

**IIWXXI**

INTERNET IDENTITY WORKSHOP 21

identitycommons working group



## *Book of Proceedings*

[www.internetidentityworkshop.com](http://www.internetidentityworkshop.com)

Collected & Compiled by  
KAS NETLER, HEIDI N SAUL AND BRADFORD WINDLEY

Notes in this book can also be found online at  
[http://iiw.idcommons.net/IIW\\_21\\_Notes](http://iiw.idcommons.net/IIW_21_Notes)



**October 27, 28, 29 2015**  
Computer History Museum  
Mountain View, CA

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



## Content

|   |           |
|---|-----------|
| About IIW .....   | 3         |
| At IIW .....  | 4         |
| IIW 21 Session Topics .....   | 5         |
| <b>Tuesday October 27</b> .....   | <b>9</b>  |
| Heart & iGov .....  | 9         |
| Finding Customers for VRM .....   | 13        |
| SCIM is Done Intro & Q&A .....  | 15        |
| Basics of Blockchain.....   | 16        |
| Mobile Connect/MODRNA WG Overview/Update .....                                      | 18        |
| Identity Broker Pattern: 15 Fundamentals .....                                      | 19        |
| Questions: Why JWT? SAML vs OAUTH vs JWT.....                                       | 20        |
| Open ID Logout .....  | 21        |
| Registry Directory ~ based on BlockChain that is ROOTless and NOT Centralized ..... | 23        |
| HIE of One .....  | 24        |
| Fast Modular Exponentiation in Javascript for Cryptographic Authentication.....     | 25        |
| OIDC vs. SAML What are you missing and how do you solve it? .....                   | 25        |
| User-Managed Access (UMA) Intro & News.....   | 27        |
| Thinking in Crypto: #RebootingWebOfTrust .....                                      | 28        |
| Azure AD integration in Windows 10.....   | 29        |
| An Identity Rocku-mentary .....   | 31        |
| OIDC OP Testing - Hands On .....  | 32        |
| Introduction to Consent Receipts .....  | 32        |
| XDI and Semantic Dictionaries.....  | 33        |
| Is OIDC+OAUTH2+UMA complete? What about SAML2+ID-WSF2+XACML? .....                  | 34        |
| Burning Bridges and Breaking Brokers.....   | 36        |
| Consent receipts in UMA .....   | 37        |
| SCIM InterOp Discussion .....   | 39        |
| Potential Roles for Blockchain in Identity .....                                    | 39        |
| The Personal Learning Environment .....   | 41        |
| <b>Wednesday October 28</b> .....   | <b>43</b> |
| Vectors of Trust .....  | 43        |
| Re-delegation and Revocation with OAuth 2 .....                                     | 44        |
| International Perspectives .....  | 45        |
| BlockChain Use Case: (not bitcoin, not identity centric) Distributed Ledgers .....  | 46        |

|   |     |
|---|-----|
| Identity Film .....   | 47  |
| OpenID Connect Certification: the view from the trenches.....                       | 49  |
| Non-Person Entities .....   | 51  |
| Multi-Protocol, end2end Trust Assured Frameworks for Personal Data Ecosystems ..... | 53  |
| Decentralized Directories/Registry (using Blockchain) .....                         | 55  |
| Ethereum: a general purpose BlockChain.....   | 55  |
| Beyond Ad Blocking .....  | 57  |
| Selective Disclosure .....  | 58  |
| Post Password World .....   | 59  |
| Trust ~ Elevation with UMA and Connect .....  | 61  |
| U2F Update.....   | 61  |
| Blockchain Auth: Passwords login w/blockchain using JSON web tokens .....           | 65  |
| Book Preview: OAuth 2 in Action.....  | 66  |
| Citizen Data Schema .....   | 66  |
| Blockchain & UMA: Two Great Tastes ...Do they go together? .....                    | 67  |
| Societies of Things .....   | 68  |
| OpenID Connect RP Certification Hands-On .....                                      | 70  |
| Who Cares About Our Personal Data? Mapping Innovations and Showing the way... ..    | 71  |
| SCIM Credential Management Discussion.....  | 73  |
| Forbidden Knowledge.....  | 74  |
| Non-Person Entities .....   | 75  |
| UMA: Interop Testing, ARP Use Case .....  | 77  |
| Cradle to Grave.....  | 77  |
| What Does “Log Out” Mean? .....   | 79  |
| Security Loft .....   | 80  |
| Citizen ID Cards: white paper concepts/good designs .....                           | 81  |
| Thursday October 29.....  | 82  |
| The Permanent Web .....   | 82  |
| ABAC - Attributed Based Access Control .....  | 82  |
| Digital Identity 2nd Edition / Non-Person Entities.....                             | 84  |
| OTTO Private BlockChain Help .....  | 87  |
| The Cultural Barriers to Privacy.....   | 88  |
| Is Identity Always On.....  | 88  |
| Blockchain Governance.....  | 90  |
| Customer Funding .....  | 91  |
| OIDC Federation for Higher Ed .....   | 92  |
| Beyoncé as a Service.....   | 93  |
| Cradle to Grave.....  | 94  |
| What Does “Log Out” Mean? .....   | 95  |
| What’s Next for IIW .....   | 97  |
| Thank You to All the Fabulous Notes-takers!.....                                    | 98  |
| Demo Hour .....   | 99  |
| IIWXX #21 Photos by Doc .....   | 101 |
| Thank You to digi.me .....  | 102 |
| Thank you to our IIWXXI Sponsors.....   | 103 |

## About IIW

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

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

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

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

The event is now in its 11th year and is Co-produced by Kaliya Hamlin, Phil Windley and Heidi Nobantu Saul. IIWXXI (#22) will be April 26 - 28, 2016 in Mountain View, California at the Computer History Museum. Super Early Bird registration is open now at: <https://iiw22.eventbrite.com>

IIW Events would not be possible without the community that gathers or the sponsors that make the gathering feasible. Sponsors of IIWXXI (#21) were:

|   |   |  |                                       |
|---|---|--|---------------------------------------|
| <b>Microsoft</b><br>Conference Dinner                 | <b>Google</b><br>Welcome Dinner                     | <b>Mozilla Foundation</b><br>Tables & Power, Welcome Reception | <b>Nexus Group</b><br>Barista         |
| <b>Gigya</b><br>BBQ Lunch                             | <b>ForgeRock</b><br>Projectors                      | <b>VMWare</b><br>Mexican Lunch                                 | <b>Covisint</b><br>Lightening Demos   |
| <b>SailPoint Technologies</b><br>Conference Reception |   | <b>AVG</b><br>Morning Breaks                                   | <b>WSO2</b><br>Afternoon Break        |
| <b>Janrain</b><br>Morning Break                       | <b>digi.me</b><br>Doc Center and Open Space Gifting | <b>Identity.com</b><br>Open Space Gifting                      | <b>Welcomer</b><br>Open Space Gifting |

If you are interested in becoming a sponsor or know of anyone who might be please contact Phil Windley at [Phil@windley.org](mailto:Phil@windley.org) for event and sponsorship information.



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

Eve Maler

VP Innovation & Emerging Technology -  
ForgeRock



At IIW ...



Thanks  
to our

S  
P  
O  
N  
S  
O  
R  
S



We go out  
to dinner  
together  
at the  
end of the  
day...



...so the  
conversations  
can continue  
in a casual  
setting



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

Stina Ehrensvar  
CEO & Founder of Yubico



## IIW 21 Session Topics

**Tuesday October 27, 2015**

### **Session 1**

- 1A/HEART & iGov
- 1C/Finding Customers for VRM Products
- 1E/SCIM is Done - Intro Q&A
- 1F/Basics of Blockchains
- 1G/Mobile Launch of MODRNA - Overview/Update
- 1H/Identity Broker Pattern - 15 Fundamentals
- 1K/Questions: Why JWT? SAML vs OAuth vs JWT

### **Session 2**

- 2A/Open ID Connect Logout Mechanisms Progress + Status
- 2C/A Registry Directory ~ based on BLOCKCHAIN that is ROOTless & NOT Centralized
- 2E/HIE of ONE Personal UMA Authorization Server Project
- 2F/myTERMS User-Asserted Terms (Mozilla + Customer Commons + Others)
- 2G/Fast Modular Exponentiation in JavaScript for Cryptographic Authentication
- 2H/OIDC vs SAML - What are you missing & how do you solve that?

