IIWXIX INTERNET IDENTITY WORKSHOP 19

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_19_Notes

October 28 - 30, 2014
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 – the Internet Identity Workshop

The Internet Identity Workshop (IIW) was founded in the fall of 2005 by Phil Windley, Doc Searls and Kaliya Hamlin. IIW is a working group of Identity Commons. It has been a leading space of innovation and collaboration amongst the diverse community working on user-centric identity. The event is now in its 10th year and is Co-produced by Kaliya Hamlin, Phil Windley and Heidi Nobantu Saul.

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.

For additional information about IIW: http://www.internetidentityworkshop.com

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

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/

IW #20 will be April 7-9, 2015 in Mountain View, California at the Computer History Museum. Registration is now open at: https://iiwxx.eventbrite.com

IIW Events would not be possible without the community that gathers or the sponsors that make the gathering feasible. Sponsors of IIW #19 were:

Microsoft ~ Google ~ Gigya ~ Neustar ~ Yubico ~ NetIQ

Nexus ~ OasisID ~ Qredo ~ ForgeRock ~ Mozilla

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:

IIWXX #20 April 7, 8 and 9, 2015
IIWXXI #21 October 27, 28 and 29, 2015

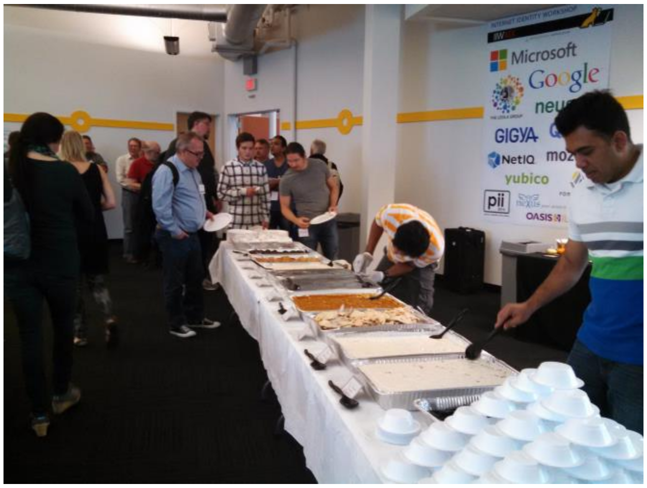
"IIW is the mecca for identity and privacy innovation. It's beneficial for newbies and it's an essential collaboration forum for the stalwart pundits who nurtured this emerging field."

Mike Schwartz
CEO Gluu

At IIW ...

For the second time the San Francisco Giants win the World Series during the Conference Dinner on Wednesday evening

Thursday means Indian Food for lunch



At #IIW Unicorn Hats are not simply tolerated, but welcome!

IIW 19 Session Topics

Tuesday October 28, 2014

Session 1

- Notifs …. a new messaging medium – Jim Fenton
- Interoperable Consent Management – Steve Greenberg
- Account Sharing at the IDP (Identity Provider) – William Denniss
- Boarderless Connectivity (Ambient & Ubiquitous) – Bob Frankston
- Surveillance Identity and YOU - Aestetix
- Root Identity – Decentralized ID Tech – Adrian Gropper
- Respect Connect Protocol – Dan Blum
- Identity Verification for People w/o Paper Trail (Open Discussion) – Chris Papazian + Yoz

Session 2

- XDI / Respect Connect 'Person ~ Business Connections' (Demo) - Markus
- Sustainable Net Protection "After Wikipedia Goes Light" – Britt B, Phil W, Sean B. Doc S
- Oauth SPOP Working Session of Document in Working Group Last Call - Hannes
- XDI Graph Editor Demo - Hubert
- Inter-Federation w/Shop: How to Develop Rules for Joining Federations Together – R.Wilton
- Amazon Web Services (AWS) and Open ID Connect (OIDC) – Zihang
- MAFA Mistaking AUTHN for AUTHZ – Alan Karp

Session 3

- XDI / Respect Connect 'Person ~ Business' DEMO! - Markus
- FIDO U2F Security Key – Emerging Standard Respecting Privacy - Stina
- OAuth & Authentication / What can go wrong? Working Session of IETF,Oauth – Hannes, Justin
- Identities of Dead People – Sarah Allen
- Google "TAPPS" for Education – Kris Alman
- Investing and Crowd Funding VRM – Nathan & Kevin

Session 4

- For the Greater Good ~ 'You are not a Special Snowflake' – Justin R
- Internet of Things (IoT) Door Lock Use Case – Hannes
- SCIM V2 – Phil Hunt
- Online Trackers and Advertisers That Use Them – Hyon Lee
- Model Thinking: A framework for VRM – Nitin Bedjatia
- Building RS ~ AS Trust With UMA – Maciej Machulak & Eve Maler
- Travel to….. CYNJA SPACE – Heather, Chase, Les

Session 5

- Freedom Box "Danube Edition" - Markus
- NAPPS Working Session – John B
- Trust on Both Sides + LOA's Vectors of Trust &Consumer Protection – David Kelts, Paul Grassi
- Ours or Theirs : A discussion of SSL Trust stories in Identity Protocols - Matt
- VRM + CRM: next steps – Doc S
- Use Managed Access (UMA) … Authorization for Internet of Things (IoT) /IoT & Identity -

Wednesday October 29, 2014

Session 1

- OAuth Work Group Status Check - Hannes
- How Do We Engage and Protect Kids In Cyperstace? – Heather, Chase, Les
- Health Relationship Trust – Eve Maler & Deb Bucci
- User Consent + Consent Management + STATS + Demo and Discussion – David Simonsen
- Firefox Social API: 2 years in, what next? – Christopher Arnold

Session 2

- SCIM API Extensions: Who wants to add what? Interests? - Bjorn
- The VRM Social Network – Drummond Reed
- Mozilla Subscribe 2 WEB – J.B.
- Gold Identity Federation – Roger Billings

Session 3

- User Asserted Terms for VRM – Mary Hodder
- Personal Data Ecosystem Consortium (PDEC) Exploring the Future with Dean Landsman
- OAuth Challenge Grant? – Samual E (Nexus)
- NSA Surveillance in Austria - Markus
- Build a New Saas app With Enterprise Identities: What would you do? – Patrick Radtke
- FEM vote. US The RE-Founding Sisters – Real Representation in Virtual Districts – Britt Blaser
- The State of Anonymous Credentials (discussion) – Andrew Dawes

Session 4

- Open UMA Implementors' meeting - - interop, feature tests…. – Eve Maler
- Mobile Darwinism: From mobile to mobility – Michael Becker
- VRM + CRM Part2 The VRM Strikes Back - Nitin
- Amazon Web Services (AWS) and Identity Management: What's New? – Shon Sham
- Conflict Resolution in Community - Kaliya
- Field Trip: Musuem Demo of IBM 1401 - Oscar

Session 5

- Continuation of open UMA Implementers' Meeting – Even Maler
- Mozilla Listens to IIW – Sean Bohan
- Threat Based Authentication: Understanding the Risks of RBA – David Waite
- IoT Modeling with Picos: "Lessons From Fuse" – Phil Windley
- Trusting "Trust Frameworks" What needs to regular people have to make this "real?" - Kaliya

Thursday October 30, 2014

Session 1

- UMA Demo - Maciej
- Micro Services Containers, Reactive Manifesto and…. Identity – Dave Danford
- OpenID Connect: Easier than you probably think it is – Justin R
- What Is A Federation? – David Simonsen
- Firefox Interest Dashboard – Kevin Ghim

Session 2

- ARM mbed/IoT - Hannes
- Notifs – (Repeat) – Jim Fenton
- Vectors of Turst ---- Continued – Rainer H, Colin W.
- The VRM Social Network Part II – Drummond R & Doc S
- QREDO Rendezvous Protocol – Hugh Pyle
- Introduction to the Indie Web – Ben Werdmuller

Session 3

- Twitter in 2015: What do you want to see us do visavis account security , recovery, identity & privacy – Mollie Vandor
- FIDO U2F Security Key Explained - Stina
- The REAL Internet of Things + IoT – Doc Searls & Bob Frankston
- Access Token with Access Control List for IoT – Erik Wahlstrom

Session 4

- OAuth 2 Scope Design Discussion – Ajanta & Eve
- VRM + CRM Part 3 - Nitin
- Anchors of Idenity & Account Recovery /Round Table Discussion – Bill Mills

Session 5

- NAPPS Working Session Part 4 -
- Online Voting: What do we need to have happen in “identity” before online voting happens? – Andrew Jennings
- CRM + VRM Branding for Consumers and Developers – Micah Mc
- Mozilla + VRM/Intersecting 2015 – Sean Bohan
- Bob’s Kabitzing Tour of the Museum

Tuesday October 28

Nõtifs

Tuesday 1B
Convener: Jim Fenton
Notes-taker(s): David Waite

Tags for the session - technology discussed/ideas considered:

Pseudonymous secure opt-in notifications

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

Point: Non-human-consumable items (like addresses) have a tendency to become targeted towards humans. See URLs, vanity license plates

Question on messages targeting multiple roles for people represented differently to individuals; if the notification is just content, eventually the different representations will be targeted toward different people

Question: for Notification agents, is there an opening toward cloud and ad-supported provider for notifications, vs running your own. Big players have advantages in email with things like spam control; notification agents should be on a more level playing field

Message format: may have additional tags, formatting, etc. for the body in the future

Suggestion: Consider/look at JOSE for cryptographic functions - presenter has not considered yet because of existing DKIM background.

There was an agreement that excluding values from signatures would optimize some cases of broadcasting a fixed message to a large # of people without requiring resigning per message

Observation from the view of one armed with the OAuth hammer: webfinger lookup for user notification service; oauth authorization for adding notification

Push to SMS as a feature for less capable user agents? Already envisioned using a service like Twilio

Clarification: Signature is verified by notification agent, not exposed to end user. There is a certain amount of trust by the user to their notification agent.

Additional point: On submission, a notification agent gives an identifier to the submitted notification, so that agents can expose a way update or best effort delete notifications

Users can delete notifications, although bit under-defined. System specifically ignores user actions for notifications (view, deleted)

Privacy protection: notifier does not know user, just uuid. Notification Agent has access to messages for a particular user, but you have the option to choose one/many agents or run one yourself.

Interoperable Consent Management

Tuesday 1C
Convener: Steve Greenberg
Notes-taker(s): Eve Maler

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

Interesting efforts going on:

Authentication and Authorization in Constrained Environments (ACE): IETF working group
XDI Link Constraints: OASIS technical committee
User-Managed Access (UMA): Kantara work group
KRL: technology platform from Phil Windley
OAuth: IETF standard/working group
Open Mustard Seed: effort
ID Data Web: company
Where Are You From (WAYF): federation
Consent Receipt: draft spec from Kantara Consent and Information Sharing work group
Identity Broker: product from UnboundID
Open Digital Rights Language (ODRL): W3C standard
Health Level 7 (HL7): health standard
SBVL: standard business (something) language?
Extensible Access Control Markup Language (XACML): OASIS standard/technical committee
Platform for Privacy Preferences (P3P): (failed) W3C standard
Capabilities: security concept that is an alternative to access control

What's needed: common semantics and useful translations around: 1) identity, 2) data, 3) permissions, and 4) transactions.

Some themes to consider:

- Consent versioning
- Alice-to-Alice (app-to-app) vs. Alice-to-other-party
- Synchronous (during access attempt) vs. asynchronous (before access attempt and after access attempt)

Account Sharing at the IDP

Tuesday 1D
Convener: William Denniss
Notes-taker(s): William Denniss

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

It is a fact today that many people share accounts, particularly within their own household (family, housemates, etc). They do so for convenience, to share streaming content, for paying shared bills, and other reasons. Today people typically achieve this by sharing their username and passwords.

Identity Providers (IDPs) are trying to move people away from the username and password model and towards federated sign-in. Should IDPs support the account sharing use-case by allowing multiple people to login to one Relying Party (RP) through a single IDP->RP identity relationship?

Session Notes

The session was an open discussion with many interesting points raised by the participants, including:

- If IDPs don't explicitly support account sharing, people will continue to share their accounts anyway. Sharing either their full IDP credentials, or continuing with username/password at the RP as they are today.
- IDPs need to offer the same value as username/password in regards to sharing
- Some concern that IDPs enabling sharing would be "changing the deal" for RPs
- Most media sites already have clearly defined rules around sharing, that are unrelated to the number of people signed in to a single account (e.g. Spotify: 1 stream at a time, Netflix 2 streams at a time). If sites that care about multiple users already implement rules to control sharing, changes at the IDP layer may not impact them greatly.
- While the best approach would be for RPs to all implement their own sharing mechanisms, most sites don't seem to care
- Strong support for an idea to declare that a user is being impersonated by adding an extra claim to the ID token, allowing RPs to optionally take action on it.
- By declaring that the user is being impersonated, all RPs by default will get sharing support, but those who don't want it can opt-out by detecting this claim.
- Discussion about whether the id token should declare the user being impersonated, or the user doing the impersonation as the 'sub', but most people settled on the former to achieve sharing with zero-implementation by the RP
- Discussion on whether the impersonation field should contain the user's own sub, a directed identifier, or no identifier at all
- With a valid identifier of the user doing the impersonation, RPs could use the impersonation claim to do other interesting things, like recommendation tracking

(e.g. Netflix recommendations) which could be revenue positive. This could help sell the feature to RPs

- There are added security benefits of this approach too – by knowing the actual human-user, you can build a better security profile (multi-city access by two people sharing an account looks less suspicious)
- Participants noted several cases of username/password sharing even within the sensitive medical medical context, for example a nurse that logs in as the doctor to add notes. This proposal is not trying to address that use-case however.
- Impersonation at the IDP layer doesn't solve use-cases needing granular Access Control Lists (ACLs), although if the id token does contain the user doing the impersonation, RPs could log an audit trail that includes the actual user, which is still a large improvement over the username/password sharing that happens today.

Follow Up

- William to continue the discussion with interested parties, and to consider drafting and extension to JWT for subject impersonation claims.

Borderless Connectivity (Ambient & Ubiquitous)

Tuesday 1F
Convener: Bob Frankston
Notes-taker(s): Bob Frankston

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

Link to Blog Post: http://frankston.com/public/?n=beyondneutrality

Surveillance, Identity, and You

Tuesday IG
Convener: Aestetix
Notes-taker(s): Kris Alman

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

Local level efforts to address issues of surveillance

Domain awareness Center (oaklandwiki.org <http://oaklandwiki.org>) in Oakland; central headquarters of camera data; no notes without reasonable suspicion; good policy with constraints yet demonstrating continued crime reduction (drugs, homicides); City of Oakland continues to want to get money from DHS…

2009 DHS went to Oakland for surveillance center (which is bigger center than SFO); city of Oakland in addition to port of Oakland. Who gets access to recordings? Ad hoc privacy committee created for writing a privacy policy. Potential this can serve as model public policy.

Scope and purpose: emergencies. Recognition that the scope will likely expand. The city of Austin is working on something similar. NYC and Boston have identital policies. Vidsys contracted to do surveillance; set up feeds

Binney's thin thread a model.

Surveillance: Commercial tracking vs governmental tracking; but government is using back door to data (e.g. google clouds overseas) 18 USC1030-CFA2703d

Different democratic process for the two; corporate surveillance is "optin"; labeling is helpful for latter; EFF sends updates to privacy changes; the Acxioms and Facebooks can't be reined in; difference between data collection and data shared;

Identity: User profile

You: Issues of transparency

Recommended policies: Ad hoc citizens committee with privacy officer to be appointed and whistleblower ordinance that allows it to be ok (so far only one person that can get information); references to fair information practices; requirements for audit;

Data (video stream) v information (a bookmark): both can be seen as metadata

Q as to how federal laws take precedence; data sharing policies come into; question of data ownership; only data have jurisdiction of is the bookmarks; videos not stored by city; data retention records act for CA.

2 years for Port of Oakland. No facial recognition. An officer is monitoring. Can remediate if feel wrongly identified—which means you only hear that you are recorded when there is a lawsuit.

Root Identity – Decentralized ID Tech

Tuesday 1H
Convener: Adrian Gropper
Notes-taker(s): Bill Mills

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

Discussion around what a unified identity should look like so a user can own and manage their identity in a unified way and managing whether linkages are visible or not and how that might be managed. Also the discussion of how to make an identity system independent of any single entity so no single agent has control of identity for a user.

- round table intros
- Adrian's intro

- A person (has/should have) a root identity
    - various personas can be attached: FB, twitter handle, etc.
    - should be decentralized
    - what does authentication of the root identity look like?
        - Adrian asserts that biometrics is key here.

Discussion around what "decentralized" means, similarly "ownership"

Authentication and identities. The idea of independent certifying entities. Trusted entities to do certification.

Example of Apple Pay that allows payment that enables payment but gives the payee no info about the person, and the RiteAid/CVS competitor which grants tons of info about the payee. These are interesting qualities to compare.

