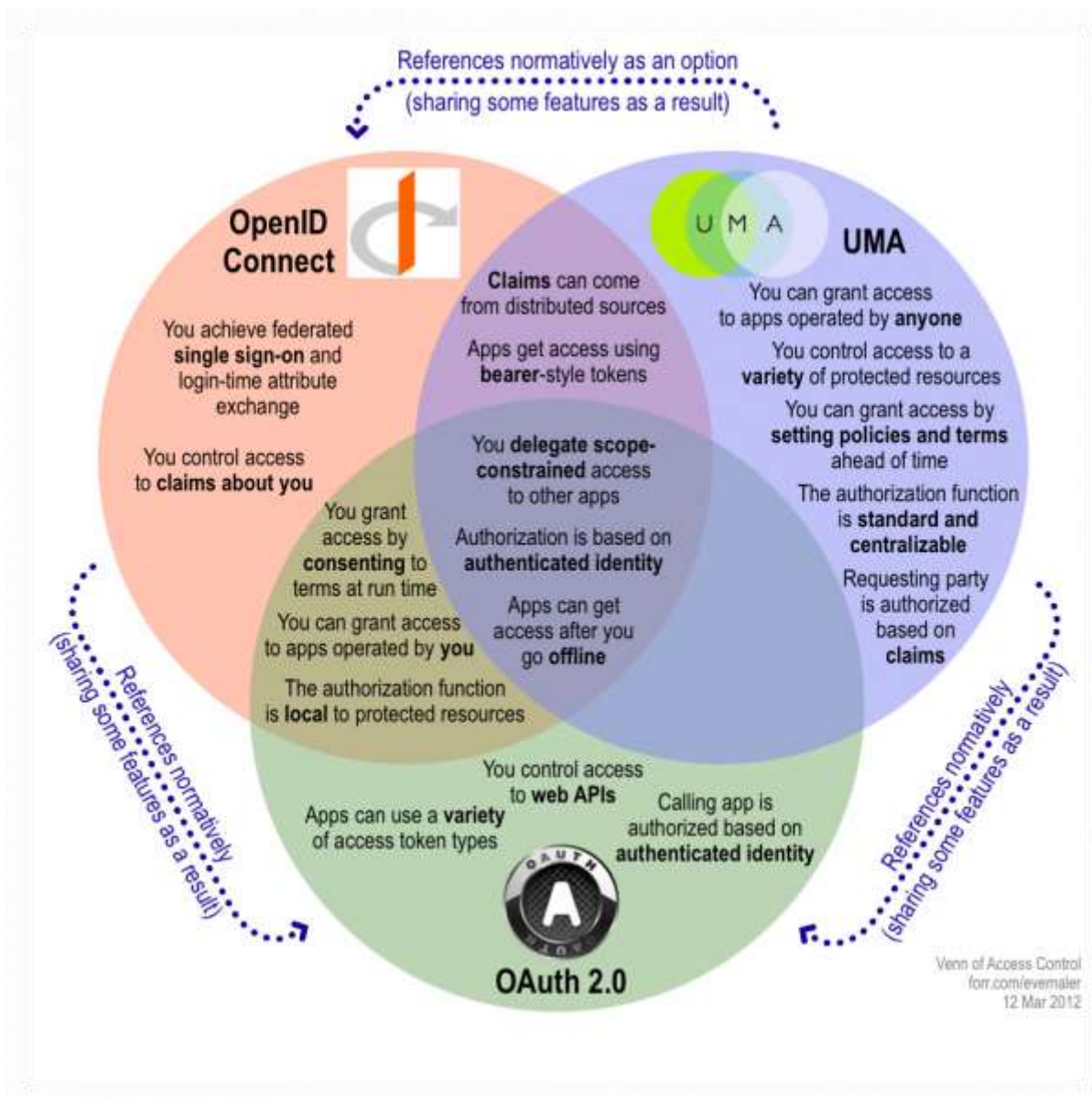
LOA Defined in a Table



David Kelts – Identity Spectrum evolved into Levels of Assurance



Mike Schwartz contributed Scott David's Levels of Trust



Eve Maler – Venn of Authorization

Implement Indie Web on your service in minutes (Indie Web Camp)

Thursday 3J

Convener: Kevin Marks

Notes-taker(s): Kevin Marks

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

[Google](#), [HTML](#), [Indie Web Camp](#), [Instagram](#), [Internet](#), [Microformat](#), [microformats](#), [Real-time web](#), [Semantic HTML](#), [Semantic Web](#), [social media](#), [social media tools](#), [Technical communication](#), [Technology/Internet](#), [Twitter](#), [World Wide Web](#)

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

Ideas behind this session are at Indie Web Camp.