### **Session 3**

- 3A/User-Managed Access (UMA) Intro & News
- 3C/Attribute Privacy in Federated Model
- 3D/What is the Impact of the Blockchain Technology to the PKI base eID Schemes?
- 3F/Thinking in Crypto..... #Rebooting Web of Trust
- 3G/Azure AD Integration in Windows 10 - What does it mean to have a orgID Cloud Identity
- 3H/An IDENTITY Rocku-Mentry ? A documentary about the past, present + future of Identity in the IIW Community
- 3J/OIDC OP Testing - hands on

### **Session 4**

- 4A/Defining Consent - Collecting Personal Information with Notia Consent Receipts
- 4D/XDI (Extensible Data Interchange) and Semantic Dictionaries (an update on XDI Core I.O and XDI.org)
- 4F/OAuth 2.0 for Native Apps (draft IETF best practice) NEW!
- 4G/Making Money from Grassroots, Distributed ID Platforms (???)
- 4H/Is OpenID Connect + OAuth + UMA Complete? Why Should I switch from SAML + ID-WSF2 + Xacml?

## 4I/Burning Bridges and Breaking Brokers

### Session 5

5A/Consent Receipts in UMA

5C/SCIM Interop Discussion

5F/XDI Registry Working Group - a rootless, decentralized, lookup service empowering the personal data ecosystem (based on the bitcoin blockchain)

5G/Potential Roles for BLOCKCHAIN in Identity

5H/Personal Learning Environments (Domain of One's Own, LMS, etc...)

5J/AAD in Windows 10 (Part 2 from 3G) Now that I'm Joined...



**Wednesday October 28, 2015**

### Session 1

1A/[Vectors of Trust]

1C/ Re-Delegation and Revocation with OAuth

1D/International Perspectives

1E/BlockChain Use Cases (not Bitcoin, not identity centric) & Distributed Ledgers?

1F/Identity Film - Brings IIW & Core Topics to Life...

1G/Account Chooser Working Group

1H/Open ID Connect Certification: The news from the trenches - Google

1I/Non-Person Entities - Delegation, Proxy and WS02, API manager

### Session 2

2A/Multi-Protocol Frameworks for Personal Data Ecosystems

2C/Decentralized Directories/Registry (using blockchain)

2D/Dynamic Client Registration Security Issues

2E/Ethereum a general purpose BlockChain

2F/Next Steps after Ad Blocking (200 million votes for what?)

2G/Selective Disclosure - "I'm older than 18, you don't need my birthdate" Principles, Open Questions

2J/Post Password World - How do we get there? BRING IDEAS!

### Session 3

3A/Trust - EI - AKA "Stepped-up Authentication" with UMA and Connect

3C/U2F Update - including mobile, passwordless, and more...

3D/Blockchain Auth: Passwordless login with the Blockchain using JSON web tokens

3E/Delivering Oauth Tokens to Things (or NAPPs 2.0)



3F/Book Preview! OAuth2 in Action  
3G/Citizen Data Schema - SCIM, IWTs, OIDC/Interoperability of National eIO programs  
3J/BlockChain & UMA - Two Great Tastes... Do They Go Together?

#### **Session 4**

4A/RISC - Sharing Security Events among Service Providers  
4C/Societies of Things  
4D/OIDC RP testing - Hands On  
4E/ Personal Data Ecosystem Consortium (PDEC) Who cares about our personal data? Mapping Innovations and showing the way...  
4F/XDI Registry Working Group (Mtg #2 of 2) More "Pumpkin Theater"  
4G/Forbidden Knowledge - Genomes, Facebook, and other High Dimensional Data  
4H/SCIM Credential Mgmt Discussion  
4I/Identity Proofing - Can it be done well? Especially Remotely?  
4J/Speed Demo Reprise

#### **Session 5**

5A/IoT Privacy and Personal Data  
5C/UMA - Interop testing, ARP use case  
5D/HELP! Federated Profile Across the Autodesk Knowledge Network - Ideas? Standards? Architectures? Suggestions?  
5E/Thinking in Crypto - Signing JSON ?What are your best practices?  
5F/Thought Experiment: What if sites opeted-IN to USERS? (DNT + TPS + Uses Submitted Tags)  
5G/Privacy from Cradle to Grave "What is the effective consent?"  
5H/What Does "LogOUT" mean?  
5J/Security LOFT - A volunteer organization promoting modern APP Security Standards!  
5K/BlockStore: Scalable Secure Storage with the Blockchain  
5L/Exploring Possibilities for Citizen ID Cards - A whitepaper re: core concepts/good designs



**Thursday October 29, 2015**

#### **Session 1**

1A/The Permanent Web  
1G/ABAC - Attributed Based Access Control  
1H/First Experiences with the Estonian e-Residency ID

#### **Session 2**

2D/How will Current and Legacy ID Specs [SAML,OIDC, OAuth...] Interact and/or be Replaced by BlockChain Technologies?



2G/Help Phil outline Digital Identity 2<sup>nd</sup> Edition  
2H/OTTO - Private BlockChain HELP

### **Session 3**

3A/ The CULTURAL Barriers to Privacy  
3G/IDENTITY - Is it always "On"? and Who should control the switch?  
3H/BlockChain 'Governance'

### **Session 4 / Working Lunch**

4C/Mozilla Listens to IIW  
4F/All Things Photography  
4G/Customer Funding  
4H/OIDC Federation for Higher Ed

### **Session 5**

5A/Beyonce as a Service  
5F/What Next for IIW?



*"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

## Tuesday October 27

### Heart & iGov

#### Tuesday 1A

Convener: Justin Richer, Paul Grassi, Debbie Bucci

Notes-taker(s): John Fontana

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

Two new protocols at the OpenID Foundation ~ HEART and iGov

Heart is in health care patient centered use cases. Patient controls consent

iGov is working in gov. sector, citizen facing. - Justin is involved in both efforts.

- there is some commonality but differences in the end goal
- where do we align things are some of the questions
- want to make what we do in Heart does not conflict with what we do in iGov, unless we make a conscious effort to split things.

I want it to be impossible for a dev to stand up a server at say IDP that is both heart compliant and iGov complaint – they should at very least be compatible not directly conflict with each other . they should use lot of same constructs and requirements, they should be able to cross reference at tech spec level.

Heart has draft protocols on the book now. Some things pulled from other places like Argonaut.

iGov just getting spun up– not a shell of a profile yet. Taking in legacy GSA profiles. There is X-509 PKI stuff, saml and info card profile.

blue button protocol from a few years ago fed in t HEART.

Green button fed into iGov. notion of clear button, pull out common aspects/ principles, there is some type of underlying structure here we might be able to get down to.

For HEart, we have 5 profiles planned for HEART - there are two profiles planned for iGov one for OIDC and Oauth

HEART set high bar for baseline security and interop got rid of shared secrets, in heart all authN is based on asymmetric key pairs. Not x509 key pairs – that does not work. Using openID style infrastructure less PKI.

using RSA key pairs are currently mandated. All based on JOSE, you can do elliptical curve, RSA two flavors,

baseline interop,, proposing RS256 Jose method of sigs, be mandatory to implement. There is widespread support for this, crypto libraries and Jose libraries.

the other point, this is not intro to heart session

other big piece of Heart security profiles beyond, is interoperability.

you have to publish the discovery end point. this is basic way to draw lines in sand to say this is what this is what needs to exist for people to more easily work together.

Mandating token introspection to enabling resource server with authZ server to work together. Mandate tokens issued are all signed JSON web tokens....Want them to be applicable across many deployments.

Q: brokered or not brokered – is there issue with discovery not turned on? NO

the other half of this is dynamic client registration, we have soft recommendation to enable for both oAuth AS and Idp

makes a lot of sense in Heart case, .....may also make sense for gov side, but have to properly define context.

Heart. mandate dynamic client reg,, but we have a bit of text that says you can decide scopes, types of clients. We many have stronger recommendations.

Justin: what is end state of the thing you are trying to do with this?

High level requirements

Paul: selfishly we want these two profiles to have baseline security and interop and be in both, without having bunch of having gov use cases yet, I look at this at a peer to our saml profile. So baseline security , privacy interop profiles and by the way, cross border use cases and we get to interop immediately.

you have hit on some of the other policy and technical hurdles., the time it takes to implement saml is ridiculous. We have some interesting attribute fundamentals that could be rationalized.

Talk about threat models.....