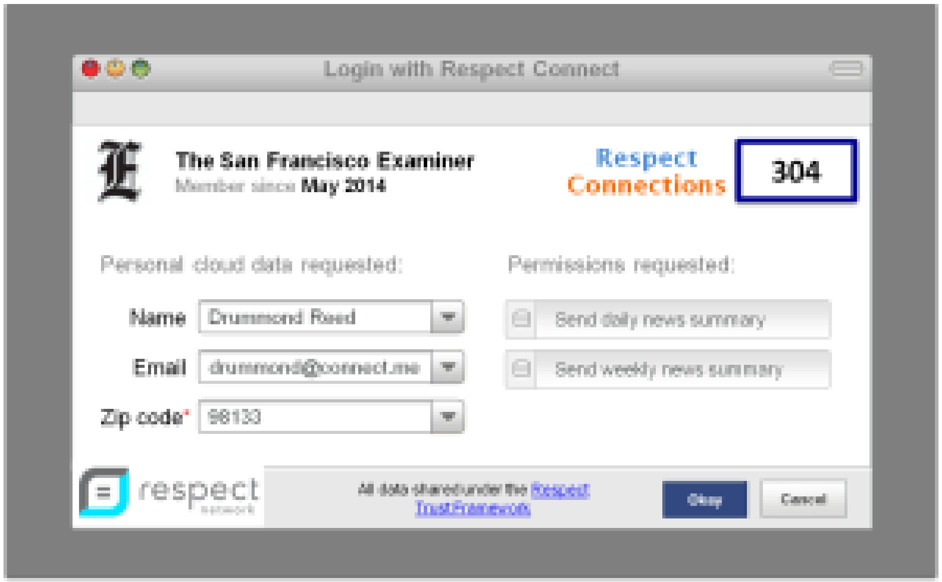
Analogies to SSL/TLS root CAs if one authenticator or entity is "certifying" identities.

Respect Connect Protocol

Tuesday1J
Convener: Dan Blum
Notes-taker(s): Dan Blum

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

We walked through Respect Connect, which is the protocol for establishing connections between peer personal, or business clouds, on the Respect Network.
More info here: https://www.respectnetwork.com



Login with Respect Connect

The San Francisco Examiner
Member since May 2014

Respect Connections 304

Personal cloud data requested:

Name: Drummond Reed
Email: drummond@connect.me
Zip code*: 98133

Permissions requested:

□ Send daily news summary
□ Send weekly news summary

All data shared under the Respect Trust Framework

How Do We Authenticate w/o A Paper Trail?

Tuesday 1K
Convener: Chris Papazian, Yoz
Notes-taker(s): Sarah Allen & Matt Berry

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

Many systems are built around challenge questions that rely on information about buying a house, having multiple permanent addresses, etc. There are people who don't have that history. How do we verify them?
How do you do identity verification for new immigrants or other people without financial history?

UK Government — gov.uk working on an online identity verification system, historical the UK government

Texas allows 6 forms of identification to get a voter ID card; however, people who are new to this country may have none of them

In the US, we typically assume that people have:

a single, exact birth date

name that conforms to first name & last name

Use cases:

take an online persona and match them to a real-world identity

Consider alternate real-world authentication?

such as: real-life in-person verification

Is it ok if one person creates multiple accounts? for buying a house, sure. For a gun registry, that would be a problem.

Lexus-Nexus search:

- banks use this to verify identity

- was fully breached and all of the data was taken — all that data is now in the wild

Another use case IDP (Identity Provider)

want to know that I'm taking to the same person that created the account — biometrics are perfect for this, since you can't lose that like a password

I don't actually need to know your true identity “abidingness” is more important than identity, it’s tough to be anonymous and non-ephemeral

not we require another channel in addition to a password (email or cell phone)

Social scoring

calculations: 200 friends, had the account for 10 years, some score that its a legitimate identity

Voting needs to be anonymous, but also secure and provable

in Arizona you can look up voter record by voter ID or driver’s license

Levels of Establishing Trustworthy Accounts

Self-attested (enter your own data)

KBA - knowledge based authentication

Social Scoring or Account Consolidation (Klout, TrustCloud, LendDo, length of time? # friends?)

External Validation (miCard, or verification of deposit in an account - prove you have that acct)

Sponsored Member or Employee Accounts

Identity Proofing to get an Account (show up in person with evidence of paper trail)

it’s like the problem where spam email is more email than real email

there was an idea about “proof of work” — where you would have to do something computationally intensive to send an email

the levels about are identity verification is based on proof-of work

could create a distributed system where local governments verify that someone is a real per on

Could we have some organization that is non-profit and trusted by the people? you go there and they take your fingerprint and they give you a cryptographic ID that you can use, they don’t reveal your fingerprint. That org could verify that the IDs were unique.

new crypto algorithm LRSW - person sets up their identity, then organizations verify something about that identity

Pseudonym Systems, Lysyanskaya, Rivest, Sahai, Wolf, MIT LCS paper

Oakland and NY, EBT cards (cash cards) incent someone to retain one identity

16,000 years of human interactions, if I was a shopkeeper, I know whether to trust someone because I recognize them and pattern of interactions — certain pattern of speech, look a certain way

BC government has done a lot of work on these issues. Population that loses their ID cards. Biometrics is a photograph. They have a chip-enabled ID card. Chip is a random number. If you lose it then it gets turned off. Thought through use cases for marginalized populations. A unique identifier for each system — linked to an individual identity.

polymorphic identification — one card, diff IDs for diff systems

Can you assert the unique ID? (or do you care who this person actually is)

Can you recover the ID? (how important is persistence?)

Can you rotate your credential?

Can you have privacy through pari-wise identifiers?

New York City did a trial where people had to check into a homeless shelter.

They goal was to study the length of the average stay. (3 days, only 5% chronically return)

You need someone to vouch for the people who no one will vouch for — you need a social organization or government organization.

Concept of vouching

I know someone who is ok, so I am ok

People vouching for people. Could work for undocumented people. Immigrants or homeless.

Could there be an internet-equivalent of a notary?

We don't need a situation where people trust the government? Instead the government needs to know that it can trust a particular person. However, this is a very narrow sense of trust — have you received these benefits before? Are you a veteran?

There are ways to imagine this being solved by personal cloud. Your personal cloud knows your birthday and will tell the store you are over 21 so you can buy alcohol, without revealing my birthday.

The block chain (like bitcoin), append only, distributed, encrypted.

When I am born, that fact is logged and encrypted and I'm the only one who can de-crypt it. I can give select people a secret decoder ring to decrypt that piece of personal data and they could verify it.

Matt Berry
This session was hosted by a company that was shopping for an IDP. The primary trait they were seeking from the IDP is strong “meatspace” identity verification; however they also had a target audience of people who traditionally don’t have paperwork such as driver’s licenses, voting records, or birth certificates. Traditional meatspace identity verification has been heavily rooted in government documentation, but populations such as the homeless, the mentally unstable, refugees, and non-legal immigrants often don’t have these sorts of government records to identify them. There was mention of a number of government programs that deal with these sorts of populations already. The British Columbian Government was mentioned as having a universal ID card based on biometrics. The City of Oakland, CA Government had an EBT card program based on visual comparison of photographs (in this program, the end-users had to remember their names in order to find the photograph).

This invoked a discussion about different means of doing identity verification; both in meatspace and in virtual spaces. The American CIA, as an example, conducts a long interview process where identity is established by gathering evidence of identity over the course of a lifetime. Consumer background checks determine identity by gather artifacts of past loans and credits. Social networks were brought up as a more pragmatic (and faster) means of establishing a virtual identity. The theory is that the more content and the longer someone has held on to a virtual identity, the more trustworthy it is. This is similar to the proof-of-work system of spam email prevention.

Someone asked if the system being built by the session hosts could tolerate duplicate virtual identities for the same meatspace identity. Many systems can tolerate duplicate identities, on the condition that the system can still assert that the same identity is logging in this time as last time. An example of this is any system that allows a user to save the state of their application and then return later to complete it. Other systems, such as online voting systems, cannot tolerate duplicates.

XDI/Respect Connect Person < -- > Business Connections Demo

Tuesday 2A
Convener: Marcus Sabadello
Notes-taker(s): Marcus Sabadello

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

We showed a demo of a "Newspaper" website and a "Pizza" website.

In both demos, there is a "Respect Connect" button on the webpage. When the user clicks on the button, an authentication and authorization flow is initiated in which the user interacts with their personal cloud. They can accept or reject a "connection request" which was in the button.

If they accept, an XDI link contract is created in their personal cloud, and the website can subsequently access the personal data it had requested.

The website is called a "Requesting Authority". The user is called an "Authorizing Authority".

OAuth SPOP Working Session of Document in Working Group Last Call

Tuesday 2C
Convener: Hannes
Notes-taker(s): Hannes

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

Nat gave a status update of the recently submitted SPOP document (see http://tools.ietf.org/html/draft-ietf-oauth-spop-02). Nat presented some slides that explains the problem and the currently described solution problem: http://www.tschofenig.priv.at/iiw/2014/Hannes SPOP.pptx

Based on the feedback several clarifications will have to be made to the document. A few participants volunteered to review the document, which is currently in Working Group Last Call.

XDI GraphEditor Demo

Tuesday 2D
Convener: Hubert
Notes-taker(s): Sarah Allen

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

XDI-GraphEditor
eXternal Data Interchange http://neustar.github.io/xdi-grapheditor/

XDI is semantic graphs at its core - use it to represent organizations, peoples, things, document attributes and relationships between nodes

a problem that the XDI community had was how to explain this and illustrate it, as well as editing

based on D3, open source,
- pure javascript and D3
- XDI2 Javascript library
can import and export XDI or create/edit interactively

Q: this could be a means to generating a cloud card very quickly? taking information from the graph and serve it up in a visual way — maybe in the future

Right now it is a tool, but in the future it could be used in UIs for graphs
can control visual attributes of the graph with sliders

sample XDI: =alice/#friend/=bob

This is really a teaching tool for XDI
demonstrated alice having an email address
every node in XDI is addressable, and attributes are nodes

Hubert is on the technical committee for the protocol, working on simplifying the protocol
Initially, this was simply a way to understand the protocol through visualizing it
Can switch to a tree layout, instead of a force layout
Nodes can be collapsed and expanded
Zoom in / out
can drag nodes out of the way
will highlight errors — which parts of the statement are wrong

Tableau — gives knowledge workers insight into the data, over time this may get to the point where people can see relationships
Wish list: - focus on a node and only show connections to the node

How to develop rules for Inter-federation

Tuesday 2E
Convener: Robin Wilton
Notes-taker(s): Robin Wilton

Tags for the session - technology discussed/ideas considered:

Federation, inter-federation, interoperability, eID, governance, rules in

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

This session gave a summary of the "defining/developing rules" topic from the Internet Society's Sept 2014 workshop on Inter-federation.

A slide deck is available which summarizes the discussion: RW-Rules-for-Interfed.pdf

Link to Slide Deck:

Amazon Web Services (AWS) and Open ID Connect ~ Q&A

Tuesday 2F
Convener: Zihang
Notes-taker(s): Matt Berry

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

Question: How does AWS discover IDPs?
Answer: The user enters the Issuer URL and we use the Open ID Connect Discovery Profile (without the WebFinger component, as the end user has given us the Issuer URL).

Question: How does AWS translate from an OIDC Principal to and AWS permission set?
Answer: Let's do a quick recap of AWS Authentication and Authorization before we answer this.

Recap: AWS vends long-term Access Key and Secret Keys to users in the AWS system (IAM Users). These long term credentials are used to authenticate requests, and permission sets are attached to the IAM Users. It is not wise to use these credentials in deployed applications however, as the application can be reverse engineered to extract the credentials. Instead, use short-term Session credentials that expire after 1 hour. IAM Roles are used as the principal for these sessions. The identities for the sessions themselves are ephemeral, but they link back to the permission set of the IAM Role. The IAM Role dictates who can 'assume' the role, i.e. obtain a set of session credentials. So in the case of SAML or OIDC, the IAM Role 'trusts' an OIDC provider. Using STS.AssumeRoleWithWebIdentity, an ID Token can be exchanged for a set of Session credentials for an IAM Role.

Answer (post recap): AWS translates OIDC Principals into IAM Roles, and uses the permissions associated with the Role

Question: Can the OIDC Identity Provider pass attributes/claims through to AWS' Authorization language?
Answer: We pump select attributes/claims through for both SAML and OIDC, however the list is much shorter for OIDC as there is no commonly accepted list of standard claims. We have considered making our implementation extensible to support custom attributes/claims and we are still researching cost/benefit tradeoff.

Question: How temporary are temporary credentials?
Answer: minimum of 15 minutes, maximum of 1 hour. Before the hour is up, an application can request new credentials, but a new ID Token is required for security purposes. This should be mostly transparent to end-users because the IDP will maintain a session for the user.

Question: How does AWS handle multi-tenant IDPs?
Answer: Depends on the flavor of multi-tenancy. Salesforce, for example, has a single identity pool and different users can log in to different salesforce applications. In this case, your IAM Role will need to check the client ID of the application to effectively limit the pool of users down to those valid for a particular salesforce application. For multi-tenant IDPs where each tenant gets its own issuer string, there are no special considerations, as AWS sees them as different IDPs.

MAFA Mistaking AUTHN for AUTHZ

Tuesday 2H
Convener: Alan Karp
Notes-taker(s): Alan Karp

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

We discussed a simple mistake that should never happen. However, it happens often enough to have been named, Mistaking Authentication for Authorization. It showed up in the non-normative material in the UMA spec, and has been found in several popular password managers. The question is; why does this simple error get through security reviews?

To illustrate the problem, consider a rental car reservation. Somewhere under the covers of the UI, some code says

```
confNo = carCompany.book(bookingData)
```

and the UI shows

```
Confirmation Number: 8376BA
```

When you want to upgrade to a fullsize car, the user fills in a form specifying the confirmation number and the new car size,

```
Confirmation Number: 8276BA        Car Size:  Full
```

Under the convers there is code something like

```
carCompany.changeCar(“8276BA”,”full”)
```

The error occurs when the system checks the user’s authentication to verify permission to invoke the changeCar method but does not check to see if the user has permission for the specified confirmation number. Notice, the typo in the confirmation number. The result is that the wrong reservation gets changed. See, I said it was a silly error.

Although most of the few attendees at this session disagree, I believe the error happens because the confirmation number designates a protected resource, but it looks like pure data, which makes it easier to miss the access check.

For other reasons, I have been proposing that we treat resources, such as the car reservation, the same way we treat services, such as carCompany. That way the relevant code becomes

```
confSR = carCompany.book(bookingData)
confSR.changeCar(“full”)
```

Because we see a method being invoked on confSR, we are more likely to recognize that it is a protected resource and needs an access check.

XDI/Respect Connect Person <--> Person Connections DEMO

Tuesday 3A
Convener: Markus Sabadello
Notes-taker(s): Markus Sabadello

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

This is similar to the previous XDI/Respect Connect demo session, but between individuals.

An individual "Markus" uses a web browser to open a cloud card published by another individual "André". That cloud card contains some of André's public attributes, and it also contains a "Respect Connect" button.

If Markus wants to see André's private attributes, he has to click on the button, which triggers a flow that sends a "connection request" from Markus to André. Assuming André approves the request, he will create an XDI link contract in his personal cloud which allows Markus to view the private attributes of the cloud card.

FIDO U2F Security Key – Emerging Standard Respecting Privacy

Tuesday3B
Convener: Stina,
Notes-taker(s): John Haggard

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

Link to presentation:

https://www.dropbox.com/s/fwwglpx8ralxgvs/FIDO%20U2F%20Security%20Key%20by%20Yubico%20(IIW).ppt?dl=0

OAuth & Authentication

Tuesday 3C
Convener: Hannes & Justin R
Notes-taker(s): Hannes & Matt Berry

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

Justin presented the write-up about OAuth & Authentication that was sent to the IETF OAuth mailing list, see http://www.ietf.org/mail-archive/web/oauth/current/msg13708.html

The meeting lead to good feedback that will have to be incorporated and several persons volunteered to do another review.

Matt Berry ~ OAuth 2 is more of an auth framework than a complete auth stack. A result of that is that many RPs implement what they think is a secure OAuth stack, but what is in fact not secured. The reason is often due to one of a small number of common pitfalls that the OAuth Working Group is hoping to solidify in a blog post. One major point is that OAuth is not an authentication protocol. As Justin put it “it is the difference between chocolate and fudge. You need chocolate to make fudge, but one is not the other”.

A pre-publish copy of the blog post is available at Justin's Github repo. Justin is appealing for copy editors before the post is sent to the website to be published. The key items on the "don't do this list" are:

1. Using possession of an authorization token as proof of authentication (it's not)
2. Using an OAuth protected identity endpoint as proof of authentication (it's not)
3. Accepting access tokens from places other than the authorization server (don't do this)
4. Accepting access tokens that lack audience restrictions (could be hijacked)
5. Spoofing of user info endpoint as a means of injecting user information (a la #2)

The point #4 is an interesting one because OAuth lacks a means to convey that information. Two options are to have a token identity endpoint where the audience is returned, another is to introduce a second token into OAuth (at this point, just use OIDC).

Identities of Dead People

Tuesday 3D
Convener: Sarah Allen
Notes-taker(s): Sarah Allen

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

Link to presentation:
http://www.slideshare.net/sarah.allen/identities-of-dead-people

Google "TAP"PS for Education

Tuesday 3G
Convener: Kris Alman
Notes-taker(s): Kris Alman

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

Google apps for education lawsuit: Google violated federal and state wiretap laws by intercepting electronic Gmail messages and data-mining those messages for advertising-related purposes, including the building of "surreptitious user profiles."
http://www.edweek.org/ew/articles/2014/03/13/26google.h33.html?cmp=ENL-EU-NEWS2

Student Privacy Matters "Restoring Privacy in the Era of Big Data":
http://www.studentprivacymatters.org/?p=289
Rationale for data collection good: data-driven decision-making; improve quality; decrease costs

But is data being used appropriately? Is it being repurposed? Shared inappropriately? How would we ever know? Do risks of profiling in health and education increase when businesses gain access to data? Do certain businesses have conflicts of interest? If so, how should their scope be limited?