Kevin introduced, explained webmention, a simple way to notify any URL when you link to it on your site. Includes two parameters: source and destination. It's how he collects his tweets on his home page, also using Bridgy to implement the backfeed from Twitter to Kevin's [...]

[Continue →](#) 2015 April 9 · [friends/family](#), [future](#), [records](#), [tools](#) · [Leave a comment](#)

Open Notice and Consent Working Group

Thursday 4F

Convener: Mark Lizar, Mary Hodder, Justin

Notes-taker(s): Judy C

Tags for the session - technology discussed/ideas considered:

Tagged: [API](#), [authorization server](#), [Consent](#), [Kantara Initiative Working Group](#), [Oauth](#), [Technology/Internet](#), [trust networks](#)

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

Eve: Justin was sketching out a kind of technical specs, but it's not in our requirements yet. RESTful API in JSON format, with register-able endpoint, lodged in a protected way, OAuth-protected resources. You could do interesting things with a collection of these. Looks like this will be implemented about version .8; we're at .6.

Justin: UMA and OAuth cases are subset of larger usage cases of Consent Receipts.

Mark: has a spreadsheet of the many jurisdictional requirements for where consent needs to be implemented.

me: look at higher level, design for that. Implement details at jurisdictional level.

Mark: want to design for international user base.

Steve, Internet Society: We have no funds for this, not looking to make this happen. Also need to see requirements.

Mark: any requirements from Justin for technical model? Justin: much of it: pick a name, write it down, move to next stage. There will be errors in .7. Doesn't yet tell us what to do. Mark likes slash and burn. Justin: define data model in terms of values and structures (what needs to be where), map actions upon objects into API.

Justin: version numbers don't mean anything, they're not real milestones. Publish what we have as 0.7.0, update to 0.7.1, refine in 0.7.2. Next milestones with particular targets is point to switch to next version.

Desire to map to ISO standards and definitions (particularly [ISO 29100](#), European Standards).

Three stakeholders: people, organizations and regulators (enforcement). Is there a form of universal consent receipts yet? There's a common set, but needs work. Third party sharing is one complicating factor. In trust networks, you need to list 3rd parties, can manage data in that context. Mark: dynamic consent. Justin: consent needs to be an API.

Adrian et al.: a special term I dream of in medical area: don't ask me for consent unless you first give me my own data under my own control of my own authorization server. Only then will I consider other uses. There are two kinds: voluntary consent vs coercive consent. We must be informed to give voluntary consent, else it's not an enforceable contract. Looking for ways of keeping vendors honest. If we can force them to expose this UMA alternative, even if only 1% use it, the process keeps them honest. Mark: there are good companies. Joe: this is a form of a trust framework. Adrian: unless we force shutdown of the "dark network" of medical info, we won't be able to export through a public API. Very different from utility co's green button (which is a public API).

Justin: UMA is a proper subset of this. There's a lot of conceptual and machinery overlap. There are lots of other things that are unrelated to UMA. Withdrawal of consent receipts will go nowhere because they're not asking for it. Also, there are multiple security mechanisms that need to be combined. Removal of authorization doesn't necessarily stop the data flow.

Adrian: you can't have informed consent on distribution of entire records; you don't know what uses will exist for that data in years to come.

Mark showed a draft Scale of Assurance and how that maps to Consent Receipt.

[Continue →](#) 2015 April 9 · [future](#), [records](#), [tools](#) · [Leave a comment](#)

[In] security Sessions

Thursday 4J

Convener: Jim Fenton

Notes-taker(s): Jim Fenton

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

We had a small but engaged group for the Insecurity Questions session. We discussed several examples of "security" questions that appear on the Insecurity Questions blog site:

<https://insecurityq.wordpress.com/>

Several key points:

- Despite what some sites say, setting up "security" questions does not improve your account security, it degrades it.
- "Security" questions are really about cutting customer support costs, not about improving security
- This is a practice that is effectively banned in some areas of Europe (e.g., Sweden).

Send us more examples! See the instructions at

<https://insecurityq.wordpress.com/about/>

Architecting Future Scenarios: Digital communities that self-balance on reputation, privacy & other norms // Pen Names

Thursday 5E

Convener: Matthew Schutte, Amy Ng

Notes-taker(s): Matt and Amy

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

Future Scenarios Audio/Video link: <https://youtu.be/IH1rETUdehE>

This was a discussion about possible future scenarios for information systems and society. Discussions included:

- The Borg
- Totalitarian Regimes
- Corporate Feudalism
- Anarchist Dystopia
- Global Networks that mimic local villages and reputation

Discussion also dove specifically into Privacy, Technology that facilitates privacy control as well as concepts such as areas where such technology fails for certain people or purposes while succeeding for others.