High level requirements

Heart ....Argonaut

Debbie: in beginning we had interop, if you did Argo and did Heart – there was no interop. It took lot of strain to get Argo to recognize H and vice versa. Now that we are adding iGov, we don't want to do that interop issue again. We want to avoid this

Justin: that is what we want IIW 15, to get out of this here.

argonaut providers are just getting to understanding oAuth, they are struggling, they are doing username password. But we think this is a more secure connection.

difference here is iGov does not exist yet. it is being set up and standard building group to define how people interop in this space.

that is different from Heart and Argonaut, ie, picking names and values.

iGov is almost a clean slate. But lot of legacy profiles and attribute bundles that are established. Heart is codifying what is already running

in Heart, setting things up so we have OAuth 2. Profile... says if you are doing OAuth, this is what you have to do. on top of that is OIDC profile... it extends OAuth stuff. UMA is on top of OIDC – inherits from both of these; we have some FHIR scopes in use here and the last profile is FHIR UMA...

this is all built so you can break it apart – the FHIR side is health care specific on iGov side core it is OIDC profile, it is about enduser ID and authN. Authz and policy management wrap nicely around this and it can all work together.

Question to OIHF is what can we do so we can minimize the drift between Heart and iGov?

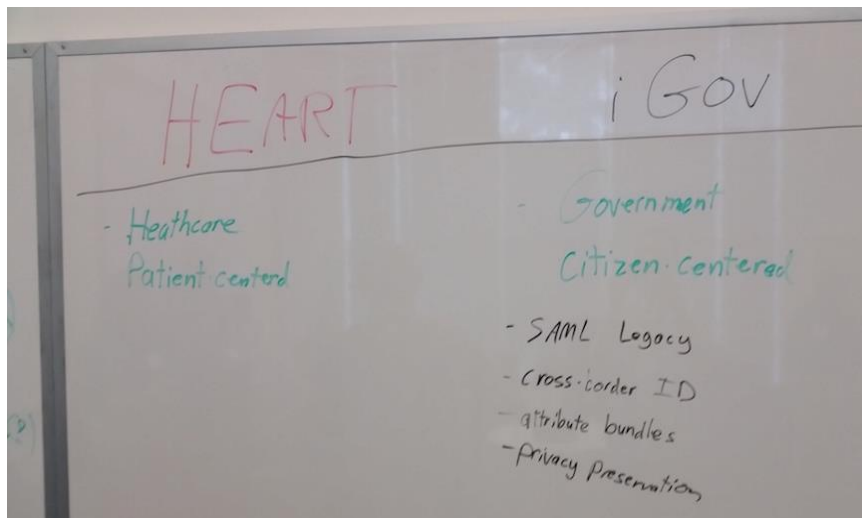
how much of this belongs in iGov and how much in Heart and can there be a neutral third party to do the basics.

proposal for moving forward. - Justin Richer

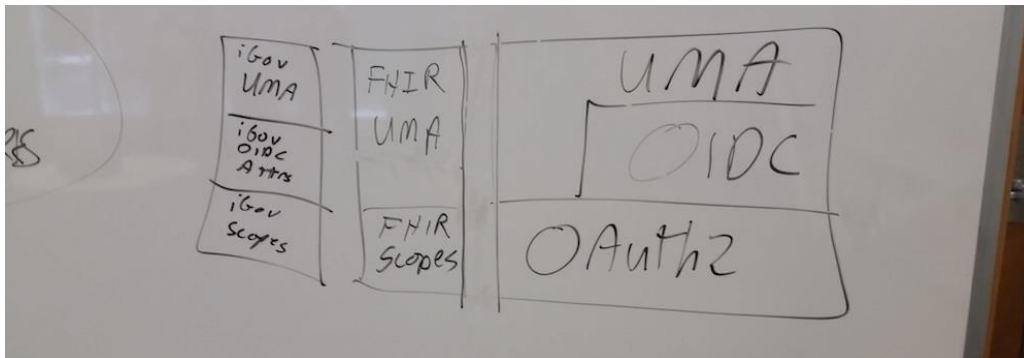
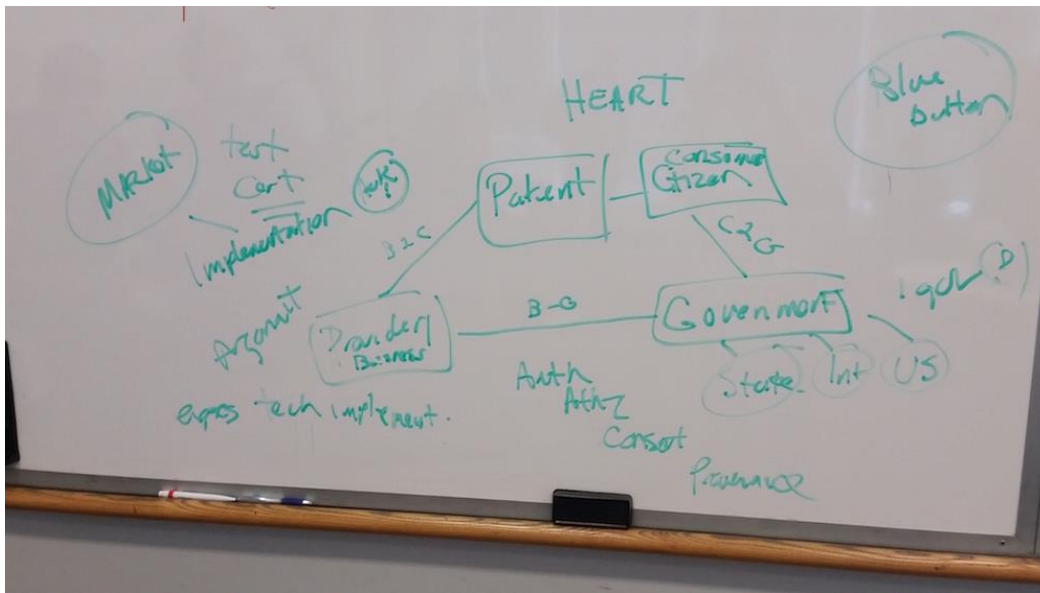
As iGov starts we make an explicit motion in iGov to refer to the Heart security profiles as the baseline and build on those – do that to start.

If it makes more sense for Heart give that up ownership of those and have iGov work on those, we can make that move. If it makes more sense to converge, hope we don't come to that, we can make that decision when we get there

Paul: I second, iGov has not had the international conversation. I hope common sense prevails.







## ***Finding Customers for VRM***

**Tuesday Day 1C**

**Convener:** Kevin Cox

**Notes-taker(s):** Ben Werdmuller

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

One of the most important things is to practice your pitch, on a regular basis, to people outside your space, in order to refine your value proposition.

In VRM at the moment, there's only one sort of customer: the organizations. Individuals are not going to buy at the stage the space is in right now. When organizations have bought in, individuals might.

Organizations will pay, and have the best, most useful data already. They want the personal data they hold to be private. Personal data is closely tied to an organization's bottom line: it is their business. Without it, they're out of business.

Personal data involved in an organization's business is not just the individual's: it's also jointly owned with the business. Both parties can have their own terms for use of that data, which are mutually agreed upon.

Does it work? Yes. Two examples:

Edentiti - Started to make money in late 2008, and is profitable today. Individuals gather information about their own relationships with other entities, and ask those entities to prove that those relationships are valid. Once individuals have done that, they can prove that all their relationships are valid - and can give the result of this process to an organization, who trusts the process and now can trust the individual. Doc Searls says this is called "attestation". Edentiti got into the business by screen scraping third party organization websites in order to prove relationships, which organizations themselves were not prepared to do.

Yodlee - Provides a similar mechanism for proving relationships and identity by screen scraping bank data.

Screen scraping is not a good idea: it violates the principle of jointly agreed terms, and is an unsafe business.

Bridging the dark web might work. Here, you set up an interface to prove relationships with dark web vendors. This is inherently risky for other reasons.

And of course, you can OCR hard copies and PDFs of identity / bank documents.

But: If you give users a view of all their data, and let them make their own connections as part of an easy-to-use dashboard, then the vendor can also see all their organizational data. (Does this violate the personal data ownership principles of VRM?)

When some immigrants enter the country, they have trouble getting credit cards, because they don't have other credit cards to cross-reference with. Banks are interested in mutually sharing information about individuals with the government (eg the immigration department). By creating a public

dashboard, and giving the individual the ability to give permission for this information to take place, the individual effectively becomes their own data broker. However, because this is of value to the bank, they effectively become a customer of the VRM vendor.

WelcomeAboard is one such data dashboard.