- Business associate agreements with "covered entities" in health care
    - All Payer Claims database vendors: include defense industry (General Dynamics) and big health care data aggregators (Milliman*, OptumInsight, Truven) http://www.apcdcouncil.org/vendors

- Businesses as "school officials"
    - inBloom

    - Google Apps expanded services include Classroom, which is linked to student information system https://www.edsurge.com/n/2014-10-14-google-launches-five-improvements-to-classroom-tool

    - Pearson cloud-based scoring for clinical tests

FTC complaint for "pharmacy risk scores" http://www.ftc.gov/enforcement/cases-proceedings/062-3189/milliman-inc-matter; http://www.washingtonpost.com/wp-dyn/content/article/2008/08/03/AR2008080302077.html

The Gates Agenda: philanthropy to numerous nonprofits, including Data Quality Campaign http://www.dataqualitycampaign.org/

Commercial and governmental surveillance easier with changes in HIPAA and FERPA law since 9/11.

Data mandates: disastrous student information system in LAUSD; huge errors that could impede graduation for 38,000 students, costing $15,000 to $25,000/day to fix. http://www.latimes.com/local/education/la-me-lausd-student-data-20141028-story.html

Health and education sectors are outsourcing work to businesses that make money from advertising; it's cheaper and more secure; higher ed. perspective of students is share more… though they may feel differently in the future.

Further, there are still hacking risks; in health care, the largest data breaches are by business associates; recent breach of 4.5 million records at Community Health System's for-profit hospital chain.
HHS Office of Civil Rights has database of breaches >500.
http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/breachtool.html

No easy solutions with data mandates, costs and security v privacy

For the 'Greater Good' ~ 'There are no Special Snowflakes'

Tuesday 4A
Convener: Justin Richer
Notes-taker(s): Matt Berry

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

I arrived a bit late to this discussion.
The discussion focused around the topic of "do we allow massively distributed algorithms to control aspects of our life. Assuming we allow this, do we allow them to optimize for the general case at the expense of some individuals".

The scenario that was presented was a futuristic world where cars drive themselves via a distributed algorithm. The question that was asked was "do we allow the algorithm to make you 3 hours late to work once a month so that the majority of people can be 10 minutes early?".

There were lots of tangents and talking past one another, but there were some statements that stuck. Specifically, that Technology changes Society, Society reacts to aversions causing Government to act, Government impose laws upon the Technology.

Technology -> changes -> Society -> reacts -> Government -> laws -> Technology

An example is the recent Facebook experiment where a distributed algorithm plighted some users while delighting others. The technology changed, causing society to react.

There are no laws around this sort of behavior, but such laws are now being drafted.
Another major point was about the detection of such anomalies and who is responsible for addressing them. How do we detect localized issues in a distributed algorithm, and who is responsible for owning that infrastructure. Once a localized issue is detected, who complains about it and to whom?

Some of these questions have been actualized today, for example when New Jersey Governor Chris Christie closed the George Washington Bridge on his opponent. The detection of the traffic anomaly was immediate and widespread, however we won't know the response until after the elections. Transparency into this process is also a must.

Finally, someone raised a point that none of these problems exist in isolation. Often the localized issues are not a problem because, for example, not driving means you can now work-from-car ©®™. Non-individualistic societies also would have drastically different reactions than many western societies.

Internet of Things (IoT) -- Door Lock Use Case

Tuesday 4B
Convener: Hannes
Notes-taker(s): Hannes

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

Hannes went through one of the use cases from the IETF ACE working group, namely the door lock use case. The following slides were used as a basis for the discussion: http://www.tschofenig.priv.at/iiw/2014/Door-Lock-UseCase.pdf

In addition to the door lock use case there was a brief discussion about the different design patterns used in the IoT environment: http://www.tschofenig.priv.at/iiw/2014/Design-Patterns_HannesTschofenig.pptx

It was clear from the discussion that there will never be an agreement on how even a simple use case should look like and it is probably a useless effort to try to get some agreement on the user experience or the properties it should have.

SCIM V2 Intro

Tuesday 4C
Convener: Phil Hunt
Notes-taker(s): Phil Hunt

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

A brief introduction of SCIM (System for Cross-domain Identity Management) was given and its primary use case.

We went through the major enhancements of SCIM v2 vs. v1 and the current IETF status which is that the specification has now reached working group consensus and is moving forward to standard status.

We had a lot of good discussion on some use cases and how ownership and points of administrative control: e.g. control from the enterprise, vs. a designated cloud service provider, etc.

We had a great discussion on event notification and the general problem with REST services for coordinating identity change events across an eco-system. This sets the stage for the Day 2 SCIM presentations on future work.

Online Trackers and Advertisers That Use Them

Tuesday 4D
Convener: Hyon Lee
Notes-taker(s): Hyon Lee

Tags for the session - technology discussed/ideas considered:

Trackers, Advertisers, ISP, PII, Personally Identifiable Information, Ad Network

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

Discussed what Online Trackers were and how Advertisers use them.
Not much can be done other than completely block information (cannot throttle the amount of information), as the trackers and networks invalidate the entire request if the information is tampered with.

There are talks of ISPs attaching pii to outgoing packets.
VPN/Https might be a way to combat the ISPs.

People are surprisingly open to sharing their information.

The new generation is coming into a world where sharing information is the norm – proper education of the risks may be necessary.

AS<->RS Trust in UMA

Tuesday 4I
Convener: Maciej Machulak and Eve Maler
Notes-taker(s): Eve Maler

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

We reviewed this UMA-related spec module:

http://docs.kantarainitiative.org/uma/draft-oauth-resource-reg.html

...and went through this introductory slide deck:

http://kantarainitiative.org/confluence/download/attachments/17760302/UMA%20101%20at%20IIW.pdf?api=v2

We discussed questions and comments centering on how an authorization server would handle registrations of ten thousand resources for users managed within, say, a corporate system. Currently it would expect each unique resource "owned" by each individual user to be registered separately. This and other patterns could be optimized in various ways in future.

Travel to Cynjaspace

Tuesday 4J
Convener(s): Heather Dahl, Chase Cunningham & Les Chasen
Notetaker: Heather Dahl

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

The Cynja is a universe. Just as training wheels allow kid the freedom to ride a bike, CynjaSpace allows them to train for freedom the adult cyber world.
http://www.thecynja.com/

- We ease kids into the adult world. We have a watershed on TV, we have a kids menu, we have training wheels on bike. There is a demarcation between the world of adults and the world of children.
- But when it comes to technology and the Internet, we just let them navigate the adult world.
- And sometimes they wipe out.
- We know kids fall over.
- And parents are alarmed.
- Look at all of the things that parents need to focus on to protect their kids.
- And this is what we give them. If kids don't like doing homework, why would adults like doing it? And this looks like homework.
- Here's Shirley the dog. I guess she is supposed to make all of this look fun. Shirley we can do better than a dog leaning against bullet points. And we can.
- We help kids and their parents navigate the world of cyberspace in one place.
- It's education combined with security & privacy.
- Kids want to feel empowered. They want to feel confidence. They want to be awesome. The Cynja inspires kids to WANT to be safe. And that's a huge win in any parent's book.

Freedom Box Danube Edition

Tuesday 5A
Convener: Markus Sabadello
Notes-taker(s): Markus Sabadello

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

I demo'd a prototype of a FreedomBox called "Danube Edition", which has a number of functions for a more free, private, and decentralized Internet, e.g.:
Running web applications such as Known (a personal publishing platform), OwnCloud, Mailpile.

The box can provide an "Unhosted remoteStorage" server, and an XDI personal cloud. It can also act as a router and send Internet traffic through Tor or a VPN.

The FreedomBox "Danube Edition" has a programmable light which provides visual feedback when one's personal data is accessed.

More information at http://freedomboxfoundation.org/
And http://projectdanube.org/.

Internet of Things & Identity & UMA

Tuesday 5J
Convener: Joe Andrieu, Eve Maler, Marcelo Da Cruz
Notes-taker(s): Joe Andrieu

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

Nest -- In home, data going to cloud
PlayaLightz -- Wearable social network blinkie
Fuse -- Car data wirelessly sent to personal cloud

Opportunities?
Concerns?
Solutions?

Do you need an identity?
Not technically for isolated control you can do it with an authorization code.... but for all practical purposes, you'll need to share control and/or refer to a device in a conversation, and identity will get attached

Low power RF

```
Devices ->   API  -> Apps
          |          |
```

Where the API is in the cloud, at the service provider. Two boundaries: between on-premise and off, i.e., between the home and the cloud, and between the API provider and cloud apps.

For example, the NEST thermostat connects to the cloud, then the server exposes a restful API to apps

Today there is no way to control Nest locally. It requires access through the cloud. The capability to control locally is uncommon in consumer apps, but is common in the enterprise.

What we need is something, a registry, for apps to be able to reach back into the local resources.

What you want to do is to negotiate the ability to access the resource.

People / Devices / Cloud Services !!!?!?!?!?!?!

Eve Gave an UMA presentation
Constrained environments ...

Connected dishwashers leak data... privacy concern.
So we would like to authorize access...

What about smart medical thingies

And OMG, Solar Freaking' Roadways!!

Requirements:

INSANE SCALE
Discovery

The Refer use case: refrigerated shipping containers: ship needs to discover the container.

What about GPS leakage: walking the dog leaks GPS data about us.

Partitioning

ACE
Authorization in Constrained Environments

Eve: Cannot solve IoT unless you simultaneously solve for both IoT and the Web.

The question is who owns that data, who is responsible, or uses that information. That's what makes is an identity problem.

Who has title?
Who has what kinds of access?

How far can existing technologies meet our needs?

XACML... Extensible Access Control Markup Language...
Scale - no
discovery - no

Privacy - 1/2
Flexible - no
Partitioning - 1/2

OAuth 2.0
Scale - partial
Discovery - partial
Privacy - partial (consent good)
Flexibility - yes
Partitioning - partial

UMA!:

See presentation for more stuff.
http://www.slideshare.net/xmlgrrl/maler-io-t-access-control-iotaconf-2014

UMA is about interoperable RESTful authorization-as-a-service

UMA also allows asynchronous permissioning based on pre-arranged rules, in contrast with OAuth, which is really built for synchornous permissioning when Alice shares with Alice (sharing data between apps as the same individual). But then Alice shares with Bob, synchrony can't be assumed--and Alice isn't the active user on both services...

UMA covers the granting of entitlements (through scopes), asynchronously, because it isn't requiring the grantor to be online at the time of access request.

What's the experience like? Just like "sharing" a doc in Google apps.

Fuse needs to use OAuth to connect their MVNO account to their fuse account. But when that access token expires, how do you reacquire access when the user isn't there to get a popup?

So, if the car is getting towed after that token expires can prevent data tracking.

Healthcare.

Challenge: Imagine these services without the cloud. IoT can be 100% local without service-based identifiers and communications.

Wednesday October 29

OAuth WorkGroup Status Check

Wednesday 1A
Convener: Hannes
Notes-taker(s): Phil Hunt & Matt Berry

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

Hannes listed the current set of documents that are in progress (see http://datatracker.ietf.org/wg/oauth/documents/)

SPOP was discussed yesterday. There was concern about the name

OAuth Token Exchange - works like an assertion swap may be slightly different than the version from Justin.

Phil asked is the problem going away because people are finding other ways. Justin indicates that some are using his draft solution but its not been picked up.

Dyn Reg has had no activity. Hannes will check with Kathleen on the status.

Dyn Reg Mgmt is being published as an experimental draft. Hannes and Justin will do a shepherd write-up. The write-up went to the mailing list here: http://www.ietf.org/mail-archive/web/oauth/current/msg13717.html

The Dyn Reg Meta data document was folded into Dyn Reg and should be dropped. Hannes marked the document dead after the meeting.

Token Introspection - Hans from Ping has been implementing and has been sending comments back to Justin.
Justin gave a brief intro into the use case for dyn reg for the IIW group. In a distributed service the RS often needs to get information about the token.

There is still discussion on scale of polling. Justin suggests using caching with introspection. Phil commented that this seems to go against the scenarios that demand revocation be checked per use. The alternative pattern that can be used is pub/sub to deliver notifications to the resource.

Breno commented that clients are rarely interested in checking validation. Google is looking at both introspection and pub/sub models.

Scotty mentioned one technique is to have the AS issue different lifespan tokens based on risk. A read token might live substantially longer, while a privileged/high-risk scope would be short-lived requiring re-authentication.

Action items: According to Justin there is still some editorial clean up required.

JWT is in IESG eval plus the 3 assertion documents.

Hannes is expecting these documents to be finished in December.

Proof-of-possession documents have not made a lot of progress. The security architecture describes the use cases and requirements.

Hannes showed the POP architecture slides form the Toronto meeting and reviewed the documents. Here are the slides: http://www.tschofenig.priv.at/iiw/2014/IETF-OAuth-PoP.pptx

TLS channel-id is a new spec (resurrected) that can fit as part of the client to resource server pop — the proof is occurring at the transport layer. However this is not a message signature. The concerns are apparently focused on blocking MITM attacks and/or truly application layer security.

Breno mentioned his concern with message signing is there is no expectation of wide inter-operability. There are just too many intermediaries messing with the data. He suggests we focus on protecting the payload.

Breno mentions that a lot of the issue is in the frameworks: what happens between TLS and the actual application code.

Matt Berry
This was a working group meeting discussing the progress of several draft documents; specifically the OAuth Symmetric Proof of Possession (SPOP), OAuth Token Exchange, and OAuth Token Inspection draft documents.

The OAuth Token Inspection draft speaks to situations where the AZ and the API server are not the same system, thus the API server needs a mechanism to determine the liveliness of the access token (supposing the token is a reference instead of being an irrevocable encrypted blob). There was a long discussion of Push vs Pull semantics. Justin (the draft's author) is in favor of a pull mechanism where the API server pulls liveliness information from the AZ. Another gentleman was of the opinion that the AZ should syndicate this information to the API sever, however there was efficiency and scalability concerns with this. Access tokens may be used once and discarded, or never used, thus is makes little sense to syndicate their state to each API server. Both are valid approaches depending what is being optimized for. Justin invited edits to the draft.

The Proof of Possession discussion focused around the interactions between the RS and the client. They can be secured via TLS Channel binding, however that requires touching deeper parts of the stack. The benefit is that web service containers are free to manipulate responses, as the security lives lower down the stack. The downside is that Docker-like systems might not expose the TLS layer so adoption may be poor. Another option would be signing HTTP request headers. The pushback here is that some web service containers will manipulate some headers. A draft is in the works to canonicalize the HTTP request before signing, leaving out potentially problematic headers. This is essentially what AWS' HTTP Request Signature V4 does.

How Do We Protect Kids in Cyberspace?

Wednesday 1B
Convener(s): Heather Dahl, Chase Cunningham & Les Chasen
Note Taker(s): Dahl/Chasen

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

- Safe vs. unsafe search results (ie: golden girls)
- Gamification of search
  - Including analytics for parents
- Usability Gap -> Browsers are hard, apps are easy.
  - Reinvent the browser?
- Get rid of technical aspects of UI's. (ie: printing)
- Apple parent controls are cumbersome
- Use tools to teach, create reports. Create positives.
- Add tags, self learning, natural language, parental collaboration.
- Microsoft Family Safety a good reference.
- Dashboards are important
- Sandbox for kids to play
- Remove abstraction. What is the business of the Internet?
- Some parents don't understand the technology they are teaching their kids.
- Authority->Circles of Trust->Move the trust layer up

HEART Workgroup

Wednesday 1C
Convener: Eve Maler, Deb Bucci
Notes-taker(s): Eve Maler

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

We discussed the formation of the new HEART WG. We didn't project slides, but worked from the following slide deck:
https://www.dropbox.com/s/bmobdubr363h70j/HEART%20charter%202014%2010%2027.pptx?dl=0

We also discussed the FHIR API as a key exemplar of what we're protecting:
http://www.hl7.org/implement/standards/fhir/

Everyone is welcome to join the new group; this page is a placeholder:
http://openid.net/wg/heart/

To take part, you will need to fill out this IP form:
http://openid.net/ipr/OpenID_IPR_Policy_(Final_Clean_20071221).pdf
or
https://www.docusign.net/Member/PowerFormSigning.aspx?PowerFormId=2318fff5-f8d3-4ba8-801b-0080a6805199

We are lining up membership in the next few weeks and will be meeting formally in teleconferences in the new year, if not sooner. We plan to hold a F2F meeting at the HIMSS conference in April 2015 in Chicago:

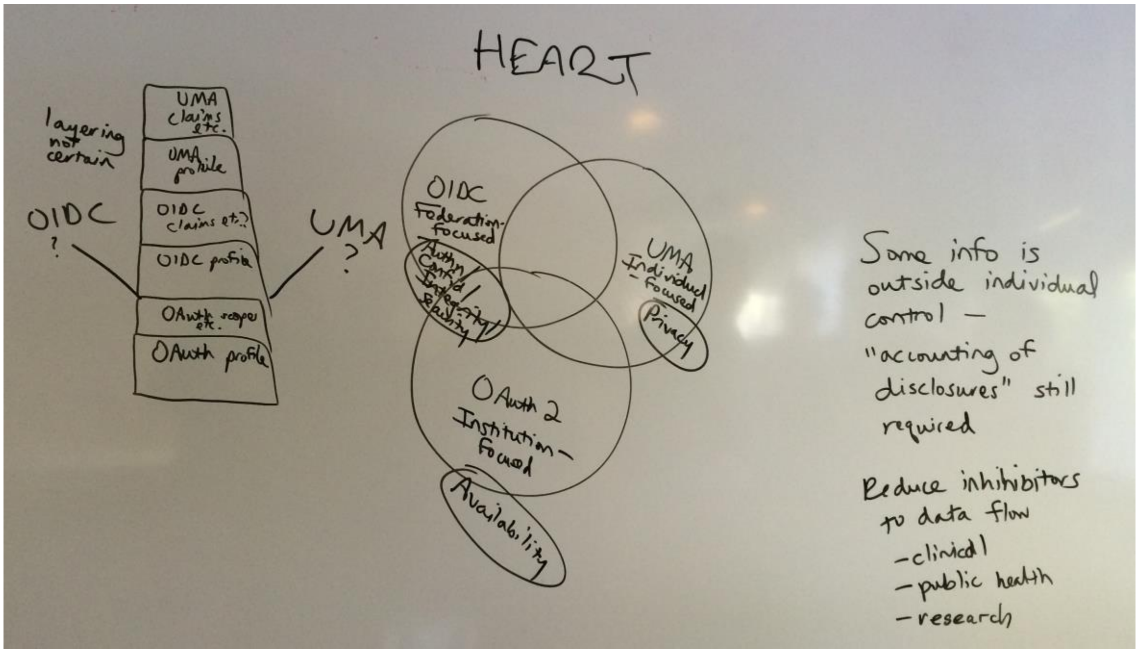
http://www.himssconference.org
The Venn diagram below is an extension of a set of slide deck notes that can be found here:
http://kantarainitiative.org/confluence/download/attachments/17760302/Venn%20infographics.pptx?api=v2

Adrian Gropper and Jin Wen made some really good observations on the Venn, respectively:

OAuth represents an institution focus; OpenID Connect represents a federation focus; and UMA represents an individual focus.
OAuth represents a service availability focus; OpenID Connect represents a security/authentication/integrity/confidentiality focus; and UMA represents a privacy focus.