Amy's Notes for Pen Names: The session ended up being mostly about Matt's topic. In general, I had assumed that folks would want to have separate actual identities (legal) and pen name (artistic) identities. I also had a second assumption that people would want pen name identities to expire at some point, but the group didn't agree with this last point. I used an analogy of old computer systems: mainframe computers, VAX machines, SGI workstations, IBM desktops, the Atari 800, 5-1/4" floppy disks, 3-1/2" floppy disks, iOmega drives, etc., and talked about how those technologies didn't have forwards compatibility built into them, so why would we expect our identities to do that?

So the summary is that 1) everyone agreed that they wanted separate identities on the internet, and that there are various ways to achieve that technologically, and 2) no one agreed that those identities should expire, since the feeling was that it helped someone build their reputation online, and that the background / history would help aid that.

Matt - People within the group didn't think it was technologically likely that identities would expire, which is different from thinking that they "shouldn't" expire. An example: people can always snap a photo of the original, and could write translation software that makes "unreadable" content (due to storage in some deprecated medium) readable by anyone.

An awareness about the limits of our ability to use technology to enforce expiration led the people in the discussion to focus instead on searching for other tools to help communities agree upon, and enforce, expectations about concepts such as expiration of identities, redemption and similar such norms related actions.

Mozilla Listens to IIW

Thursday 5F

Convener: Sean Bohan & Brian Warner

Notes-taker(s): Sean Boahn

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

Agenda: Mozilla has been to IIW before, but this is Brian's first time. We want to engage the community and start discussions around what Mozilla is doing in Privacy/Identity and what the community needs. Brian had deck slides and they will be posted.

Notes:

- Mozilla is an Ecosystem of multiple platforms (desktop, android browser, \$25 smartphone OS)
- We are working on Persona, Accounts, Sync
- Marketplace for apps and small-scale storage are also a part of that and critical needs
- Mozilla is using symmetric encryption keys
- Not an not an Identity Provider for 3rd party services, our work right now is aimed at mozilla services
- We need to know browser has rights to modify or read and the auth mechanisms as well
- sync/storage accept browser id insertions
- Client creating data -using KeyB because server should not see it
- Use case - Firefox marketplace to buy html applications
- run from any desktop browser
- receipts tied to Firefox account
- greet you by name

Crowd:

- Have we looked at UMA?
- UMA on top of OAuth
- Mozilla:
- We don't know much about UMA - and will look into it
- User Managed Access - more for user controlling policies for access to the data
- We are thinking of whitelisting specific apps and the marketplace can learn without asking
- 3rd parties have to get permission

Crowd:

- UMA for the person to control
- good opportunity - who wouldn't want to use PDS for some requirement
- wonderful opportunity
- mechanisms like that - share specific data - separate keys
- share keys with different recipients

Adrian -

- MIT has 2 camps looking at OAuth
- one camp - PDS users must use it as part of the big data thing
- second camp - make sure the server, encrypt, so server can't be controlled and keys to the server are handed out specific to the query
- service based system - payment serv or shipping serv
- legal recourse if it's required

Crowd:

- doing purpose built value add vertically integrated version of YAS?

Mozilla:

- Firefox accounts - our intention right now is to solve the needs that we have, to solve for issues we have - also to get to be a bigger player in this space by bringing more to the space
- Right now the only APIs supported would be Mozilla services
- The Profile stuff we are working on is new
- User Personalization is related
- Drummond:
- Gen question - whole ecosystem, interop, doesn't it make sense for that what we are building be an interoperable personal cloud
- These questions are the questions for all uses of personal clouds: encryption, how to encrypt? etc.
- If best practice/interop are developed and Firefox is a user agent - then it seems we cross into new space

Brian:

- what features you want in the browser to support it?
- things we thought of - before Accounts was "profile in the cloud" - should be retrievable from any device - interesting ways to combine 2 factor stuff, kiosks, flight, etc.
- "pickle" - get browser profile to be cloud and not local drive
- extend from that - other things kept in synch with other cloud services
- bookmarks synch with other cloud services
- bookmark synch - provide better framework - synch server one choice

Adrian:

- Wants to see on the slide is a cert authority –
- agrees with asa and Drummond - if moz would use it's leverage to put the 3 things together - demand issues desire to evolve consistent steppingstone and the splice point into the reality of pki with all of it's faults
- wants Mozilla to solve user experience prob for PKI
- Drummond:
- adoption of pclouds and user recognition of clouds
- Mozilla listening - big deal