Connections are made by content not identity. Pieces of information are syndicated; organizations keep control of the data, as they have liability for leakages. Similar to Digime and Known. Links are made between the copies and the original (again, similar to Known). They're not connected to the central user identity: the data is permanently linked to its other copies.

Communications are made with messages, not sessions. The Internet was meant to work with messages, not circuits. This makes the network more easily scalable.

Access control is set via the applications, not the data. The data is different in different contexts, which are dictated by the applications.

You don't need complicated data structures. Keep it simple. (Similar to the indieweb approach.)

Why do it this way? Kevin says:

- Organizations will buy.
- You don't need to make giant changes to existing changes - small pieces are loosely bound.
- It's more scalable.
- Doesn't require collaboration or agreement with multiple organizations.
- Can potentially fit in with work being done by all VRM companies.
- It's 100% distributed.
- It removes most perceived legal problems with VRM, because it removes ownership questions, and clarifies ownership.
- It works best if it's not proprietary.
- Customers will fund it.

This model gives identity to any thing. And a single model can fit all things. It's simple - in the same way that the indieweb technologies are simple. Applications for specific contexts sit on top of the platform that the model provides. "This gives us a way to put a prefrontal context on the Internet of things!"

You can charge for open source software based on reputation. Banks want to be assured that software they're installing is good software by their definitions: so you sell the most trusted implementation, which happens to be open source. (Known is dubious about this, having found that users confuse "free as in speech" and "free as in beer".)

If you want to sell, the group pointed out, you need to start with the "why". Show people why they should care. Tell them succinctly. Create prototypes, get feedback, and iterate. That's the main way you will get customers: make something that solves a real problem that people will pay for a solution to.

## **SCIM is Done Intro & Q&A**

**Tuesday 1E**

**Convener:** Kelly Grizzle

**Notes-taker(s):** Susan Carevic

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

SCIM, Provisioning, Deprovisioning, Protocols

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

SCIM: System Cross Domain Identity Management

Basics: Take REST and combine with Identity. 2 major portions:

1. Protocol: create/search/read/update
2. Define Schemas: data types/define objects within server (Resource types). Extensibility
  - a. Out of box: User and Group resource types

Origins: 5 years ago, desire to create standard for identity management\SCIM is complete as of September 2015!! Given 3 RSCs:

1. Use case document 7642
2. 7643: Schemas: data types, how to define types, what a user and group is (Standards Track)
3. 7644: protocol document – how to use REST protocol (Standards Track)

Essence: cross-domain concept is what makes it interesting, as opposed to LDAP.

HTTP/HTTPS: historically way to get to web//LDAP on cloud – a lot of non-standard things need to be done for this to work.

SCIM: design principles: needed a schema model that had the core attributes everyone uses. Each domain is going to have completely different requirements. If I provision to your companies website, no need to rewrite my client. I can shove data to you, and you take what you need. Eliminates rigidity of XML format.

SCIM rules: generally favor service provider: Let server decide what it wants to do in favor of making the client's life easier

Use cases:

Provisioning to multiple systems at same time/deprovisioning

Identity: What is a Cross domain identity: Federated Identity: lots of systems don't work with federated identities, they need their own. Its having that same identity spread out across multiple systems. Each application tracks its users through its own set of identities. Each app will have certain set of information that app needs to function.. nothing to do with security functions it accepts.

SCIM: provides a common interaction mechanism for access to and management of heterogeneous identity environments.

Experience: We provision everyone into Google, BOX, O365, Amazon. Google and O365 don't have SCIM interfaces. This is a matter of time.



For many people, they can't build until someone is provisioned. Incentive to have provisioning end point. Acceptance of protocols: need incentive

SCIM: What can you do (high level)

Client initiated. Client = Consumer of a service provider like (IDP). Piece of software running on behalf of the thing that manages the identity for a user (Http clients/services).

Example:

Cloud Provider: such as Salesforce, Webex, PING, ... (uses SCIM)

## ***Basics of Blockchain***

**Tuesday 1F**

**Convener:** Muneeb Ali

**Notes-taker(s):** Dave Sanford

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

Slides:

<http://blog.onename.com/experiences-with-scaling-blockchain-based-data-stores/>

Muneeb (from OneName) started the session with presentation: 'Building Global PKI with Blockchain'. Bitcoin solves distributed consensus without relying on trusted party. Unconfirmed transactions are made and then they become confirmed. Data needs to be synched with the distributed ledger – by attaining agreement on the state of the system. Blockchain solves this problem – by giving everyone (who wants it) a copy of the file – therefore there is the same state for everyone. It acts as a peer-to-peer network which periodically (approximately every 10 minutes) decides what can get added to the file.

Who has the authority to write to this file? Bitcoin miners are trying to solve a hard problem. Whoever solves the problem – which defines the new block.

Incentives: People are incentivized to do work on the longest chain. Some discussions of 'proof of work' as well as 'proof of state'.

There are now approximately 21 million bitcoins. Every block generates new bitcoins for miners until (projected) approximately the year 2140. There are also transaction fees, the intent is that transaction fees will provide enough incentive after 2140 to incentivize continued mining – given the volume of transactions at that time. As soon as you mine a block – there is a high incentive to advertise. When there are competing blocks in the systems – some blocks may need to be erased, so some entities wait until up to 6 new blocks before they view a transaction as validated by the final consensus block.

The hash of the public key acts as a bitcoin address. Bitcoin uses ECDSA with the SECP 256K1 cipher. The only way to prove that your transaction has been validated is to go to the validated block and confirm. Full broadcast nodes talk to each other and do transactions and each block contains transactions. The hash of the last block is computed using a nonce value to meet a certain criteria (e.g. starts with 5 zeros, requiring 6 zeros would be even harder). This hardness factor is designed to cause

new blocks to be validated approximately every 10 minutes. Every two weeks hardness is re-evaluated based on the time validation took over the previous two weeks. The current block size is 1MB which equates to approximately 4,000 transactions/block.

The question was asked how much of this material is specific to the bitcoin blockchain vs. other blockchain? It was agreed that much of this discussion is about the bitcoin blockchain – in part because many types of non-bitcoin transactions can be built on top of it and that it is so large that compromising it would be very very hard. There was some discussion of the ‘group leader election problem’ and the ability of blockchain to ‘establish truth’, which could be extendable to PKI and other areas. Some questions – not answered about alternate chains and their alternative incentive structures.

For the user, sending a transaction is very simple – just sign and send to a bitcoin address, which means that you need to be able to ask for someone’s bitcoin address. The ledger is currently only 40GB and a full copy of it is only needed by full nodes (but is available to everyone). A key is only used for a single transaction – so the use of ECDSA does not represent a forward security vulnerability.

If you have to wait for six new blocks for sufficient validation of a transaction – does this impact the ability to support real time operations? The answer is yes, which is one of the things that some of the alt chains are trying to address.

Currently there are approximately 5300 full nodes, My (light node) wallet only needs to know its own transactions.

From a high level blockchain is doing two things:

- 1) Creating a validated time sequence (block 1, 2, 3 ...) and approximate time (6 blocks ~ 1 hour)
- 2) Ownership with private keys – bitcoins are just one thing for which ownership can be established – any digital asset, names, data, code – can have its ownership proven

Namecoin is a forked blockchain, which provided decentralized DNS, OneName have now implemented the same functionality on top of the bitcoin blockchain – primarily because there were too few entities and miners involved with namecoin making it not as inherently secure as the bitcoin blockchain. For naming – you register a hash of your name, if you subsequently reveal the hash as being a hash of your public name, ownership is hard to contest. This hash is stored in a 40 byte op return field in the bitcoin transaction – and can be thought of as a \$0 bitcoin transaction. For the name service, there are still transaction fees.

Side chains were too advanced for this discussion.

We use block chain for consensus – you could imagine different federated (more centralized) systems that still allow auditing. These systems could have ban periods or arbiters (EFF, ICANN, ..).

Bitcoin blockchain is powerful and secure because of network effects, there is so much infrastructure invested by such a diverse group. In a federated system, you might not need the overhead of mining. Can notarize the data in blockchain and store the data elsewhere.