The profile specs we will be producing are layered. We don't actually know yet if the OpenID Connect and UMA profiles will be separately layerable on top of the OAuth profiles, or if the UMA specs will depend on the OpenID specs, or what.

Some information is outside individual control, but nonetheless needs to be monitored for sharing; this is what "accounting of disclosures" is for. We want to reduce inhibitors to data flow for three reasons: 1) clinical; 2) public health; and 3) research.



Firefox Social API 2 Years In, What Next?

Wednesday 1H
Convener: Christopher Arnold
Notes-taker(s): Christopher Arnold

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

Two years ago Mozilla pioneered a new extension-less API for quick customizations of Firefox. Termed Social API, the platform allows services to socket in chrome-level notifications (Push to user), share actions (Push from user), Save-to-cloud, News and Activity Tickers.

The platform has gained broad support from companies that each define their own user engagement model. (Facebook, Google, Twitter, Tumblr, Delicious, Pocket, Cliqz, Goal.com, Odnoklassniki, Mixi, Weibo, Sphere, Vkontakte, Saavn, Zimbra)

Benefits of software-less browser customizations are:
-Different services can't conflict with each other in the browser, therefore they cannot cause performance issues.
-Speeds the flow of engagement as the services can activate on their own domains without bouncing users over to a marketplace for download.
-Minimizes weight on the browser.
-Speeds engagement with a service by allowing a chrome-level access point.
-Lessens phishing risk if users reduce habitual download willingness.

-Places control of communications between the web services and their end users directly with no intermediary.

What this is not:
-Doesn't replace all use cases that extension developers have coded.
-Doesn't permit any service to have surveillance of other activities in the browser.
-Not standardized yet. Currently this is only a Firefox initiative. But the manifests are public and can be adopted by other browsers easily.

Try current services here: activations.mozilla.org/
Documentation on the platform is here: https://developer.mozilla.org/en-US/docs/Mozilla/Projects/Social_API

SCIM extensions

Wednesday 2A
Convener: Bjorn
Notes-taker(s): Erik Wahlström

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

- Small intro of SCIM (see https://www.simplecloud.info)
- Sessions goal is to figure out what people are and have been working when it comes to SCIM extensions.
- Note: This is extensions to SCIM, and it will not load down the general specs.
- Use cases:
    - Credentials Mgt
        - A client can send a password. But there is no mechanism for a server to say that it does not meet any quotarea. Life time, lengths.
        - VMWare, Intel, neXus, UnboundID, Cisco, Ping.
    - Streaming bulk data
        - How to send a bunch of data objects in realtime. Do we need a new endpoint.
        - Interests from: Microsoft, Leif, Patric
    - Change Notification, PubSub
        - Publish and subscribe.
        - Interests from: Oracle, Cisco, Salesforce.
    - ForgetMe
        - Client don't want to do a normal delete, but a more formal forgetMe call.
        - Interestes from: Ping, UnboundID.
    - Verification / attestation / LoA / Source
        - How to mark attributes with metadata for where data comes from. How to tag an attribute with LoA.
        - Interests from: HP
    - Device Provisioning
        - Add new Resource types in SCIM.

- For example a Device. iPhone, Android, VoIP and other devices that talks to the world needs an entry.
- Needs a Device resources that's a base for all types of devices.
- How do you assign devices to device resources.
- Interests from: Intel, HP, Oracle, neXus, Cisco.

- Entitlements and roles
  - Does the current element need semantics?
  - Interests from: HP
- Obfuscation / redaction
  - Sometimes you don't send all of the information, for example tokenized credit card information. Does SCIM need to define how to limit the access to attributes in resources.
  - Clients seldom have full knowledge of the full resource.
  - Interests from: TBD
- Service Provisioning
  - Interests from: TBD
- SCIM as "Directory"
  - Security model and access model.
  - Interests from: TBD
- Ownership and delegation
  - SCIM is missing information about what type of relationship a reference have.
  - Interests from: TBD

- Schema extensions
  - Consumer with age, preferences...
    - Interests from: UnboundID
  - Access Cards
    - Interests from: neXus
  - OAuth2 Clients
    - Interests from: Oracle
  - GeoLocation, a datatype for geolocation.
    - Interests from: Ping
  - Tenancy
    - Interests from: VMWare
  - Devices (IoT)
    - Interests from: TBD
  - Ownershop/Delegation
    - Interests from: TBD
  - Finance
    - Interests from: TBD
  - Multiple personas (roles/relations)
    - Interests from: TBD
  - Privilaged
    - Interests from: TBD

The VRM Social Network (Part I & II)

Wednesday 2C
Convener: Drummond Reed
Notes-taker(s): Micah McGraw

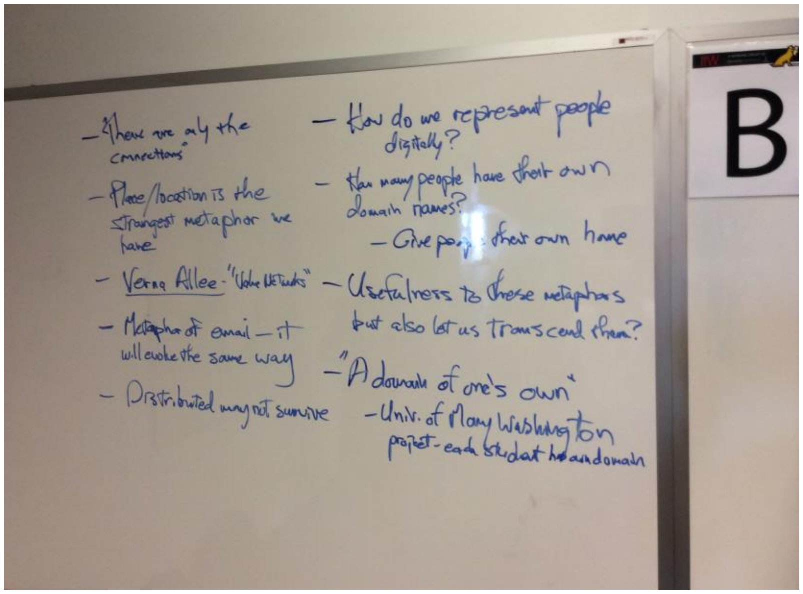
Tags for the session - technology discussed/ideas considered:

VRM, Social Networking, Ello, Diaspora

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

VRM and social networking

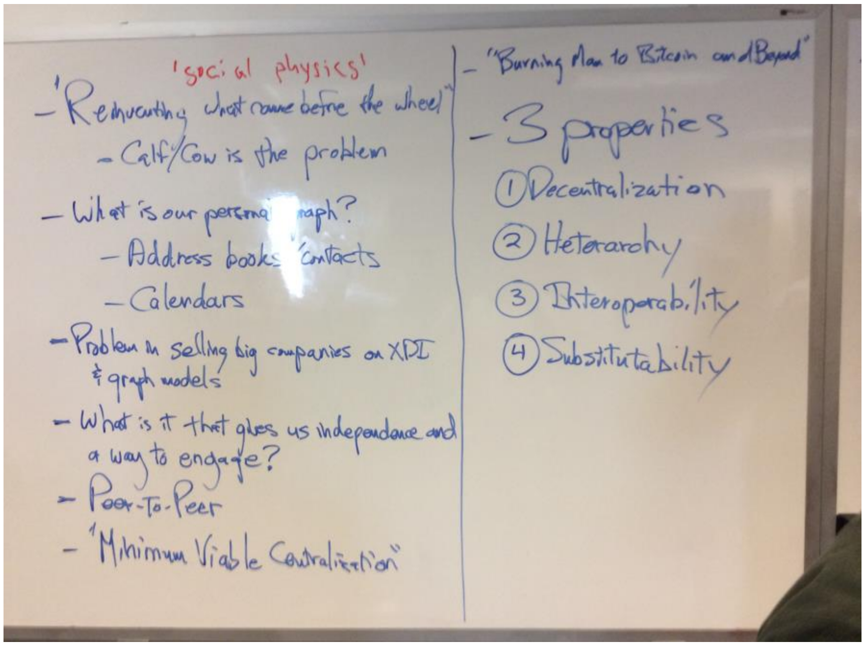
- Respect network
- Open standard personal distribution cloud
- Trust frameworks
- Ello and Diaspora
- Projectvrm.org - Docs blog post
- New paradigm from client server - graph based???
- Social networks before social networks (Rolodex)
- Where is social information centralized
- Minimum viable centralization
- Burning to bit coin and beyond
- Targeting the young builders that are unaware of the rules (rule breaker)
- 1990 silo email providers with proprietary system
- 2000 SMTP
- What will the evolution of social networking look like
- Committee of the whole
- Personas
- Context == conduct
- Home on the web that's theirs - social networking is like share cropping
- What are the metaphors that describe the new paradigm
- Domainofonesown
- Identity is not node it's the connection
- Domain is home
- Where never not on the net anymore
- Xdi/uma/openid
- Book: Value Networks
- Blogs were the early social networks
- Do people really embrace central authority's
- Cookie model - do we want to be plate the cookie or chocolate chip



- "There are only the connections"
- Place/location is the strongest metaphor we have
- Verna Allee - "Value Networks"
- Metaphor of email — it will evolve the same way
- Distributed may not survive
- How do we represent people digitally?
- How many people have their own domain names?
  - Give people their own name
- Usefulness to these metaphors but also let us transcend them?
- "A domain of one's own"
  - Univ. of Mary Washington project - each student has a domain

B

- Place/location is the strongest metaphor
- we have
- Verna Allee – "Value Networks"
- Metaphor or email – it will evolve the same
- Distributed may not survive
- How do you respect people digita
- How many people have their own domains
- Usefulness to these metaphors, but let us also transcend them
- A domain of my own



'social physics'

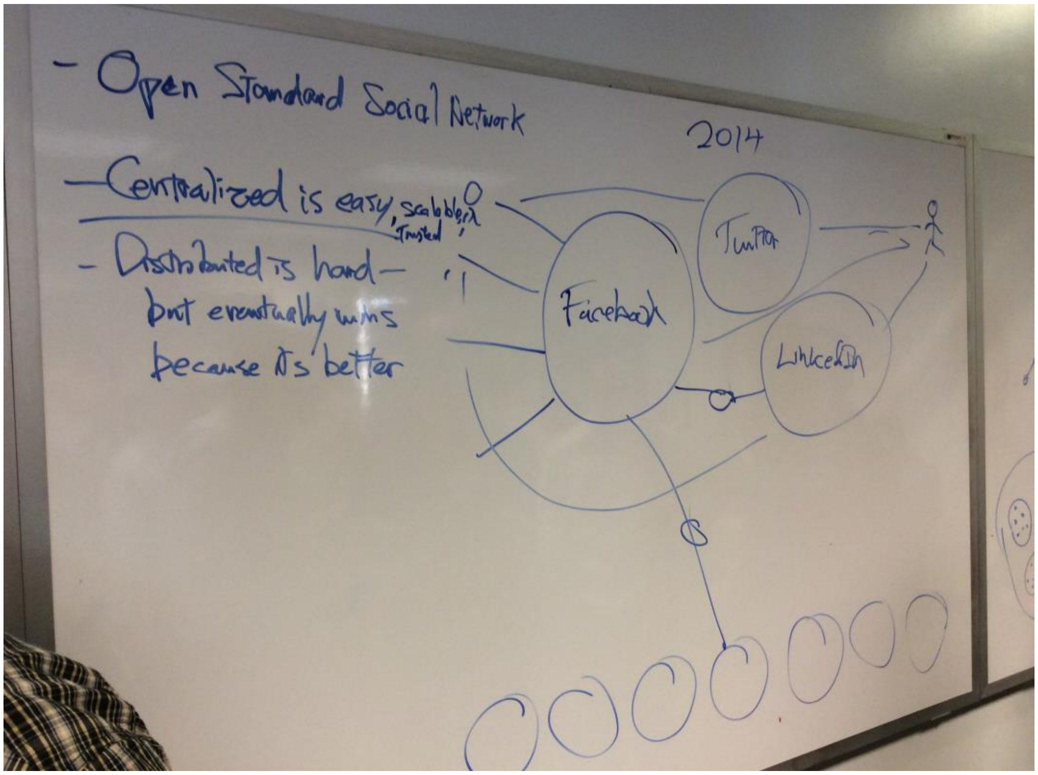
- 'Reinventing what came before the wheel"
  - Calf/Cow is the problem
- What is our personal graph?
  - Address books/contacts
  - Calendars
- Problem in selling big companies on XDI & graph models
- What is it that gives us independance and a way to engage?
- Peer-To-Peer
- 'Minimum Viable Centralization"
- "Burning Man to Bitcoin and Beyond"
- 3 properties
  1. Decentralization
  2. Heterarchy
  3. Interoperability
  4. Substitutability

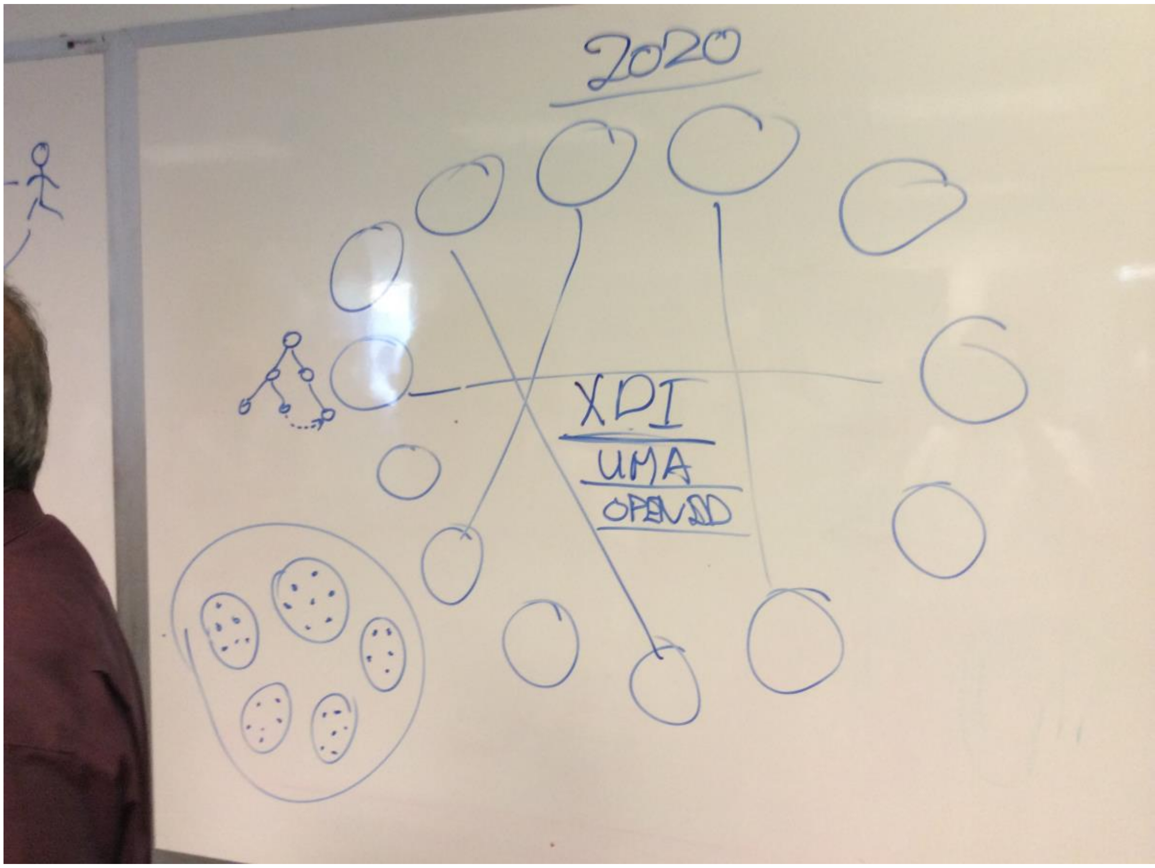
Reinventing what came before the wheel
What is our personal graph -> Calf/cow is the problem
What is personal Graph?

Address books and contacts

Calendars

Problem in selling big companies on graph models
What is it that gives us independence and a way to engage?
Peer-to-peer
Minimum viable centralization


- Open Standard Social Network
2014
- Centralized is easy, scalable, Trusted
- Distributed is hard - but eventually wins because it's better
Twitter
Facebook
LinkedIn


2020
XDI
UMA
OPENID

VRM Social Network – Part II

Date – October 30, 2014

Doc Searls was in the session.