Asa:

- Uses chrome - because it has users he can switch from and testing
- If Firefox were not conflating concepts of accounts and who I am that would be great
- Better: there would be a hard and fast - this cand that can learn and see how behavior models diff personalities that would be grt
- ideal - go to banking site and not worry cookies or connections would be needed
- dont need a plugin or ridiculous chrome profiles

Brian:

- Big thing to fix and nail down the UI for that
- Thinks we need to have aspects of Firefox Accounts that affect the behavior of the browser - ties to Sync
- website signing into with other identities
- remembers set of emails you have control over
- remembers last email - defaults to that
- set of addresses persona knows about
- mapping rp to address
- ID given to a given website - enables within that profile

Ping Identity person:

- killer feature to be secure discovery service
- introduce to the right services (federation or something else) pds - if we can be central place that stores pointers but gives usability and ability to plug things in
- not just an ask for PDS integration - ask for this to be a theme and a system others can plug into
- BETTER IF browser delivered privacy exp they want

Drummond:

- Early features - ironic "what can browser do for me"
- from his perspective - privacy prob
- private browsing modes one aspect
- new aspect control over info and releasing - lot picking up on it
- html 5 meta referrer none

Brian thinks it's great

Sean says Mozilla is definitely coming back to IIW

H.E.A.R.T. Working Group Session - UMA Security Profile

Thursday 5H

Convener: Justin, Eve

Notes-taker(s): Eve

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

Brainstormed list from going through (most of) the existing OAuth profile that was contributed to the HEART WG:

1. UMA usage of embedded OAuth:

- Relevant to PAT issuance and AAT issuance
- OIDC/OAuth client authentication implications - use JWT stuff?
- Add more MTI grant types a la OAuth profile?

2. UMA usage of (extended) JWT when bearer RPT is introspected:

- Borrow ideas from OAuth profile 2.2?

3. UMA redirect logic:

- Copy OAuth instructions

4. UMA OAuth client registration (both UMA RS and UMA client):

- Use JWK advice

5. UMA AS config data:

- Add a key property?

6. UMA RPT profile:

- Need to do anything? Already have bearer token that must be introspected to get extended JWT
- Add time-to-live strategy stuff

Random idea: Add a diagram to OAuth profile for client trustedness and UX implications?

"IIW is the place we go to be challenged, to think and set the direction of our business. It is three days of discussions & deliberations where you can really test, improve and even launch that next step toward growing your company in an environment that supports people with passion and ideas. Thank you, IIW!"

Heather C. Dahl & Chase Cunningham
Co-Founders, [The Cynja](#)



The Third IIW Women's Wednesday Breakfast



We had many new faces at IIWXX including quite a few women. At the close of Tuesday's circle we invite the women to connect over breakfast Wednesday morning. This year the table was overflowing ~ maybe we'll need two of them in October!



We shared who we were, what we did, where we came from in the world, along with a bit about what inspired our work. We talked about the topics we had heard discussed on the first day of IIW and the ones we hoped to discuss in the coming days.



We hope you will reach out and invite women colleagues you know in the field who would enjoy and contribute to IIW. We can't wait to meet them.

Thank You to All the Fabulous Notes-takers!

There were 84 distinct sessions called and held. We received notes and/or white board shots for 67 of these sessions. Thanks to those of you who submitted notes and information!



Demo Hour



1. **ForgeRock OpenUMA implementation of User-Managed Access (UMA):** Eve Maler
URL: <http://www.forgerock.org/openuma/>
"Privacy is hard." "People hate consent dialogs." Actually, privacy can be easy, and consent can mean control. UMA enables open API ecosystems with privacy-enhanced data sharing built in. OpenUMA shows how easy the user experience can be.
2. **Gluu, Inc. Demoing the Gluu Server's UMA functionality:** Mike Schwartz, CEO
URL: <http://gluu.org/overview> , <http://gluu.org/uma>
How to use UMA, a new standard profile of OAuth2, in the Gluu Server to control access to APIs and web resources.
3. **Decentralized, Linked Credentials:** Brian Sletten
URL: <http://opencreds.org>
The W3C Web Credentials Community Group researches and implements potential future standards of interoperable, network-friendly credential exchanges. I will demonstrate a prototype of a decentralized credential exchange ecosystem.
4. **How Identity Can Combat Current Data Breaches:** Chris Barngrover, NetIQ
URL: <https://www.netiq.com/solutions/security-management/data-breach-threat-detection.html>
After data breaches occur, post analysis often finds clear evidence of malicious activity in the audit logs. WHAT IF you can detect threats to your systems in time, to stop the attacker before they can do damage? This demo will propose a new approach.
5. **Lumenous:** LaVonne Reimer, Descant Inc.
URL: <http://www.lumenous.net/solution.html>
Lumenous is a data-sharing platform that uses a business credit profile as visualized personal data store; Demo will focus on key features embodying design according to the principles of ethical data management.
6. **MeWe: The World's Private Communication Network:** Mark Weinstein
URL: <https://mewe.com>
Welcome to MeWe: The revolutionary new experience where you connect to your contacts and communities and we never sell you or your data. Let's MeWe!