## **Mobile Connect/MODRNA WG Overview/Update**

**Tuesday 1G**

**Convener:** Torsten Lodderstedt

**Notes-taker(s):** Sebastian Ebling

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

OpenID Connect, Mobile Connect, MODRNA

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

\* Torsten explains involved parties (SP = Service Provider, OP = OpenID Provider -> in this case Mobile Network Operator (MNO), Authenticator = SIM based Authentication on a mobile device

\* MODRNA is an OpenID working group that standardizes discovery, registration, and authentication with Mobile Network Operators

\* Q: is it a browser flow

\*\* A: it depends. Most operators implement OpenID Connect code flow

Challenges the WG is going to cope with:

1) finding the op

2) registration

3) controll authentication process

\* Finding the OP is a challenge

\*\* OpenID is based on E-Mail Addresses

\*\* Phone number in case of Mobile Connect

\* RP register once and establish a trust relation ship

Q: Why do you think this will work

A: Phone-based authentication is already in place. For example Whatsapp, SMS OTPs as 2nd factor. Utilizing the SIM card could improve authentication and UX.

Q: Why should individuals trust Mobile Network Providers?

A: Survey results indicate people (at least in some regions) trust operators more then other players.

I: Changing MNO is a problem when identity is locked to the MNO

A: PPIDs have to be portable across operators

I: You are still locked to have a mobile contract with a provider that supports Mobile Connect

I: Checking if PPIDs can moved can be part of the process of onboarding to a new operator

\* People identify with Applications an Devices not with SIM card. See Apple Pay, Facebook. Identity is connected to

Apps/Devices.

Q: Device or number: What are we more attached to?

Q: Who creates the demand for MC?

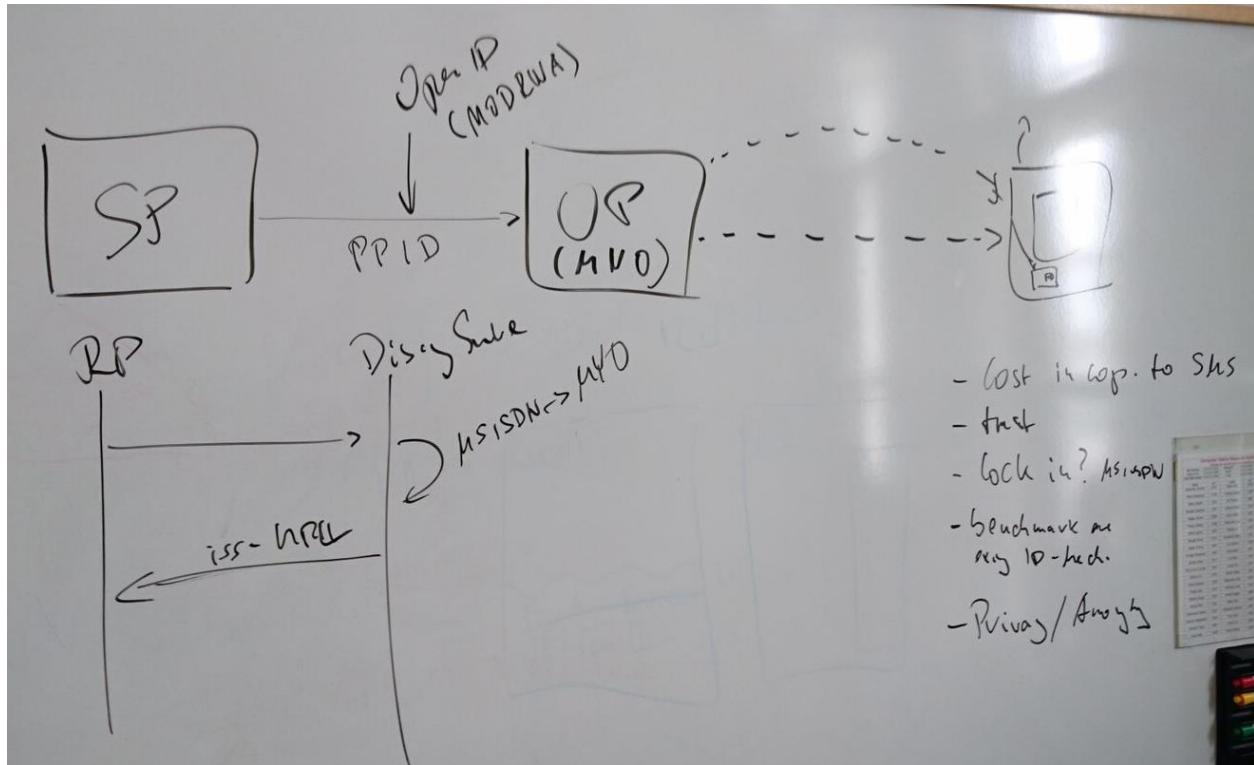
A: GSMA thought this is a good idea. MNO already have validated information about you and want to become identity. There is demand from the market.

Is there interest from the SP side?

A: Google likes the idea of getting rid of SMS and participate in validated information. Simpler recovery.

A:

Torsten shows the flow:



\* What happens when you have no mobile connection (travel/roaming)?

\* What happens if I lose my device? Can I lock everything in one step?

\* What should be the first service providers use that service?

\*\* Insurance companies

\*\* Banking / commerce -> financial transactions

## Identity Broker Pattern: 15 Fundamentals

Tuesday 1H

Convener: Prabath Siriwardena

Notes-taker(s): Prabath Siriwardena

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

### 1. Motivation

- Gartner predicts by 2020, 60% of all digital identities interacting with enterprises will come from external identity providers.



- b. The need to integrate legacy IAM systems with standard based ones rises.
  - c. Overcome anti-patterns
    - i. Spaghetti Identity
    - ii. Federation Silos
2. 15 fundamentals
- FEDERATION PROTOCOL AGNOSTIC
  - a. TRANSPORT PROTOCOL AGNOSTIC
  - b. AUTHENTICATION PROTOCOL AGNOSTIC
  - c. CLAIM TRANSFORMATION
  - d. HOME REALM DISCOVERY
  - e. MULTI-OPTION AUTHENTICATION
  - f. MULTI-STEP AUTHENTICATION
  - g. ADAPTIVE AUTHENTICATION
  - h. IDENTITY MAPPING
  - i. MULTIPLE ATTRIBUTE STORES
  - j. JUST-IN-TIME PROVISIONING
  - k. MANAGE IDENTITY RELATIONSHIPS
  - l. TRUST BROKERING
  - m. CENTRALIZED ACCESS CONTROL
  - n. CENTRALIZED MONITORING

### **Questions: Why JWT? SAML vs OAUTH vs JWT**

**Tuesday 1K**

**Convener:** Venkata Tadepalli

**Notes-taker(s):** Venkata Tadepalli

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

1. JWT and SAML are two different formats of getting assertions from Identity Provider (IdP)
2. OAUTH is an authorization protocol used for delegated access; here the Service Provider (SP) issues the access token and refresh tokens. These tokens can be issued in JWT format
3. SP is not required to verify the JWT in the following Use Case;
  - a. If the ServiceA has received the JWT from IDP and is not intended to delegate any access to 3<sup>rd</sup> party service
  - b. And the JWT has sufficient claims that needed for the ServiceA to process the request
  - c. And the ServiceA can verify the JWT signature with the help of the public key (if the JWT comes with public key)

## Open ID Logout

Tuesday 2A

Convener: Mike Jones

Notes-taker(s): Mike Schwartz

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

Unlike the other parts of the OpenID Connect specification, logout is still in flux. There are three different approaches: session management, front channel (passing logout via browser), and back channel (passing directly to RP).

The mechanisms we are discussing are for the OpenID Connect provider to communicate to the RP's that a logout event happened--i.e. Single Logout (SLO).

Front Channel is easy to implement, via POST or an iFrame HTTP method, and perform logout in browser. Problem is that its not a reliable communication channel--what if the logout never actually occurred. Closing the browser used to do the job, but now that doesn't work in many cases.

Back Channel can be more reliable, but its much harder to implement. For example, at EIC a financial trading firm mentioned a use case where an iFrame is used to provide a single experience for a future trading site. This user needs to make sure you are logged out of both the trading firm, and the backend future trading site.

Session Management using an OP iFrame inside every RP website, and counts on the fact that the OP knows when the session script changed. Other javascript asks the OP iFrame if the user logs out. Its ok to poll frequently, because its just a inter-browser communication. There was resistance to adding Javascript to each page. Also, there was problems with the RP not getting the javascript running if the tab was closed, although you would be logged out properly if you were to return to the site.

-----  
----- Back Channel Logout Discussion -----  
-----

Logout token is similar to an id\_token, but has extra claims: jti, logout\_only, and sid (session id). Also its prohibited to put a nonce in a logout token. The idea is that you should never be able to confuse an id\_token with a logout\_token. SID is used to refine the scope of the logout to one session.