Goal of today's session:

6 Properties:

1) Decentralized
2) Heterarchy
3) Interoperability
4) Substitutability
5) Independence
6) Openness

Pain Points that exist in the current solutions:

1) Not everyone is on it – true ubiquity (Facebook, LinkedIn, Twitter)
2) Privacy and Personal Data
    a. Privacy is a new luxury good.
    b. Privacy – when they understand what it costs.
3) Discrimination
4) Security (lack of)
5) Freedom Infringement
6) Legal – privacy by consent cannot be known (big data problem).
7) Economic measure of accountability – how to be an economic actor.

VRM:

1) Independence/Agency
2) Sovereignty
3) Ability to engage socially

Principals:

1) The nodes are people
2) Mirror the same architecture of the Internet
3) A place for value exchange between people
4) Must come from the people
5) 4 party model
6) Relationships/Connections

Political Movement Framework:

1) Digital Personhood
2) Marc Davis' PII take

Mozilla's "Subscribe to Web"

Wednesday 2D
Convener: JB
Notes-taker(s): Christopher Arnold

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

VRM day JB Piacentino presented Subscribe to Web (aka S2W)

How can we fund the web and empower users while considering privacy at the forefront?
Advertising has spurred innovation and free services without users paying (on the surface)
It reaches limits. There are tracking approaches that have taken a greater significance.
You're seeing content being designed "around ads" This is termed "Native Advertising" where the content is designed to change your opinion on a subject or get you to buy something.
This shows that the ad industry is trying to counterfeit content.

Users don't see ads anymore. It's called "Ad Blindness". So the industry is extending their models further, typically with tracking. Users are reacting by installing ad blockers because they've had enough of it. A lot of users leverage ad blockers or tools to protect anonymity. Users are rejecting the model that funds the web. Meanwhile, users are still consuming the content while not paying any price for it.

Content creators are hurt if they depend solely on ads if users start to tune out.
Would users be willing to pay the amount that ads typically derive for publishers?
$12 in the US
The ad tech industry shaves off a big cut of the revenue the publishers get.
For $12 in overall spend through advertisers, a publisher might get $6.
Ads are taking over content and changing how publishers serve content. Sometimes publishers make you click three times to read one article!

Mozilla is introducing a new experiment, a new kind of contract between a user and a publisher.
For users, we want to let them have an ad free service in exchange for paying for the content they're given. Users expect to have a commerce experience with a publisher. There are some rules around it. Member web publishers in S2W get more loyalty from the user. We want this to be an open system.

S2W works on a donation model in lieu of the typical ad placements. Users put a bit of money in a kitty that is allocated across the sites I visit over the month. Sites I visit get a voucher that is summed at the end of the month.

In exchange the publishers don't need to serve ads to that user, don't need to use tracking technology. And the publisher might offer other types of content to that user.

We've implemented it as a web-API. The publisher pings before they serve the page. They ask, "Is this user a S2W subscriber?" if so, they show an environment without ads served to the free group.

We want this to be an open system like the ad ecosystem so that any publisher can implement, and any other browser can use this too.

We issue IDs to the users and the publishers in the system.

Participants are in control. Should there be a mechanism to report sites that don't act appropriately?
There might be a favicon that indicates the state of the web the user is on.

It needs to be a blinded token. You don't want to know if it's one identified user. Each transaction has a different ID so it doesn't leak fingerprintable identifiers.

This is a little bit like Kickstarter. People want to put money to great publishers to see what they are going to do tomorrow. People donate to get good future content.

We think there is will to support subscription models.

This might be beneficial on the mobile device. This could be the next step.
If you as a game developer could have a base of S2W users, you know that you're going to get paid to do what you're good at. Premium model still remains.

Perhaps we could enrich this experience with Gold, Silver, Bronze marketing approaches? Different levels of content? Maybe eventually.

We haven't yet figured out how much context the publisher should get on the page load. We think users should be in control of what they share.

We are also going to be creating a directory of content that supports S2W, so users that want to be able to specifically find publishers that are supporting their preferences.
We want to improve return on investment to publishers who participate.

We are also concerned about web diversity. Ads work for the head publishers, less so the long tail sites. Obscure blues podcast blogs might just have 100 visitors per month. They're not going to get anything from the ad model in terms of the scale they operate on.

We have to give users a way to favor a specific publisher for instance. A user needs to be in control of where their investment is contributed.

If sites are paid by the value they give end users rather than how much traffic they generate, a better web will result.

Part of what you're paying for is not being tracked right?

Personalization isn't tracking. I may declare my location because I need a local service. There needs to be a transparent offer to the user. This is essentially contractually agreed sharing of context-specific data sharing.

Verizon may track page views on your phone. But my expectation is that they provide phone service, not track my ads. Users will share information with web publishers if the benefit is direct and obvious.

Value of advertising is dropping. CTR is now .03%. People are fighting for shares of a race to the bottom. Let's just try a different model. Let the customers be in control of the transaction.

User should choose the entirety of who gets their funds.

This is a way that you can build in the sustainable model for web publishers to participate in the web itself.

Many publishers don't even know the tracking technologies that are sitting on their pages.

The weight of web pages is much higher than the content of the page that the user is after.

There was Mozilla Lightbeam that measured the different tracking attempts on users. If we're optimizing for a fast web, we have to lighten the load. There needs to be a third option on funding web content.

We're starting with experiments in Europe. We hope to learn how users engage with the system.
We want to learn of the value publishers will get on how it works. Next year we want to do broader deployments.

This is a bit like flattr. But for us this is about a transaction, not a straight donation. This is not a micro-transaction model. This avoids user fatigue. Donations take a lot of effort.

blog.mozilla.org/advancingcontent

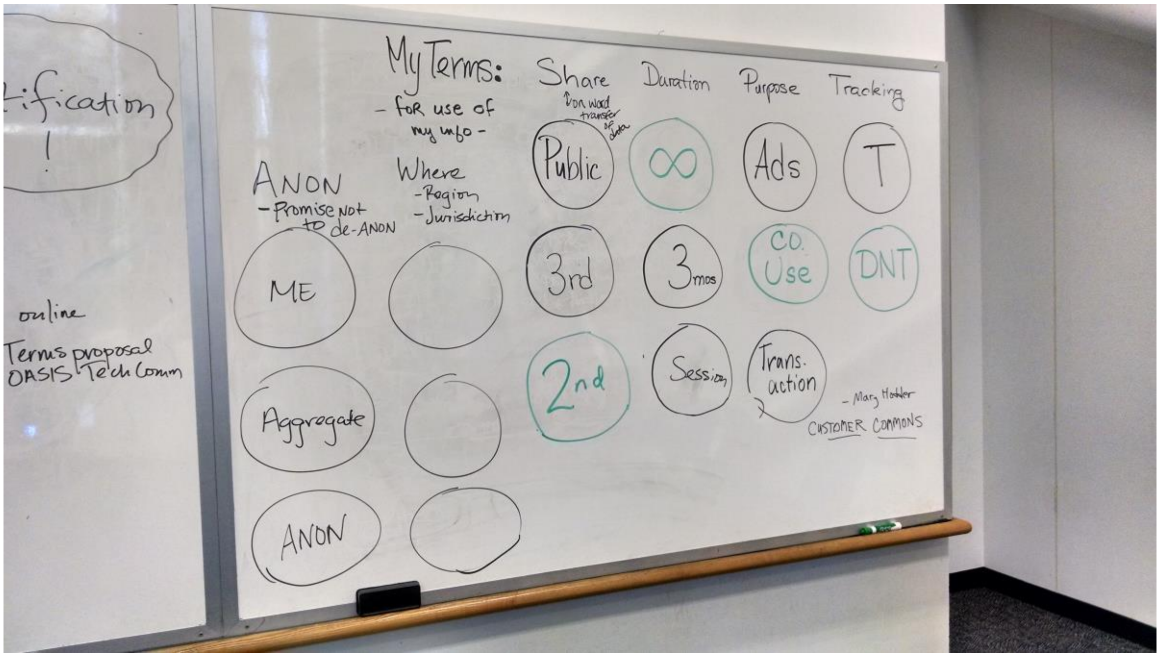
User Asserted Terms for VRM

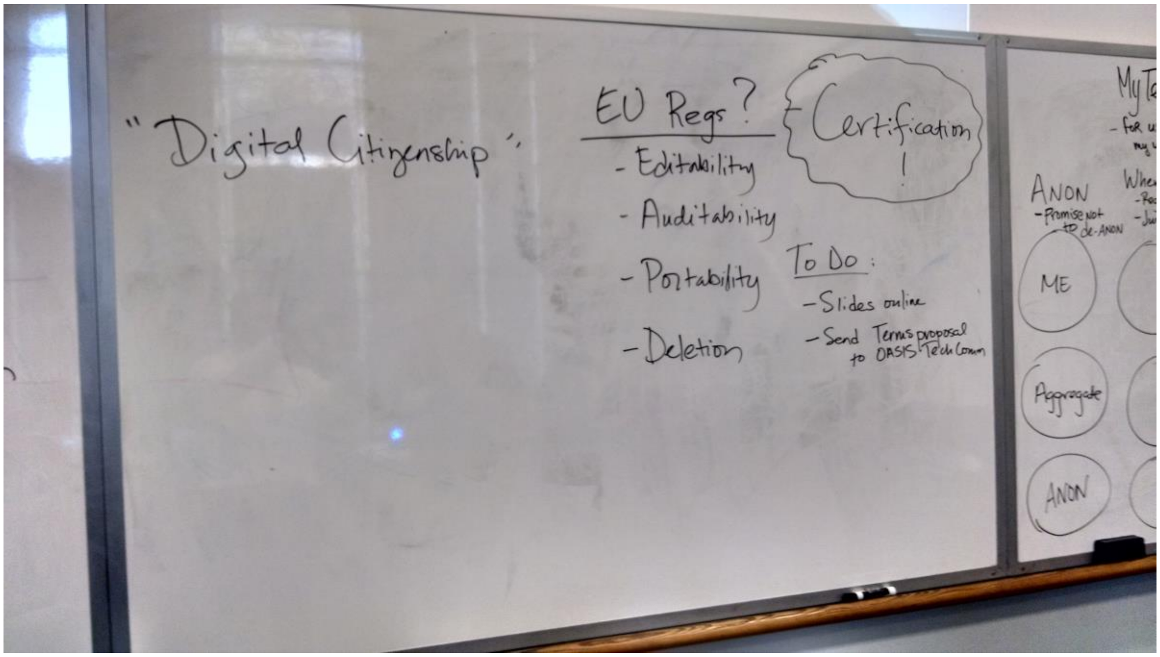
Wednesday 3A
Convener: Mary Hodder
Notes-taker(s): Mary Hodder

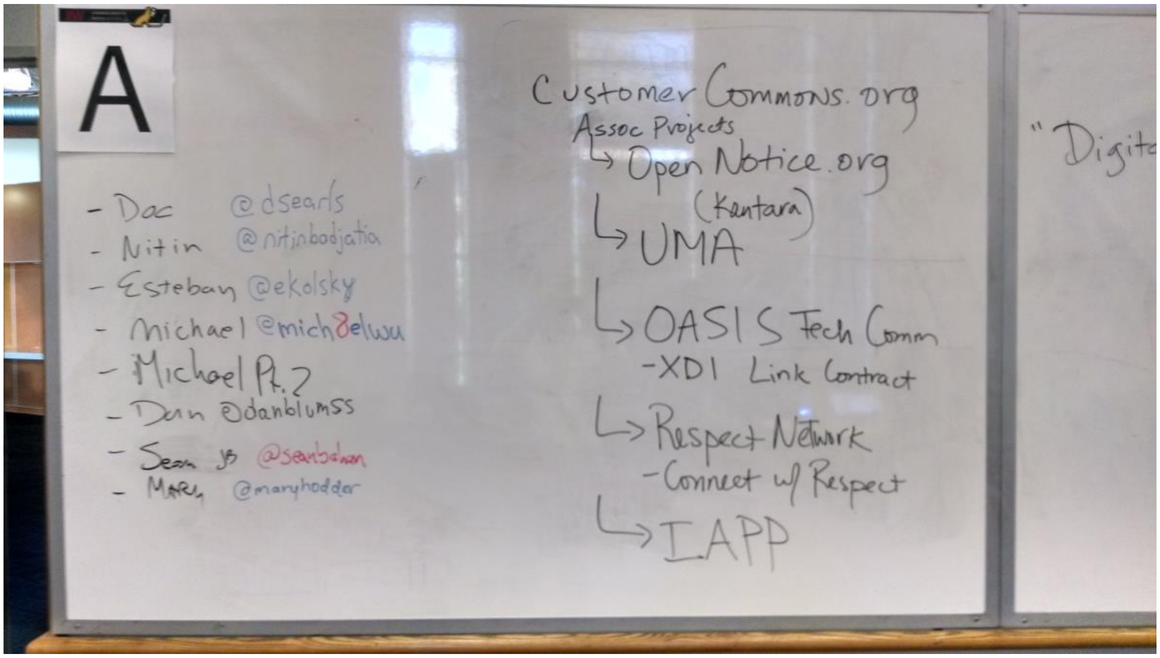
Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

The group explored how we could improve the User Submitted Terms strawman proposal...

Notes in the photos below:







PDEC = Personal Data Ecosystem Consortium

Wednesday 3D
Convener: Dean Landsman - Communications Director of PDEC and Kaliya/Identity Woman Founder/Executive Director of PDEC
Notes-taker(s): Dean Landsman

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

Introductions were made around the room, of roughly 25 participants,

NEC, Mozilla and Twitter were among the companies attending the session, as well as IIW attendees from Japan, France, Denmark and the UK. Of note is that a good many PDEC members in the US and around the globe had emailed Dean to ask if any PDEC sessions could be streamed.

Questions about PDEC goals and operations were brought up, as the room had current members, interested parties, and newbies to the organization.

Among the many topics covered: As PDEC grows, what will be the qualifiers for more companies (or individuals) to gain membership? Will PDEC as a trade organization need to do in order to be of value to members ranging from start ups to giant companies?

Kaliya noted the present annual membership fees basis ranges from $150 for bootstrap start ups to $1000 for companies with angel funding, up to $5000 for funded start ups. It was agreed that this needs to be reviewed and reconsidered, as PDEC matures and the industry itself is experiencing rapid growth.

Can large companies also play a role? How exactly does PDEC vet members? Dean offered that these issues were part of an open discussion; a PDEC Governance Committee is assembling, led by Kaliya who announced that volunteers were already aboard the committee. Dean added that as a membership group, a trade association, all input for consideration by the Governance Committee was welcome and encouraged.

Michael Becker (of mCordis), with a decade of experience as Director of Marketing at the Mobile Marketing Association (MMA) suggested that PDEC could and should be the source to its membership:

- As a Central point of information and policies (for members)
- providing Research & Insight (for members)
- a place to Create Connections, Resources and Contacts

Michael added that as a marketing and information source, PDEC would grow rapidly, with companies of many sorts as well as the trade or consumer press coming to PDEC for information, guidance, assistance and research.

Jamie Clark (of OASIS) noted that personal data stores are an emerging phenomenon, and PDEC can be the place where members can share work issues and gather to combine value and define what it is the industry is about, where it is going, and improve the lot for all members. Jamie's experience as Chief Counsel at OASIS and his work as Director of Standards would be of value to PDEC.

Jamie & Michael discussed how a standards body and a marketing arm (as a trade group) can synchronize to the benefit of many.

Jim Fournier (of Planetwork & Spherical) suggested that PDEC provide an informational role to both its members and the outside world. That there is mutual value for both sides.

Katryna Dow (of Meeco, Australia) offered that PDEC could be of great resource for marketers of a Personal Data Store (or bank, vault, locker); that they can deliver value to a brand, an individual, a government.

Katryna added that there is a perceived risk in allowing or enabling an outside party to house (or host) data, there are potential liabilities…having an outsourced solution may help mitigate that responsibility. PDEC can help bring this message out to the world at large, and PDEC members can share their experiences in dealing with these and other areas as companies in this space emerge and evolve.

Much of the discussion centered on PDEC maturing as a trade organization to include lobbying as part of its portfolio of services. Prior to that there needs to be publication of a Mission Statement, of a set of operational standards and practices. Dean noted that all of this, in fact, is in progress at PDEC right now.

There was additional discussion of PDEC martialling the discussion around Personal Data and the entire ecosystem, ranging from the various types of providers (as reflected in the diverse PDEC membership) to a consumer/user side, being the key resource, the go to point for information in the arena.

Jean Russell (of Leloa Group and also PDEC) noted that PDEC's current goals to date have been around connecting members, connecting them to information (and facilitating information together), and sharing outward what members are doing.

Kaliya added that PDEC could raise visibility in press as the trade organization of note. That such a position would have members of the press come knocking on our door.

Dean reminded the group that PDC seeks blog posts from members, as well as contributing to PDEC White Papers..

Hernrik Biering (of Peercraft in Denmark) asked how can we develop incrementally? What is practical? How do we tap into existing things? Do we have something we all need? That these are questions to incentivize the membership. He expounded on this, and Dean asked him to put that into a blog post for the PDEC site.

By and large the group agreed that PDEC is in growth mode, and that the opportunity to serve and expand is there for us to seize.

OAuth2 Challenge/Response Grant

Wednesday 3C
Convener: Samuel E.
Notes-taker(s): Erik Wahlström

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

- How to integrate physical access systems into digital access systems.
- OAuth2 in IoT scenarios where policies and deceptions is taken on the AS.
- Sometimes the AS requires different attributes for a specific client to be able to issue a token.
- Example: A IoT enabled door takes a JWT to open up the door. Sometimes the user waives an NFC/RFID based card in front of a card reader to authenticate, but sometimes the user also have to enter a PIN code to be able to open up the door. The policy for the door is changed centrally in the AS.
- The question is: Can this be defined in a new grant type that uses a challenge/response mechanism or is this outside of the spec and it's just authentication to in a code grant flow.
- It depends on architecture. Is card the client, or is the reader the client?
- What happens when things are offline? Some work have been done by neXus with a JWT that includes an ACL.