7. **Frank, MyWaves Personal Assistant:** James Ladd, MyWave Chief Technology Officer
URL: <http://mywave.me> & <https://www.youtube.com/watch?v=TA2y4Ysckvs>
James will show Frank, MyWave Personal Assistant that works with the information in your personal cloud and the services of the MyWave platform to assist you in meaningful ways. Showcase of the features of the platform which are available to all through the MyWave API.
8. **Swiss Tabula Rasa Policy Game:** Britt Blase, Nick Carducci, Morgan Rockwell Founders, Thumbprint.us
The Swiss Tabula Rasa policy game is coming to the US. What do you want us to include? Tabula Rasa, a government policy role-playing game for constituents to crowdsource policies and push them to their representatives, leveraging Polygon Identity in the Personal Democracy Cloud PicoSystem (Policy & Issues Ecosystem), supporting the PDC Knight Challenge
9. **Inter-Domain Social Graph:** Matt Vogel, VMWare
Matt Vogel will show how two users of two completely separate websites only need to become friends once for their friendship to appear on all other sites throughout the web, automatically, while retaining complete control over their privacy.
10. **U2F, Delivering Security Beyond Passwords and Flipping Authentication on its Head:** Jerrod Chong, CISSP. VP Solutions Engineering, Yubico
URL: <https://www.yubico.com/applications/fido/>
Demo will showcase FIDO U2F open authentication standards and YubiKeys – a single device to authenticate to any number of services. Actionable steps on how companies can harness strong authentication without adding burdensome steps and how increased adoption of authentication technologies is enabling true end-point security
11. **Meeco - A world first VRM & Life Management Platform:** Katryna Dow - Founder & CEO
URL: <https://Meeco.me> BLOG: <https://blog.meeco.me>
Collaborate with the people & organizations you trust. Securely manage and share your information, link IoT devices, manage social channels & connect contacts. Signal your intentions and use insights from your personal timeline to make better decisions.
12. **Bitseed Bitcoin Edition:** John Light
URL: www.bitseed.org
Bitseed Bitcoin Edition is plug-and-play dedicated hardware to deploy and maintain a bitcoin full node on your home or office network. This product can be used by developers to build bitcoin applications, and can be used by regular bitcoin users to support and strengthen the Bitcoin network.
13. **Nōtifs:** User-Managed Notifications, Jim Fenton
Nōtifs allows users to opt in to receive notifications of all sorts --from advertising to emergency alerts -- on their own terms. A prototype implementation of Nōtifs will be shown; let's talk about how you would use it!
14. **Thumbprint:** Nick Carducci & Morgan Rockwell Founders
URL: Thumbprint.us
A voter to politician communications platform where users are awarded voting tokens if they are registered to vote. This also augments communication to voters for legislative staffers.
15. **Known:** Kevin Marks
URL: <http://withknown.com>
Known is a simple, social publishing platform platform for your blog or website. It's open source and built on indieweb principles. See how it can simplify your posting.

IIWXX #20 Photos by Doc & John H.

Links to Doc's Fabulous Photos of IIWXX

Doc Day 1: <https://www.flickr.com/photos/docsearls/sets/72157652485301058/>

Doc Day 2: <https://www.flickr.com/photos/docsearls/sets/72157652828060746/>

Doc Day 3: <https://www.flickr.com/photos/docsearls/sets/72157651673994360/>

Great Photos by John Haggard

<https://plus.google.com/photos/115140003043991343368/albums/6137060682502702641?authkey=CNOSqrz7-KqWzwE>

Book of Proceedings Photos taken and provided by:

Doc Searls, John Haggard, Maciej Machulak and Heidi Nobantu Saul



"IIW is a melting pot out of which emerge ideas to change the world."

William Heath
Chairman Mydex CI



See you October 27, 28, 29 2015

for
IIWXXI

The 21st Internet Identity Workshop

www.InternetIdentityWorkshop.com

Register Here!