Back channel works for native apps. IDP may want to put a cookie to register the device on first use.

Tokens are supposed to be one-time use. You post it...

1) Discovery Values:

Can OP support it  
Optional feature: backend\_logout\_session\_required  
Identifier from the OP for the RP to use for that session.

-----  
----- Front Channel Logout Discussion -----  
-----

You have a URI that the RP registers at registration time--this is the location of the iFrame that if rendered, will log me out. Clear cookies, and change html5 local state. The reason why its an iFrame (v. img tag), is that in an iFrame you can invoke futher down logouts.

You may have a logout button at your RP or at your OP. The identity provider could provide a special button to enable the RP to signal a global logout. Its up to the IDP to decide what kind of UI the IDP wants to provide.

This approach was used not too successfully with SAML, but its the best compromise.

-----  
Is session identifier required?

In some cases, you may want an opaque identifier, by putting a session identifier in the id\_token, and to pass that session identifier as a param on the logout URI. IDP may not act on the logout unless the session id matches.

This session identifier may have different characteristics than previously specified. In this case, its not signed, its a bearer secret.

RP initiated Logout message has a state value which can be sent by the RP in the host\_logout\_redirect\_uri as a param. The OP should pass this back to the RP.

There is a misalignment between the enterprise and consumer markets. In the consumer world, the goal is to obfuscate your identity from the RP. In the enterprise world, there are security compliance issues. Also in the consumer space, families using shared devices may need to switch identities.

There is an open issue in the OpenID Working Group to Create a document describing the "single logout" semantics, and use cases.

## ***Registry Directory ~ based on BlockChain that is ROOTless and NOT Centralized***

**Tuesday 2C**

**Convener:** Lionel Wolberger

**Notes-taker(s):** Lionel Wolberger & Dave Sanford

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

The XDI Registry working group presented, in general terms, it's implantation of a registry on the bitcoin blockchain.

Discussion:

- \* names v numbers: by focusing on numbers (UUIDS type 4) we avoid semantic, intellectual property, and other issues
- \* discussed proofs of ownership and proofs of existence
- \* full and partial blockchain
- \* the role of blockstore

Dave's notes:

The XDI working group has put together a proposal that will support a decentralized and rootless registry – based on mapping a Universal Unique Identifier (UUID) to an endpoint. UUIDs are 128 bit values and in this case it is a Version 4 (random number). The endpoint might be identity data, personal data, etc.

Discovery of end-points is similar to the DNS system mapping a URI to an IP address. We want to be able to put this mapping function into a blockchain to get the shared, decentralized ledger (e.g. bitcoin blockchain) benefits.

Ethereum is also robust and has a big community. XDI.org has a Registry Working Group charter and proposal at this type.

Once you have the endpoint data (personal identity, business, etc.) and pointer mechanisms – what you get from blockchain combined with the XDI overlay:

- 1) Proof of ownership
- 2) Proof of 'continued' existence (e.g. vs. brand new account)
- 3) Escrow services – key recovery and/or replacement

The XDI group looked at Elinor Ostrom's 8 Principles for Managing A Commons as a basis for some mechanisms. XDI requires a look up service, but that requirement is generic. This proposal provides a specific proposal using the bitcoin blockchain to do that lookup.

Revocation exists, but does not erase a record of the past. First item in the ledger may say A = B, a later revocation entry in the ledger indicates that A no longer equals B – however a record of the period in which it was valid stays in the blockchain record.

One of the purposes is to enable decentralized economic incentive model – that will support the continued existence of the model and its goals – but it could use other methods of proof of existence.



Goals include:

- Endpoint via IRLs
- Proof of ownership, multiple types of proof
- Owner digital signing of last change request
- Proof of existence
- Who are the trusted registrars (and their proofs)
- Recovery – this is just secondary proof of ownership
- Quality of registry response

At this point the XDI committee is trying to keep this discovery proposal not specific to identity discovery and leave identity attributes abstract – potential endpoints (e.g. blob, token, assertions). Mainly the intent is to enable XDI based graph discovery.

The bitcoin blockchain is immutable, but allows mutable transactions to be built on top of it – still allowing everything to be auditable, because of the layer below.

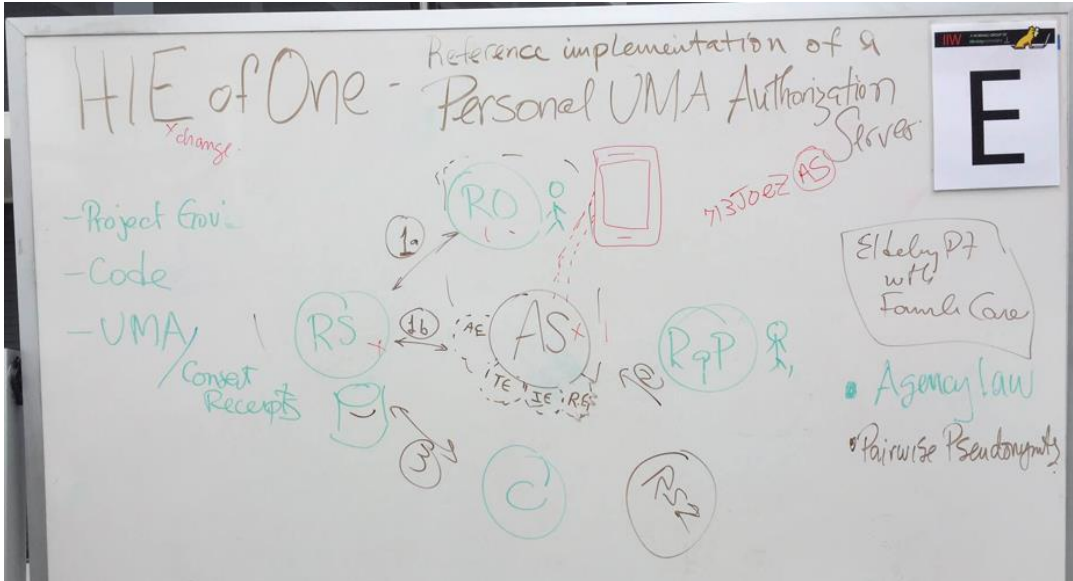
## HIE of One

## Tuesday 2E

**Convener:** Adrian Gropper

**Notes-taker(s):** Adrian Gropper

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



Facilitating UMA adoption using super-simple Agency Law as the strategy and an open source reference implementation of the UMA authorization server as the tactic. The reference implementation at [github/hioefone](https://github.com/hioefone) is in pace and anyone that wants to monitor or contribute this project should join or just contact me directly as [agroppe@healthurl.com](mailto:agroppe@healthurl.com)

## ***Fast Modular Exponentiation in Javascript for Cryptographic Authentication***

**Tuesday 2G**

**Convener:** Francisco Corella and Karen Lewison

**Notes-taker(s):** Karen Lewison

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

Authentication, cryptography, Javascript, big integer library

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

This session covered the material in the blog and attached slides from the presentation at: <http://pomcor.com/2015/10/25/faster-modular-exponentiation-in-javascript/>

## ***OIDC vs. SAML What are you missing and how do you solve it?***

**Tuesday 2H**

**Convener:** Mark Dobrinic

**Notes-taker(s):** Yuri Hirohashi

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

Both meant to solve the same problem  
Open ID connect was meant to make things simple  
SAML known for making things complex :)

SAML has a lot of solutions already  
Open ID you may encounter problems along the way

OIDC ID token has a very limited amount of definitions  
Name ID contains many more specifications

Interested in having a mechanism in

Univ. of Michigan's experience:  
A lot of times SPs, especially commercial are pulling attributes  
Wants name ID but they don't honor definitions  
Persistent ID is supposed to be opaque

On campus students gets TV access, but not off campus - is this person entitled? Problem is trying to identify where a given student lives

U of Michigan started SAML, which has slow adoption.  
OIDC faster adoption. Everyone with Google account has OIDC.  
Google consumes SAML but does not produce SAML

People would rather work with Json or XML?

Writing PHP or ruby code is easier then web server configuration

Linking identity ~ To integrate OIDC in SAML world ~ Federated logins

Need to figure out configuration and management of SAML and OIDC easier for people

iSELECT is another standard in Netherland

Don't change protocol unless you need to, if it is working

OIDC is suitable for application integration

SAML Installation experience is easier

Have you operated SAML and Open ID simultaneously? Issuing ID token and assertion? - Not yet. Using SAML but looking into Open ID

Account chooser. Local storage ~ Discovery by email ~ IDP does not prompt you for email  
Just type in credential

Open ID foundation is the governing body for the spec. Not going to solve a problem if it is for one person.