Discussions flows out in to a general security in IoT discussion.

NSA Surveillance in Austria

Wednesday 3D
Convener: Markus Sabadello
Notes-taker(s): Markus Sabadello

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

In the Snowden documents, Austria is listed as a "Tier B Focused Cooperation" partner of the NSA's SIGINT programs.

We identified four "points of presence" likely related to NSA activities in Austria: The U.S. embassy in Vienna, the so-called "NSA villa", the "IZD tower" next to the U.N. headquarters, and the "Königswarte" listening post near the Slovak border.

Build A New SAAS app With Enterprise Identities. What would you do?

Wednesday 3H
Convener: Patrick Radtke
Notes-taker(s): Patrick Radtke

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

SCIM, provisioning

There are a lot of ways to do provisioning. To cover the widest range of customers (both in terms of size and capabilities), implement

- file upload for customers that aren't capable of using automated means
- have an admin interface for deactivating users
- support SCIM

Groups that had implemented SCIM estimated effort at ~1 month, and allows customers to take advantage of SCIM hubs, so even if a customer is not capable of calling the API themselves, it is easy for them to use a product that does talk SCIM.

The Re-founding Sisters, Real Representation in Virtual Districts

Wednesday 3I
Convener: Britt Blaser
Notes-taker(s): Britt Blaser

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

"Virtual district" was coined in a 2009 paper written by Britt Blaser, David Weinberger and Joe Trippi, for the annual meeting of the Digital Government Society of North America, reviewed by Craig Newmark at the Hill. A virtual district is a social network whose members are credentialed as constituents in a real-world political jurisdiction. Background:

Real Representation

Britt's claim was confirmed by Phil Windley: it's well understood in politics that a few vocal constituents have a disproportionately large influence on policy, because representatives actually hear from so few constituents, and that the constituents they hear from rarely deal with the arcane, complex language that defines policy in the helpful way that the open source community deals with the even more arcane, complex language that defines computation.

Re-founding Sisters

A phrase to inspire young women to realize their power, based on John Ellis' book the Founding Brothers. He stressed that the "Founding Fathers" were not gray-bearded leaders, but were young, future leaders growing into their roles. Similarly, young women who think of themselves as sisters and not authority figures may be best equipped to reframe the American experiment, based on statistically valid online representation.

FEMvote.us will deploy the combined capabilities of NewGov.US + SNAPvote14.com to create a virtual district for every one of America's 435 Congressional districts. FEMvote.US is in formation by 21st century women, defined as women who have lived half their lives in the 21st century.

Britt demoed the complementary online services of NewGov.US and SNAPvote14.com. Each service places participants and their media on political jurisdiction maps and creates some level of confidence that the participant is a constituent. High confidence is a powerful motivator to politicians and their staffs.

The NewGov GEOvoter API acts as a "Polygonal Identity" provider: A participant's address is discarded after it's used to associate the identity with political jurisdictions in 8 map layers:

- state
- congressional district
- state senate district
- state house district
- county
- city

- city council district
- unified school district

Never before has an American been able to:

- participate in politics without exposing a real name and address.
- participate without attending awful political events.
- build political influence outside of the 2-party system.

This is especially important for Internet-savvy people who are not necessarily more timid than others, but who have a non-political life and value their privacy. They are precisely the kind of people who are best-equipped to debug the U.S. Operating System.

Attribute (Anonymous) Based Credentials

Wednesday 3J
Convener: Andrew
Notes-taker(s): Hugh Pyle

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

Lots more attendees to this session than expected for an esoteric crypto topic. So we started with a round of intros & asking why people are interested in the topic.

Andrew (convener): math background & voting systems. Previously: AskForIt startup. Interest areas including proving something while anonymous.

Greg - One use case is to have lots of "demo" accounts, or personas; interested in controls & management to how things become linked together.

Mads – WAYF, Denmark. Have deployed a hub & spoke attribute-federation system, but WAYF actively don't want to know everything about the users; would like to be able to deliver similar functionality, filter attributes for disclosure to various RPs, & mechanisms for users to grant usage-consent without disclosing the PII values to the hub.

Steve - VMware, access management. Balance marketing desire for tracking/login. Access control & authentication credentials

Morten - Alexandra Institute. Security & identity management work. 25years ago was young crypto nerd -> then book about anonymous credentials (Stefan Brands, etc). Thought maybe we would have a truly private internet by now, but still waiting!

Jin - McKesson - has some understanding of uProve. Use case for patient accessing healthcare, with limited disclosure as needed for service provision

Terry - interest in this stuff.

Kazue - NEC - cryptographer. Worked on group signature schemes & anonymous authentication. Has worked through approaches of: standardization, documents. Also working with ABC4trust.

Berit - Alexandra Institute. Background in math, cryptography, but not practitioner for some years. Interested in the gap between research & commercial applications,

Jim - independent - involved in the ID ecosystem steering group.

Paul - NIST - part of NSTIC program office. Business sponsor of Identity Broker. Citizen access to federal applications. Should eliminate trackability etc but don't think it does today. Want to move to something production-ready & commercially available.

William - Google identity team; Some identifiers for purposes of login mainly.

Steve - interested in pseudonymous-by-default

Mary - Google same team as William. Main applications are in federation protocols.

Reiner - independent consulting. Interested in alternatives to anonymous credentials; did a survey for kantara. How can we achieve same goals? - the Canadian late-binding model; or a mirror-like model to anon credentials, = anonymous service providers or relying parties
One problem is how to get these things started. For example, how to build into SAML.

Hugh - Qredo - software startup, building a new platform for applications of personal data; interested in use cases for rapid consumer adoption. Some seem to be around single or few attributes in retail environment.

Bill - New Zealand - ministry of education; worked with government central identity management
---
Q: uProve: active, alive, working?
  birg should be running beginning next year
  mixed signs from MSFT
  discontinued Java implementation? Nothing happening for long periods?
  decent license though, Microsoft explicitly permissive.

idemix (IBM's identity mixer):...?
  weird license, should be cautious as a commercial enterprise

uprove issuing certs every time
idemix re-using, so more efficient in real uses.
upro? mybe, if want to release multiple attributes -> slow
  talked to ronne bjernst (sp?) from Microsoft
  ZKP versus group signature protocols

Q: are they doing ZKP really?
Andrew: math for idemix is.
Uprove uses *blind* signatures (Brands). If want to bind multiple attributes they may become complicated.

ABC4trust (EU projects) use idemix?
First thing ABC4trust has a harmonized (pluggable) API for multiple systems with uProve and idemix as two.
Some politics maybe for IP issues
Sweden project - Soderhamn - smartcard with identity - education setting
   prove that you had been in classes -> track when gave feedback
   secure for purpose (no false voting) but retaining privacy
Also there's a similar project in Greece
Both proof of concept projects

Additionally there is an ISO standardization effort -> quite early, working on a study period
Head is from IBM Zurich
Will probably take 3-4 years before standards can be ready

Other? Different cryptosystems, other implementations??
Group sig libraries? ->
   hard to find a library that implements these things
   MIRACL? & few others with primitives, not end-to-end

Reiner has proposed blinding of the IDP

Q (NIST): re idemix, is it using SAML or ...?
   A: Some addendum, quite vague
   Q: Next step -> profiling so can be deployed in identity systems that support these standards
   Existing standards assume traditional PKI
   Broker model

Morten: Looking for blindable single-use certificates
   for use cases that are traditionally solved in other ways
Hugh -> blinded tokens for service access
Reiner - hopeful - layers, that's the way stuff evolves
   e.g. Gateway / add software layer for access to existing infrastructure
   plus need a back-channel
   e.g. need to send user email
Morten
   attach a coin to request
Reiner -> need a pseudonymous recipient address

Q: Jim:
anonymous/pseudonymous with respect to which parts of the transaction?
Mostly we say that with respect to relying parties

but there are lots of others - IDPs, attribute-providers, etc.
e.g. over21, usually need other information than that
intermediaries are an efficient way of solving the problem
probably want an intermediary in order to provide blinding of who is using these attributes from the authoritative source of them

morten: thing is to do the blinding yourself.
then any intermediary doesn't have the tracking of usage and so on.

Jim: more about being able to abstract some of the information

Hugh -> use scenarios? e.g. age plus photo, where photo is the "recognizer" for F2F

Morten: ZKP attributes - meaning, provable attributes, with the RP unable to pass those attributes to a third party
But: for example, liquor purchase, want to be able to prove to authorities that the user was verified
Reiner: Systems build this as a role for discloser ("designated opener"), able to unlock under special circumstances
Morten: The opener - interesting but some potential for misuse depending on your scenarios

Kazue: everyone has different needs
  but the crypto is different based on everyone's needs
  that's part of the problem comparing with e.g. SAML
Andrew: does that need advances in the cryptography? for standardization?
Kazue: where's the instance to implement?
Hugh:
Nist: working on at least three use cases
  one will be made public once solve it
    (that won't happen immediately though...)
  hub approach --> identity & attribute - implementing parts of this
  another: with msft & uprove, some work
  another: recently awarded, hub model, trying to keep subject privacy

So there are at least three attribute hubs? demonstrates a real demand for these things
  USA / nist described
  Denmark - part of ProAc - researching options
  UK - IDESG / Cabinet Office digital services - private-sector IDPs, local & central gov RPs
at varying states of development
shows that use cases are valuable

nist:
  single credential to use services from multiple US-government RPs
  attributes shared with consent
  multiple IDPs incl private sector

  good at blinding the identity, but nothing yet in place for the attributes

Signed & encrypted from IDP to hub -> strips -> repackages for the RP
Want to maintain that level of blinding for all the PII attributes

Reiner: alternative is to have end-to-end from IDP to provider
as long as the IDP has no knowledge who they're encrypting for
attributes passed through because encrypted

UK: assertions are signed across the hub
so the hub can't change - but can see the attributes as they pass the hub

Morten: Canadian system had a similar
late-binding model
blinded token
Reiner: paper see link: https:arxiv.org/abs/1401.4726

nice thing about end-to-end is that in the SAML world that's minimally invasive

Q: (Reiner) if don't use smartcards as the credentials, what can you use?
ubikey? mini-HSM -
nice, not really "anonymous" in the sense of unlinkable show;
device holds a secret key; generates keypair, encrypts the private key & sends to RP
So quite simple, and unlinked across RPs

Open UMA Implementors'

Wednesday 4A and 5A
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:

All of the current interop testers were represented in the meeting (Gluu, ZXID, Cloud Identity, Roland Hedberg), along with other in-process implementors such as Intel and ForgeRock. We discussed the current state of the interop testing, reflected here: http://tinyurl.com/uma1iop

We took a look at the somewhat volatile state of the UMA core spec as we do issue burndown, reflected here: http://docs.kantarainitiative.org/uma/draft-uma-core.html

We discussed the opportunity to develop a Best Practices for Implementors document as an adjunct to normative spec text, which could capture advice such as:

"You may want to use different OAuth grant flows for different use cases in minting protection API tokens (PATs) and authorization API tokens (AATs). For example, when the resource owner is an organization and not a human being, the client credentials flow (where there is no human user) may be appropriate."

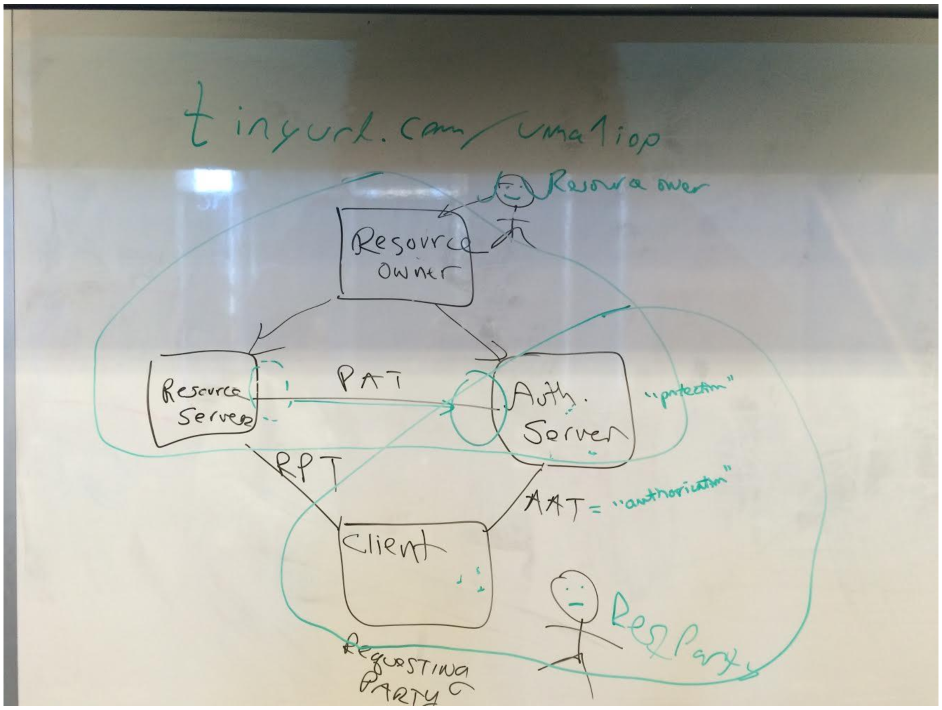
We discussed the parameters of the type of interop testing we're doing at this stage. We agreed that we're doing "implementation" testing vs. "deployment" testing, meaning that we're okay with developing test instrumentation that accepts automated testing flows vs. requiring a human being to "babysit" testing flows to, e.g., press a button during key rollover etc. We discussed possibly allowing an RS to pass some version of authorization policy to the AS during resource set registration, not for the purpose of interop-testing the policy, but just because it's necessary to provision relevant policies to an AS to let downstream interop testing take place. There are a number of ways to do this. We discussed, but didn't fully settle on, a way to have the AS simply return a "yes" vs. "no" answer to a policy question.

We discussed the current state of user authentication. Roland's test suite currently handles all of the following methods: 1) username and password (for easy form automation), 2) token authentication (for easy query parameter automation), and 3) social login. We toyed with asking him to support JWT authentication in addition, but decided not to push our luck. :-)

A diagram we returned to over and over was this one, shown on the UMA wiki (http://kantarainitiative.org/confluence/display/uma/Home):

http://docs.kantarainitiative.org/uma/three-phases.svg

We annotated it during the course of the session, as shown in the attached photo:



Field Trip: Museum Demo of IBM 1401

Wednesday 4 Museum
Convener: Oscar
Notes-taker(s): Oscar

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

CRM/VRM Framework Part II

Wednesday 4F
Convener: Nitin
Notes-taker(s): Christopher Arnold

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

Define CRM engagement into VRM instead of leaving them to figure it out themselves.
Consulting firms are engaging (CapGemini et al)
Need a tear sheet discussion guide for the industry.
Key talking points. What does their world look like? (Consultants)

Dave ~ What we want to say to companies is, "No matter who you are, you're not the one who knows the most about your customers. And you're not the one that the customer trusts most."

Ajay ~ Cap Gemini defines difference between CRM and VRM. But they don't point out why it matters.

Dean ~ See how the money is made and saved by having VRM in the equation.

Consultants need to profit from telling the story.

…$16.5 Billion in customer defined transactions from the UK perspective…

Nittin ~ To build our deliverable, we need to rationalize what we know.
Gartner talks about magic quadrant. Forrester calls it a wave.
Preso: The Forrester Wave (TM): Listening Platforms, Q1 2009
People see these as a stake in the ground.
These guys advise the enterprise buyers.
Going down to the weighting of strategies breakdown of different players in the space.
Their ranking is interesting.

Sean ~ We're in the category business though. Let those guys do the ranking. That's not our interest.

Marc ~ We need to give them "Executive Convincing Units" that will help management make decisions.

Nittin ~ TSIA has two shows a year that did 50% of the business we generated at their events.

Ajay ~ Features aren't defined in VRM because the structure can't be defined until there is more data.
…We explain what some of these capabilities are…

Sean ~ Gartner and Forrester are interviewing CEOs to. We want them instead telling them what they should be thinking in the space.

Nittin ~ Let's start our own grid.
What are the necessary criteria? Customer Empowerment, Market Makers, Company Enablement. Then lay the companies across it.
Qredo, Priceline, Uber, Thumbtack etc.
Graphs: standard maturity model. Graph: Radar Chart model for each company in the analysis

Dave ~ Some companies need to be defined at VRM (even if they don't claim it) Provide the complexity so they can.

Sean ~ And we need to claim certain companies that don't claim the identities.

Nittin ~ Consultants like to be able to say "You've got a new market to chase."

TRob ~ Priceline does something with companies that provide APIs.
Uber is actually creating the market.
What about quantified self opportunities?
Who is the authoritative source?

Doc ~ Customer Commons might do it.
We don't have the money and the labor though.

Nittin ~ I like the idea of TSIA.
At RightNow Technology we would get RFPs come in. TSIA, being neutral, defined that difference in speciality of the different players.

Marc ~ We should talk to companies in the space who have the ability to expand into VRM space.

Sean ~ Help companies understand where the gaps in the market are for key players that could fill it.

Marc ~ You can plot companies in the 3x3

Nittin ~ I want to have a VRM brain dump.

Dave ~ We need to break out IoT, Sharing Economy and Quantified Self opportunities. Companies that fall in, we can then rate them by the capability maturity model. We can define what is goodness in this world.

Marc ~ There are three basic roles.

TRob ~ Companies tend to build only for the context of their specific service.
But there needs to be machine-readable format of the API they'd give. Not the app they'd build.

Nittin ~ People can build VRM on their own. But where do they go to understand their missing links?

Dave ~ A company can't be a market maker if the requirement is that it extends across multiple parties.