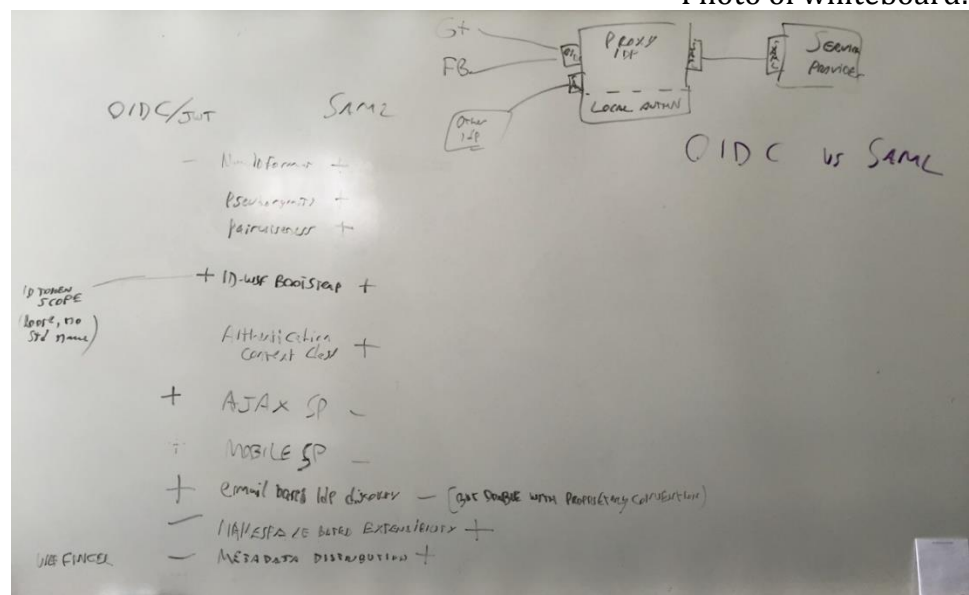
SAML - Oasis

If people have problems in Open ID, let's try to have a consistent approach to solving those. Not individually. Let's stay connected.

Want the trust of open ID connect

Meta data to be signed by federation.

Photo of whiteboard:



## ***User-Managed Access (UMA) Intro & News***

**Tuesday 3A**

**Convener:** Eve Maler, Judith Bush

**Notes-taker(s):** Eve Maler

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

User Managed Access, Working of Group of Kantara.

1.0 is released. 1.01 is in development.

- User Managed Access, builds on OAuth
- The concept of a person controlling access to their data and information.
- OAuth2 has much of the UMQA architecture in place.
- UMA contributes to a relationship of trust.
- Privacy is:
  - o Context – The right moment to make the decision to share
  - o Control – The ability to share just the right amount....
  - o Choice – True ability to say no and to change one's mind....
  - o Respect – Regard for one's wishes and perspectives
- BLT – Business Legal Technical
  - o BLT – Bourbon Lemon Tonic ☺
- Business Case of Bob, a web site operator, is in the slides
- Privacy goals vs. reality
- Transparency and controls
- Aspiration vs. risk mitigation
- Digital consent - Taking UMA from concept to reality
- Post compliance consent tools only take us so far
- An IAPP salary survey from two years ago identified that the Privacy Professional reports up to the Legal function in many companies, so interests are not necessarily aligned with people who are interacting with the business
- Smart TVs – Samsung – sending voice to a third party... nuanced communications, fear....
- UMA has a Legal subgroup now....
  - o Impose a promise on embargo on data for time or a purpose of use
- Uma is trying to make the hard way easier....
- Proactive sharing - delegation to others use case
- A “Share” button
- The new Venn of access control and consent
  - o OIDX
  - o OAUTH
  - o UMA
- Ran through an example of connecting your Fidelity account to your Tax account
  - o Authorize your tax accountant to see your Fidelity account.
- Ran through a “view my paycheck service”
  - o A pending request to extend it.
- Delegation is more important than permission
- Once you release data, it is out there

Raw audio file of session here:

<https://www.dropbox.com/s/cqyn4eczaerjrw8/Voice%20009.m4a?dl=0>

Introduction to UMA page:

<http://kantarainitiative.org/confluence/display/uma/Introduction+to+UMA>

UMA Implementations page:

<http://kantarainitiative.org/confluence/display/uma/UMA+Implementations>

UMA Case Studies page:

<http://kantarainitiative.org/confluence/display/uma/Case+Studies>

UMA Developer Resources WG page:

<http://kantarainitiative.org/confluence/display/umadev/Home>

UMA V1.0.1 Public Review draft specs (review closes Monday Nov 2):

[https://docs.kantarainitiative.org/uma/draft-uma-core-v1\\_0\\_1.html](https://docs.kantarainitiative.org/uma/draft-uma-core-v1_0_1.html)

[https://docs.kantarainitiative.org/uma/draft-oauth-resource-reg-v1\\_0\\_1.html](https://docs.kantarainitiative.org/uma/draft-oauth-resource-reg-v1_0_1.html)

Release notes for UMA V1.0.1:

<http://kantarainitiative.org/confluence/display/uma/UMA+Release+Notes>

## ***Thinking in Crypto: #RebootingWebOfTrust***

**Tuesday 3F**

**Convener:** Christopher Allen

**Notes-taker(s):** Christopher Allen

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

We walked through the advance readings for next weeks #RebootingWebOfTrust, posted on Github at <https://github.com/WebOfTrustInfo/rebooting-the-web-of-trust/tree/master/topics-and-advance-readings>



## ***Azure AD integration in Windows 10***

**Tuesday, 3G & 5J**

**Convener:** Vicky Milton

**Notes-taker(s):** Susan Carevic

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

Notes for Tuesday 3G and 5J

- What has Microsoft done in Windows 10:
- Who owns this PC?
- Windows Account Types:
- Administrator or Standard User
- Windows 8: More types of accounts:
- Local: can be converted to a MSA account. Can also be decoupled.

Microsoft account (MSA) : Cloud account. Uses OAuth, Open IDConnect, Cloud Identity, password management in cloud, but can be synced locally. Microsoft is the identity provider. Consumer account for Microsoft apps.

Domain Account (AD) : Comes with AD. Organizational identity. Off the box trust authority for windows in general. Centralized management, gets tokens from AD, uses Kerberos.

Azure AD Account (AAD): built to support O365  
(No guest account)

With windows 10,integrated AAD account with AD.

Tenant: small business customer: business relationship and their name space (Domain Name).

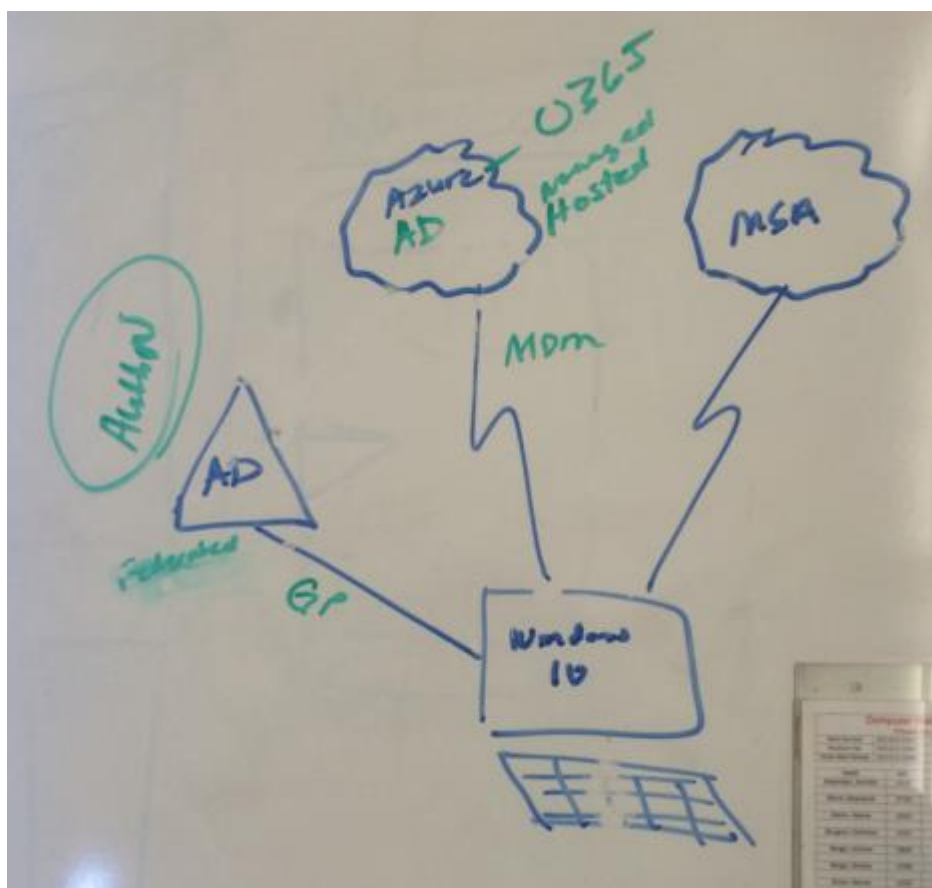
In Federated world, Azure AD would still use AD for token by using federation. Joining is a device concept.