TRob ~ People tend to limit their thinking to what an app can do, when it's the API they're supposed to carry about.
CapGemini tells companies to build apps to capture the concept. But they'll miss major points.

Doc ` CapGemini fidelity was pretty high.

TRob ~ We want to sell them into a market they can enter into, not a specific service they need to build.

Nittin ~ We'll get to those points of opportunity/clarity

TRob ~ There needs to be an authority to check against.

… Ad platform dollars can go into an experience model…
If there is shared value created in the ecosphere, there could be 1-100 characteristics.
When we talk to major institutions, they're relieved that they don't have to build something.

Dave ~ Just enabling inter-connectedness.

Ajay ~ You're going to see a lot of apps to solve specific problems when what you need is a platform.

Nathan ~ There are over 100 companies right?
Why don't we use those to extract attributes?

Nittin ~ Let's start with a best effort, then push it out to the companies on the list.

Marc ~ What about a legal framework?

Sean ~ VRM happens when certain rights are observed.

Shared Document for Editing http://bit.ly/vrmGrid

Amazon Web Services (AWS) and Identity Management: What's New?

Wednesday 4H
Convener: Shon Sham
Notes-taker(s): Matt Berry

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

Recap of yesterday's AWS session, with more detail into non-OIDC federation technologies. AWS supports SAML, OIDC, and also has a hosted wire-compatible Active Directory service.

Question: When a federated session credential expires, what is the customer experience
Answer: In the event of an expired session credential a 403 error is returned. From the Application point of view, it can attempt to refresh the credential and try the request again. If that is successful then the process is transparent to the end-user. If the IDP requires re-authentication, then the user will have to comply.

Question: In AWS Identity and Access Management (IAM), do you specify which IDPs your application wants to support?
Answer: This is correct. Create an IAM Provider for each IDP you wish to support in your application. IAM Providers hold metadata about Identity Providers that allow AWS to properly authenticate claims from the IDPs. In the SAML case, it is the IDPs public keys. In the OIDC case, it is the information needed to perform Key Discovery.

Question: Is AWS Directory Service a regional service?
Answer: Yes, each region is a separate directory, which you can join into a forest if you wish.

Question: When using the "AD Connect" option in Directory Service (where AWS maintains a VPN connection to an on-premise AD Domain Controller) is the VPN mandatory?

Answer: Yes, AWS acts as a transparent proxy for the Domain Controller in your network, thus for security reasons a VPN connection is required.

Question: What is AWS Virtual Private Cloud (VPC)
Answer: VPC is an AWS service that interoperates with EC2 that allows EC2 instances to live in your network IP space via a VPN connection.

Question: Is the "AD Connect" proxy truly transparent
Answer: Yes

Question: Can each AWS account have multiple domains
Answer: Yes

Question: Does AWS support the use of SAML Enhanced Client Profile (ECP) protocol?
Answer: Yes and no. AWS accepts SAML Authentication Response objects that are Base64 encoded. This is directly compatible with the WebSSO Profile of SAML. However, the result of the ECP protocol is an Authentication Response wrapped in a SOAP/POAS envelope. So if your SAML IDP supports ECP, then you can extract and Base64 encode the response.

Question: Does AWS support SP-initiated login to the Management Console?
Answer: SAML: Not at this time, OIDC: In good time

Question: Does AWS support SAML Discovery?
Answer: No

Question: Can I stand up an ADFS server in EC2 and use the Directory Service Domain Controller?
Answer: Yes.

Conflict Resolution in Community

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

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

Discovering ~ Creating a place within IIW community where people of disparate backgrounds, genders, cultures, ages can come together in dialogue to address conflict.

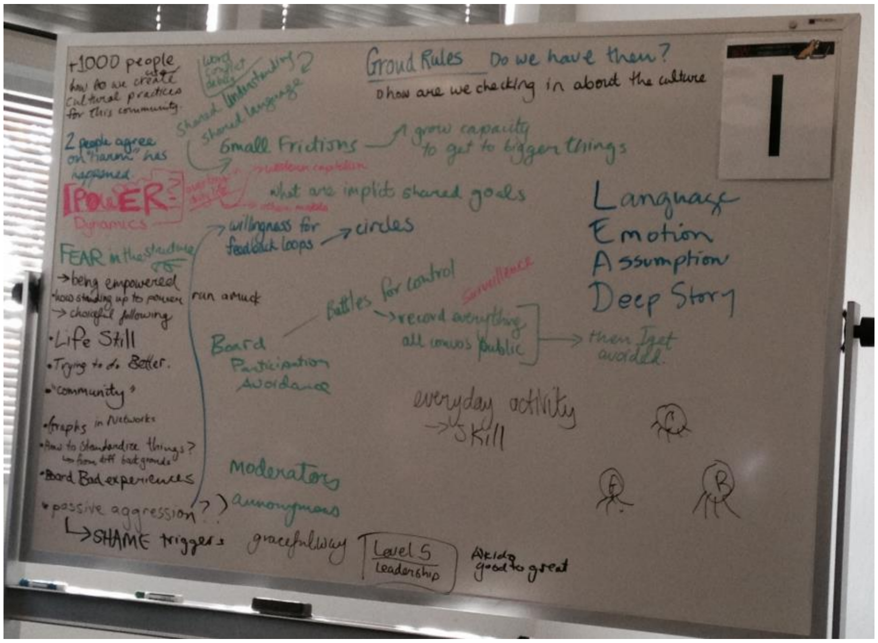
Systems & process / "Open & transparent Feedback loops"

Life skills are different for every person in how they historically address or don't address conflict as it arises.

Willingness - how is naming conflict and open dialogue around conflict a benefit? to the individual, to the community? Can the one benefit of wanting to continue participating in the IIW community be enough incentive to diffuse/address internal conflict(s) between community members.

Circles of harm: Premise is that each party to the conflict has in some way been harmed. Giver/Receiver, gradients of engagement = gradients of harm.

Community as a whole -- Be more resourceful about addressing conflict
Creative friction ~ Recognize there is a Power dynamic overlay of everyday life
Boundaries set as a group. Ground rules potential or at minimum a process to come together as a community to address conflict.



Mozilla Listens at IIW

Wednesday 5B
Convener: Kevin, Sean, Christopher, JB
Notes-taker(s): Chistopher Arnold

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

Sometimes people say "Bring back Persona" or other messages.
What can we do?

Erin, Ben- Known, a way to publish onto your own personal site.
They use Persona and they are working on Social API
We'd like to hear about Firefox OS.
We are making a platform on any device.

Google Identity team

Indiana University - Identity
Deann, Technical independent.
Ben-
Tom- Working on WebRTC and Together.js
Working on XDI infrastructure. Interested in Personal Clouds.
Brett - Femvote.us
Nittin- Customer Commons
Jeff - Paypal
David - Mobile Identity
Marc - Inventing the future
Andrew - Personal technologists.

Mobile - Firefox OS
JB- Doing an OS is the easiest way we could offer choice in emerging markets.
We can't address emerging markets with a browser that requires that you have a computer.
The operators see us creating choice for the user.

On Cloud
You've got your multiple platforms to ensure you have a coherent experience.

Ben - We want the APIs to be consistent across platforms.

JB - It's the web. We want the developer to build once and render on multiple formats.

Ben - You still need an app to upload video. Need to do compressed file types. Fantastic if you can do something there.

Marc - Mobile is cool. Blackphone was a secure phone. There are concerns about control and privacy. You could do a lot with a phone. This is in your ethos to address.

Sean - Verizon and AT&T control the layer.

JB - Our priorities are enabling access to the web for a large population.
Privacy focused device wasn't the initial objective.
However, DT is doing some initiatives to enhance privacy.
Wipe history, anonymity etc.
People can develop on top of it.

Katrina - What about Meeco?

Sean - Word. And I'll follow up on this.

Marc - you have a huge role to letting people control their data and experience.

Sean - We're doing an open source product.

Drummond - What's your view of personal clouds?

Sean - All we care about is making sure your phones are synced.
We have issues with the way data is used and abused.
Are we getting into the personal cloud business? Probably not our focus.
We can work on XDI standards etc.
We have intent-casting without a personal cloud. But we'd like to.

JB - We're taking the approach of Firefox Accounts. We're an aggregator of cloud services in.

Sean - The web should sync around you. We want to sync on my preferences layer.
You want to be in control of the implicit signal.
I want to be able to say when I don't want to see something.

Katarina - Lets' share something around that.

Sean - We'd like to help make personalization algorithms smarter.

Kevin - If you think about interest profiles, there's inbound signals where you can improve your interest graph. But there are also things you can plug in.

Sean - The question is "who decides?" We want the user to have that say.
All except for privacy.

Kevin - You can't have privacy without user control.
We shouldn't say what privacy is.
It's your data use it however you want.

Sean - URTB startups are also looking at these kinds of things.

Marc - In mobile interest space. Siri, Cortana, Google Now etc. What is UP going to do for mobile?

Sean - We tend to start from desktop. The browser shouldn't just be a window to the web, but also an agent for the user.

Marc - An outbound API might work for this.

JB - It's important to understand that we're a non-profit. We're a mission driven company. We think that products is just the best way to advance the web. If we do Siri or whatever, will that help the web?

Marc - How do you advance the web?

JB - For instance Subscribe to Web, we need to find a way to put content creators and the users closer together.

Marc - Traditional web is the web of pages. Now the web is humans with identity. The physical world is now addressable on the internet. The web is a broader notion than you're thinking.

JB - We have developed products that are access products. OS, browsers. Things that bring the web to the masses.
With content services we're trying to bring out questions of what is the web. Personalization, intent-casting, funding the web with S2W for instance.

Axil - is Apps included in the web?

Sean - We want mpesa for payments etc.

Axil - Do you have weight to do that?

Sean - We start off with desktop and we want to get there.

Axil - Would you do recommendations?

Kevin- We plan to.

Hyun - Might the browser get too heavy?

Kevin- the analysis is being done by machine learning. It needs to exist in the cloud. We have a cloud services team. But we're not sure how it's going to play out. Right now it's experimental. There has been a lot of interest.

Sean - We do a lot with extensions to start with.

Adrian- Six months ago we talked about exposing the secure element component so that other apps could use it. Apple has come out with an extensive taxonomy. So they've allowed revocation of access and lost credentials. You have pieces of these things. Is there an architecture that will evolve on the secure element?

Sean- I'll bring that up.

Brett - S2W is intriguing. I'd like to talk about a service for the soccer moms. There needs to be a forum on how this appeals to the individual.

Sean - It's a pilot just to test out the concept.

Marc - Firefox OS you can set a different terms of service around the user. In a personal data ecosystem. This could be a special attribute and differentiator.

Kevin- This is a matter of outbound signals.

Sean - We focus on only collecting data you need.

Marc - Let the user get a copy of their data.

Katrina - you can do that with Meeco.

Andrew - I remember the Knight Mozilla event in Germany. Many thought that Mozilla could give a single sign on.

Adrian - Apple doesn't control your identity. In this community we're going to see root identity. Legal sense of a persona and your other IDs and your F6 credentials are linked to it. You need to be able to terminate them from a central point to make consumers feel comfortable.

JB- How are you going to get market adoption?

Adrian- there could be regulation that push brokers or there needs to be some other way to do root ID. Not just a password store.

JB - How do you get someone to use this system? It's either regulatory. But it doesn't cover the full web. Or there is de-facto market adoption.

Adrian - you can enable a different identity tool.

Sean - But we didn't tell the users about that value when Mozilla did Persona.
We need to let people understand the importance of identity.

Threat Based Authentication

Wednesday 5C
Convener: David Waite
Notes-taker(s): David Waite

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

* Intro - a framework for thinking about authentication factors and the value they provide

* Initial scenario
  * All-encompassing system protecting both the website and a safe
Both might support an access code   Website might use location as an additional factor "he is accessing from a secure location"   Safe gets no value from that!

* Declaring specific authentication behavior and requirements based on a risk score means that you may make your score requirements when the authentication factors use do not protect against the threats you are concerned about

* Example Threats:
  * Session Initiation / Action
    - Phishing
    - Physical attack
    - Leaked credentials
    - Compromised Network

  * Session Hijacking
    - XSS
    - Sidejacking
    - fixation
    - Network vulnerability
    - Browser extension

* Constraining Attributes:
  - Local or Remote attack
  - Insider or Outsider-initiated attack
  - Funding level
  - Indiscriminate or Targeted attack
  - Personal knowledge or impersonal
  - Environment (browser app, native app, physical device)

Current work
* Evaluate threats and mitigations
  * binary value
  * evaluate behavior of attributes
    * new kind of threat? (phishing vs spearphishing)

  * distinction into two kinds of mitigation?

* Testbed
  * set up threat concerns
  * expose mitigations (password prompt, trusted location)
  * determine additional threats which may need to be mitigated

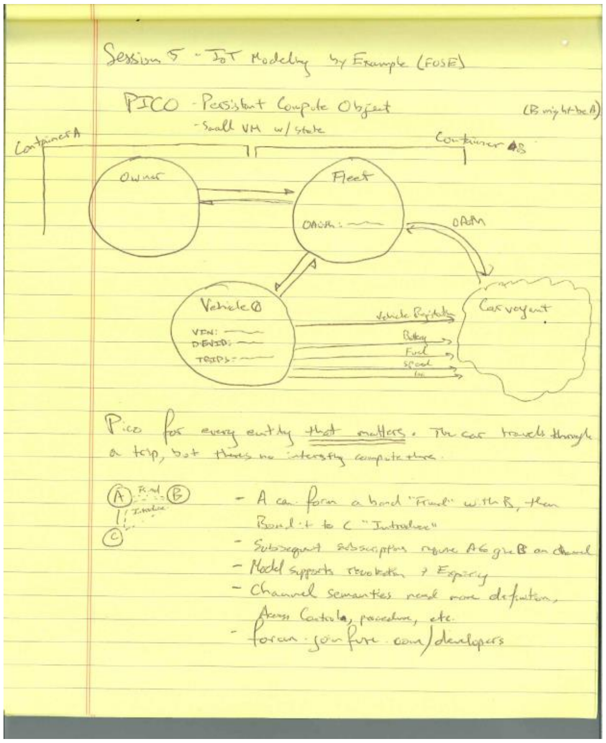
* Product Direction input
  * evaluate list of threats against mitigations provided by authentication mechanisms
  * take list of additional threats which have mitigations which we do not provide
  * prioritize based on customer needs (the threats they are concerned about)

IoT modeling with PICOs

Wednesday 5F
Convener: Phil
Notes-taker(s): Phil & Matt Berry (photo)

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

Link to blog discussing topic:
http://www.windley.com/archives/2014/10/fuse_with_two_owners.shtml
Link to below image: http://imgur.com/bMQ1LhW



Session 5 - IoT Modeling by Example (FUSE)

PICO - Persistent Compute Object
- Small VM w/ state

(B might be A)
Container A
Container AB
Owner
Fleet
OAUTH: ~~
OAUTH
Vehicle Ø
VIN: ~~
DEVID: ~~
TRIPS: ~~
Vehicle Registration
Battery
Fuel
Speed
Car voyant
A
Friend
B
Introduce
C

Pico for every entity that matters. The car travels through a trip, but theres no intersting compute there.

- A can form a bond "Friend" with B, then Bond it to C "Introduce"
- Subsequent subscriptions require A to give B on channel
- Model supports revokation & Expiry
- Channel semantics need more defintion, Access Controls, procedure, etc.
- forum.joinfuse.com/developers

Thursday October 30

UMA Demo

Thursday 1D
Convener: Maciej
Notes-taker(s): Matt Berry

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

http://www.cloudidentity.co.uk/services/user-managed-access

- Demo of UMA where B accesses A's data for Job Application
- RS sends data's identifiers to AZ
- RS pulls access control policies from AM
- Job site (RS) can discover data from PDS RS
- Receivers can request access to data asynchronous to data owner using RS
  - RS/AZ own process of notifying data owner about pending requests
- Does UMA support conditional policies?
  - No: language doesn't natively support it
  - Yes: scopes can be used to fake it "read", "read-if-ip-in-range-192.168.0.0/32"
- Does UMA support policies about data that doesn't yet exist
  - No
  - Drafts around Policies written for "types" of data are in progress

Microservices/Containers/Reactive Manifesto and Identity

Thursday 1F
Convener: Dave Sanford
Notes-taker(s): Dave Sanford

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

Dave Sanford started essentially by playing buzzword bingo by creating a list of related topics related to the software/system architecture that apparently many big Internet players have been using for some time, however more details are becoming well known:
- App containers
- Loosely coupled
- Message driven
- Elastic scaling
- Event driven
- Hybrid/Multi-presence (buy the base, rent the spike)
- Complex event processing
- Minimize required state

Dave then gave the rap that this is becoming more predominant within the industry, but also as the containers become more lightweight, micro-services can become smaller and this merges with the kinds of personal instances that this community is very interested in (Personal cloud, IoT, PICOs, PDS, ...)

Hugh Pyle (Qredo) discussed thinking of everything as streams, back pressure and viewing event streams as being pulled from the end rather than pushed through. Hugh described 'reactive systems' as primarily composed of a finite set of simple and composable primitives (map, filter, join, reduce, partition, ..) that interact with these flows. By making many of these actions as 'idempotent' there is less worry about the costs of maintaining state.

Discussions included how hadoop is batch oriented vs. Twitter's storm as being real-time.

Phil Windley showed slides and described the PICO architecture of Fuse as microservices and some of the advantages of that architecture.

Hugh also showed some reactive Java (RXJava?) code and how it provided that pull flow characteristics.

Finally we started talking about how Fuse uses OAuth and how that is probably a good model for managing the identity of microservices and authorizations in this space.

ARM mbed for IoT

Thursday 2C
Convener: Hannes
Notes-taker(s): Hannes

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

I gave a short presentation introducing tools and services offered by ARM for the Internet of Things space. The slides can be found here: http://www.tschofenig.priv.at/iiw/2014/ARM_mbed_HannesTschofenig.pptx

In addition to the slide deck I showed participants what resources to find at http://mbed.org (including the online IDE environment).

Qredo Rendezvous Protocol

Thursday 2H
Convener: Hugh Pyle
Notes-taker(s): Hugh Pyle

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

Qredo
Rendezvous, addressing, secure channel establishment
Protocol, key exchange
IoT

Qredo "Rendezvous" protocol. Currently the protocol isn't published anywhere. First delivery will be as part of the Qredo SDK and operator-hosted services. Open interop etc. is intended for the future.

It's a session-establishment protocol. Publish a name, into a global namespace; by responding to the name you open a secured communication channel with the publisher. Two-endpoint channels we call "conversations". The channel is unlinked from the rendezvous.

The rendezvous name ("tag") is any text string. It's kinda treated like a secret (only a KDF of the tag is transmitted on the network; the actual tag is to be communicated out-of-band from the publisher to the responder). Some rendezvous tags are long-term, stable identifiers, for multiple responders (each response will open a new channel). Example: publish billboard on Rte.101, or a BLE beacon, advertising a service. Some rendezvous uses are single-shot, where the first response also un-publishes the tag. Example: a single-use random-number rendezvous to be transmitted over NFC between two phones to start a chat conversation.

If the rendezvous tag is a public-key certificate, the publisher's identity can be challenged by the responder. (Alternatively just a public key, or a pk fingerprint).

The global namespace (in Qredo implementation) is a cloud-hosted, distributed, database-backed service; transport mechanics are HTTP or MQTT. The core protocol is lightweight enough that the namespace could just be done over UDP broadcast without any central resource.

Good discussions of the protocol – and use cases that led to it – and "application-level" uses, the role of unauthenticated channels vs authenticated-first channels.

Introduction to the Indieweb

Thursday 2I
Convener: Ben Werdmuller
Notes-taker(s): Ben Werdmuller

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:

We started by discussing the current state of the social web: most of us has multiple, separate profiles on various services. We illustrated, using *freemydata.co*, that many of them don't allow you to download your data.

The indieweb as a movement was founded following the federated social web summit, as a more open alternative that would concentrate on small, working solutions rather than conversations. It is based on three fundamental tenets, as described on *indiewebcamp.com*:

- *Your content is yours*: everything you post on the web should belong to you
- *You are better connected*: you shouldn't be penalized for owning your content - you should still be able to use the social platforms of your choice to reach your audiences
- *You are in control*: you can post anything you want, in any format you want, with no-one monitoring you.

The indieweb is tentpoled by events, IndieWebCamps, where web developers showcase what they've built on their own websites.

Over the last couple of years, the community has evolved a set of formats and protocols that turn the web into a full decentralized social network where each person's own website is their social profile.

These include:

Microformats 2 (microformats.org/wiki/microformats-2)
A simplified microformat specification that allows HTML to be marked up as a *profile, feed*, *post*, *reply*, *like*, *reshare*, *RSVP* and more. It's designed to be highly extensible; new standards evolve from real-life use.

Webmention (webmention.org)
A simple way to automatically notify any URL when you link to it on your own site. The *target* page checks the *source* and parses its microformatted HTML. If the source is marked up as a reply, for example, the target can republish it as a reply under the main content.

An extension called *vouch* mitigates spam by allowing webmentions to point to a trusted page that can vouch for its legitimacy.

IndieAuth (indieauthcom)
A method for using your own domain name for authentication, which is designed to make it as easy as possible to log in with your own website, without needing to implement complex standards like OpenID. A user's website points to their social profiles on third-party "silo" sites (like Twitter, GitHub, etc); when they log into a resource with their website URL, they may log in with those silo accounts (by using Twitter auth, etc).

Micropub (indiewebcamp.com/Micropub)
The simplest possible generic API for publishing to indieweb-compatible websites. Users authenticate to a third-party tool with IndieAuth. As part of this process, their micropub endpoint is discovered. The tool may then POST microformatted content to the endpoint in order to publish new content.

General principles: each of these can be implemented very quickly, and can work either as server-to-server protocols, or simply using web forms. By using the fundamental building blocks of the web, the barrier to entry is vastly lowered, and a greater variety of platforms may be built on top. The indieweb principles only work if they are implemented via a number of projects; monocultures are to be avoided.

A number of projects have emerged from the indieweb community. Most notably:

Known (withknown.com)
The first indieweb startup. Known gives you a single website for all your content. Users publish to their own site, and then syndicate their content to third-party sites like Twitter and Facebook (or software like Moodle or Sharepoint). A Pro version is available, and an integrated reader is forthcoming. Known's first market is higher education, where universities are giving each student their own domain and website, which allows them to keep their content throughout their university career.

Bridgy (brid.gy)
Bridgy acts as a bridge between "silo" sites like Twitter, Facebook, Google+ and Instagram, and webmentions. Users authenticate with brid.gy using their social media accounts; any activity on their posts is then converted to webmentions that operate on the source content on their own websites. Bridgy is commonly used with Known, WordPress, Tumblr and more.

The indieweb community shuns mailing lists, believing that they promote discussion over action. Instead, it has an active IRC channel (#indiewebcamp on freenode) that attempts to be welcoming to newcomers. Lurkers can observe on the live IRC website at *indiewebcamp.com/irc/today*.

It is a community in its infancy, growing fast, that is always looking for new participants.

Twitter in 2015: Twitter Listens to IIW

Thursday 3C
Convener: Mollie Vandor
Notes-taker(s): Matt Berry

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

What do you want to see us do visa vi account security, recovery, identity and privacy?

- Everyone attempts to strong arm Twitter into supporting OIDC.
- Their response is "auth is the bottom block in the Jenga tower"
- "Lots of the code is written, but not deployed"
- Justin says that if you have implemented OAuth 2.0, you're > 80% to OIDC

The REAL Internet of Things + I of T

Thursday 3F
Convener: Doc Searls & Bob Frankston
Notes-taker(s): Matt Berry

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

Summary: Wizards don't make points

- Good slide deck on the history of Home Automation
- "In Control" vs. "controls"
  - Being "in control" means there is an AI level
    Make it brighter -> blinds or lights or mirrors
  - Having a "control" means you can turn lights on or off.
- Not all IoT "things" work together
- They all report data back to a vendor, because there's no profit margin otherwise
- Technology doesn't have good enough AI for "In Control" yet
  - I walked onto the porch at night because I wanted to see the stars, but the AI turned on the porch lights so I could see the trash cans.

OAuth2 Scope Design Discussion

Thursday 4E
Convener: Eve Maler & Ajanta Adhikari
Notes-taker(s): Eve Maler

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

There are opportunities around OAuth scope and UMA scope interoperability.

There are user experience needs for standardized scope semantics.

In the near future, can we expect more standardized scopes because of more interoperable ways to convey them between resource servers and authorization servers?

Look at the SAML example; there are some standardizable attribute categories derived from regulations. These could map to reusable scopes.

OAuth is a framework, not a protocol; scopes come from the application level, not the OAuth level. Said another way, OAuth is a security mechanism for APIs, and doesn't say anything about the semantics of those APIs vs. its own semantics.

A useful concept Akamai uses is internal vs. external scopes, with token chaining -- not a tree but a set. Akamai re-maps scopes when resource locations change. Public (application/external) scopes are essentially part of the API.

We see authorization policy getting more complex! This seems to indicate a use case for UMA resource set registration vs. just plain single-level scopes.

It's always possible to define "flat" scopes that have infiormal relationships between them, a la the Salesforce scopes example. When is it valuable to make these relationships machine-readable? On-the-fly composition is the right rationale for structured scopes and/or resource sets. Google uses "+" for composition, e.g. "login+mail" (or similar). Standardizing such syntax could be valuable.

(Aside: "Access" vs. "delegation" is something UMA folks should discuss. Along with scopes, there's the question of passing the right identity to the resource server in the API call.)

VRM + CRM Part 3

Thursday 4F
Convener: Nitin
Notes-taker(s): Joe Andrieu

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

Capabilities Matrix http://bit.ly/vrmGrid

An invitation to do a VRM Journey Mapping from Nitin Badjatia http://designingcx.com/

Online Voting

Thursday 5D
Convener: Andrew Jennings
Notes-taker(s): Andrew Jennings

Tags for the session - technology discussed/ideas considered:

Voting, Democracy, Security

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

Reference Brad Templeton’s writings on electronic voting.

Described California’s existing system. Works pretty well, despite the flaws.

Reference the Coursera course on electronic voting.

Preserve the secret ballot.
- How do you do mail-in ballot and still have secret ballot?

Estonia has online voting.

Secret ballot:
- Employer might require you to vote in a certain way.
- Oregon requires mail-in ballot.

But these attacks don't work that well on paper because they don't scale.

What do we need from identity to have better voting?
- Better authentication with the voting authorities

Even with cryptography.
- Can make voting anonymous
- Can make voting verifiable
- The coercion problem still remains

Can vote on one compromised machine and verify with another compromised machine.

Steve says you'll always need to deliver the anonymous token physically because it can't be received on a compromised computer.

Morten talks about hand-count audit of ballots. Just need to hand count a random sample. Have to number the ballots and record how they voted as you count the ballots. (They should be identical when they go in the ballot box.) Then you choose some random numbers and make sure those ballots are counted correctly.

Andrew thinks we'll be voting online within 20 years. It will be forced upon us even if it's not secure. Steve thinks we won't be voting online in 20 years.

Bill says there is a significant problem in some cultural segments with coercion. I will take all the mail-in ballots and everyone will sign them, then I will fill them out and send them in.

Morten says in Denmark the ballot counting is all by hand.

Bill thinks the whole US will not have online voting in 20 years. But there will be a county somewhere that tries it.

Mark says psychologically, people won't accept elections without paper trail.

Morten recommends the book "Broken Ballots: Will Your Vote Count" by Douglas W. Jones and Barbara Simons.

You need to identify your goals. If those are met by the paper ballot, then make everything around it electronic, but keep the paper ballot.

Branding VRM for Consumers, and Developers

Thursday 5F
Convener: Micah MC
Notes-taker(s): Micah MC

Tags for the session - technology discussed/ideas considered:

VRM, Social Networking consumer's developers

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

- calendar + contacts were the killer consumer apps
- affinity vs direct advertising. Internet in not apt at affinity
- sustainability
- Ads have shaped culture. Ad tech has not
- Own (much larger) vs buy
- Millennials, Millennials, Millennials…

The Second IIW Women’s Wednesday Breakfast

We had many new faces at this IIW including quite a few women - at the close of Tuesday's circle Kaliya invited the women to connect over breakfast Wednesday morning. We filled a whole table and continued a new tradition at IIW.

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 80 distinct sessions called and held ~ we received notes and/ or white board shots for 60 of these sessions. Thanks to those of you who submitted notes and information!

Demo Hour

1. **CynjaSpace:** Heather Dahl, Chase Cunningham, Les Chasen, Gary Zimmerman
   URL: www.thecynja.com/
   At The Cynja, we empower kids to be safe online with our comic series. We're a multi-platform media firm teaching kids, and their parents, about technology. Join us as we take you into CynjaSpace! Check out our portl, specifically designed for kids to go online in a safe and private way

2. **SitePassword:** Ala Karp
   URL: https://sitepassword.parseapp.com
   Tired of trying to remember your passwords? Worried about storing them even if they're encrypted? Then calculate them! Use SitePassword because it makes your life easier. The fact that it makes you safer is secondary.

3. **Showing the Economic Benefit of Identity Federation**: David Simonsen
   URL: http://www.wayf.dk/en/media/projects/403
   Based on real time usage statistics of the federation and integration cost estimates, it is possible to present a highly dynamic view of the economic 'life' of the Danish identity federation WAYF - Where Are You From (some 160 services and 160 identity providers connected).

4. **Mozilla - Firefox Interest Dashboard:** Kevin Ghim - Sr. Product Manager, User Personalization, Firefox
   URL: TBD - Firefox Add-on
   The barrier to true personalization is based on an outdated belief that targeting can derive relevance signals and create useful audience segments. The Firefox Interest Dashboard's goal is to redefine personalization through transparency, user consent and control through visualizations, interest category editing and personal data portability.

5. **"Digital Credentials for Education and Professional Licensing"** : Eric Korb CEO, Accreditrust.com
   URL: https://www.accreditrust.com/truecred-framework
   Accreditrust is building a secure credentialing platform for the education and professional licensing sectors. We are extending the Open Web Platform to support trustworthy digital credentials which can be used to prove who you are on the Web. We'll talk a bit about our work on the Identity Credentials specification in the W3C Web Payments and Credentials Community Groups and demonstrate issuing, curating, and verifying digital credentials using technologies that we intend to shepherd through the W3C standardization process.

6. **Known**: Ben Werdmuller and Erin Jo Richey
URL: http://withknown.com
Publish media, notes and ideas to a site that you control, and syndicate it to social networks and collaboration software. Known works in any browser, is easy to use, and is easy to extend. Open source with enterprise licenses available.

7. **passQi LLC, passQi app**: David Eyes
URL: www.passqi.com
Bridges password and device authentication; Stores account credentials in your phone, securely "tethers" to any browser ad hoc, anonymously. Securely (AES) relays passwords to automate login. No cloud or replicated storage of passwords, automates two step verification (TOTP).

8. **IDLocker identity validation website:** Andrew Jennings
URL: http://idlocker.org
IDLocker will be a non-profit organization that validates individual identity and certifies it to other organizations without revealing

9. **PRIVO Lock Consent Management Platform & MyPRIVO Service Directory:** Steven Greenberg & Denise Tayloe
URL: http://www.PRIVO.com
For online services that want to collect and use personally identifiable information about minors, PRIVO offers an affordable, easy-to-implement platform that obtain verified adult consent and allows them to comply with COPPA requirements.

10. **Meeko Life Management Platform:** Katryn Dow - Founder & CEO
URL: https://Meeco.me BLOG: https://blog.meeco.me
Create an accurate picture of your life, intentions & digital behaviour. Have the power to own, capture & share your personal data. Manage life on your terms, gain insight, be informed to make better decisions & be rewarded for being you.

11. **CloMoSo Infused Identity - "Tracking and Securing Bread Crumbs":** Zachary Taylor & Kirk Brown
URL: https://www.netiq.com/products/cloudaccess/resources
https://www.netiq.com/products/sentinel/resources
How can we infuse identity "into our bread crumbs" when we leave the perceived security of our own cloud and track them into the unknowns of mobile and other cloud computing environments? How is better security obtained?

12. **OpenID Connect in AWS:** Zihang Pu, Matt Berry, Shon Shah
How to use Cognito to build a sample AWS-powered app that uses an OIDC identity provider. The JavaScript app allows users to sign in using their Salesforce user names and passwords and enables them to access data stored in an Amazon DynamoDB table.

13. **Personal Microservices:** Hugh Pyle, Qredo Ltd
Using the Qredo SDK to build personal data applications using a private network of services.

14. **Political Identity Protection:** Britt Blaser
URL: https://newgov.us/ ; http://SNAPvote14.com
In politics as in no other market area, customers (constituents) must be protected from each other’s visceral resentment. To wield political influence is the goal of most engaged customers, but politics REQUIRES a wholesale loss of privacy.

15. **Freedom Box Danube Edition:** Markus Sabadello
    URL: www.ProjectDanube.org
    I will present a prototype of the FreedomBox, containing about 10 different functions for better control over personal identity and data, and for a more free, more private, and decentralized Internet.

16. **FIDO U2F Security Key:** Stina Ehrensvard, John Haggard, Yubico
    URL www.yubico.com/security-key
    Merging open authentication standard, supported in Chrome and Gmail, enabling one secure hardware device to securely access any number of services, respecting your privacy.

17. **Lexii:** Kevin Seba
    Lexii is a trusted brand engagement and loyalty platform where VRM and CRM meet

IIW XIX #19 Photo’s by Doc & Nat

Here are links to Doc and Nat’s photos of IIW 19 ~

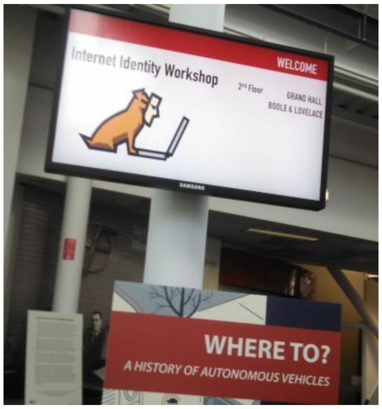
Doc Day 2
https://www.flickr.com/photos/docsearls/sets/72157649038374401

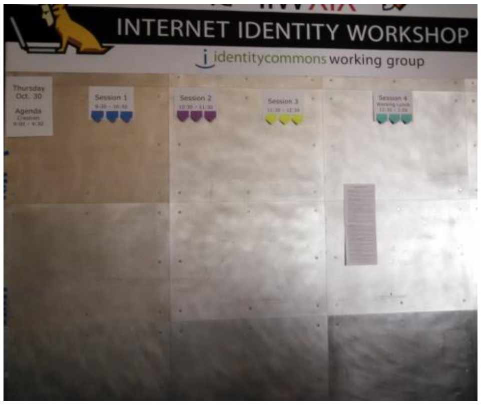
Doc Day 3
https://www.flickr.com/photos/docsearls/sets/72157648763552917

Nat
https://www.flickr.com/photos/_nat/sets/72157646842694254/

Photo’s taken and provided by:

Steve Wilson, Doc Searls, Phil Windley, Nat Sakimura and Heidi Nobantu Saul





See you April 7 – 9, 2015
for

IIW XX

The 20th Internet Identity Workshop

www.InternetIdentityWorkshop.com