Domain Account can not coexist with Azure AD account.

MDM: used to centrally manage devices. Big vendors of this use AD Azure directory.

Can't use group policy on an AAD, what permissions override?

Windows 10 only supports one MDM instance per device. Windows team looking at layering MDM.. most strictest policy will win.



AAD integrates into the operating system.. no shadow account:

- Treated more like AD as MSA, so that a corporation has control over its identities.
- Wanted to enable new provisioning models: could we provision with my identity? Could this be brought to corporations?
- When you buy a new machine and login with Windows 10 professional. AAD – it will download all corporate policies without corporations doing a thing.
  - Open up new computer with Win10 pro: asked “who owns this PC”?
    - Letting user buy an enterprise device: does this device belong to you or your organization?
      - Question doesn’t come up with Windows Enterprise, only on Professional version
    - Let’s you join a domain
    - Enter work account email : when this is done, computer asks in Azure AD if the organization is the tenant, otherwise redirected on prem.
      - If tenant found, passes org information down to machine, passes down branded ICON. If Azure AD is federated, AAD asks the computer to go to ADFS for credentials. User will be taken to sign-in page for organization. Person redirected to organization’s logon page.
        - Otherwise user enters password to join Azure.
      - Once authenticated into organization, Token added to device
      - Azure adds token to MDM server of organization and displaces Terms and Conditions (Ts and Cs) for Organization: This is “the

cliff", once you do this, your device is managed. User can unjoin if they made a mistake.

- User Accepts: device registered, policies laid down, MDM enrolls device.

- Whole flow is web driven, so that it can be changed.

Does Win 10 allow you to use something other than a password? Yes, but need a password too. Users are used to seeing a password field. Users understand two fields together, even though we know we want to get rid of passwords.

Federates with AD, will it federate with other IDPs beyond ADFS? - yes it does, but no other service provider can be the core IDP.

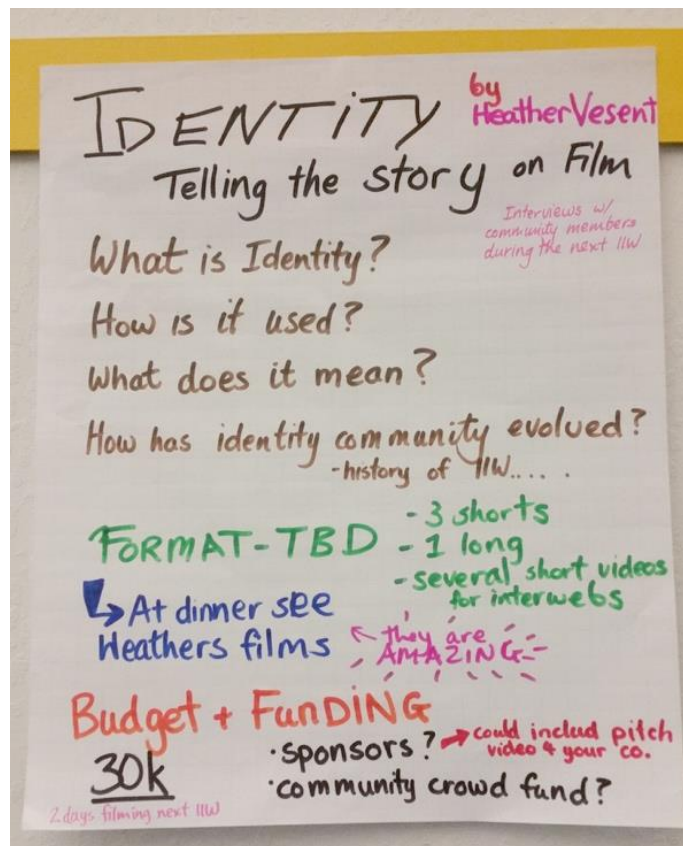
## **An Identity Rocku-mentary**

Tuesday 3H

Convener: Heather Vescent

Notes-taker(s): Heather Vescent

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



## ***OIDC OP Testing - Hands On***

**Tuesday 3J**

**Convener:** Roland Hedberg

**Notes-taker(s):** Roland Hedberg

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

Only a very limited number of people appeared.

All of which already had used the test tool and was convinced of its usability.

So, we only had a short talk about related topics, one of which became a session on Wednesday, and then called it a day.

## ***Introduction to Consent Receipts***

**Tuesday 4A**

**Convener:** John Wunderlich

**Notes-taker(s):** John Wunderlich

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

Introduction to the Minimum Viable Consent Receipt:



**Introduction to the MVCR.pdf**

Consent Receipt Demo:



**IIW\_MVCR\_Demo.pdf**

Notes to accompany John's slides/presentation:

- A company has a privacy policy to mitigate its risk. A Consent Receipt gives some power to the user.
- There is no informed consent for some kinds of data
- Consent Receipt gives teeth to consumer to say you do what you said you would do.
- If you "de-id" personal data properly, it is no longer personal data.
- There is a Github repository you can look at....
- This is more of a policy than a technical issue
- Sarah Squire has written an example consent receipt generator with an API, to be completed as a web form....
- This control gives a regulator the ability to go to a party... and say, show me the record.
  - A signed JSON object is utilized.
- Now there is clean data, positively consented; consent means good data
  - Big data is largely bad data, unconsented and randomly collected
- Consent is an audit and trust tool.

## *XDI and Semantic Dictionaries*

Tuesday 4D

Convener: Drummond Reed

Notes-taker(s): Drummond Reed

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

This session, given by Drummond Reed and Markus Sabadello, co-chairs of the the [OASIS XDI Technical Committee](#), was in 3 parts.

In the first part, Drummond covered an update on the status of XDI Core 1.0, the foundational specification for XDI (Extensible Data Interchange), under development for the last 11 years.

The update was that XDI Core 1.0 is finally finished and currently in ballot to become a Committee Specification Draft (technically the vote has already passed, but formally it closes on Thursday morning Oct 29). The link to the draft is:

<http://xdi.org/xdi-spec-docbook/xdi/xdi-core-1.0/xdi-core-1.0-wd06.xml>

We reviewed that the spec covers 3 main topics:

1. The XDI graph model and how it differs from RDF.
2. The formal XDI ABNF grammar.
3. The JSON serialization.

In the second part, Markus covered the XDI server, client, and tools code available from the XDI2 open source project, of which Markus is the lead:

<http://xdi2.org/>

Markus gave a tour of the XDI2 utilities that are available on the site and also of the Github repository for XDI2.

The third part covered XDI dictionaries and the role they play in semantic data interchange. Drummond explained how XDI dictionaries differ from RDF ontologies and XML schemas because they define reusable "words" that can be specialized in different XDI contexts just like natural language words in languages like English.

The example used was the term "flow". Flow has meaning in multiple contexts, e.g.:

blood flow  
sap flow  
traffic flow

In XDI dictionaries, <#flow> could be defined once, and then specializations can be defined. The definition context role is indicated by pipe characters, so the following are the addresses for different XDI dictionary entries:



```
|<#flow>|
|#blood||<#flow>|
|#sap||<#flow>|
|#traffic||<#flow>|
```

The specialized dictionary definitions can specialize the generic dictionary definition of #flow by extending or overriding the dictionary statements. For example, if the generic definition of <#flow> said it was an integer:

```
|<#flow>|/$is#/<$integer>
```

The a specialized definition can override the \$is# statement, e.g.:

```
|#blood||<#flow>|/$is#/<$real><$number>
```

More information on XDI dictionary entries is available both in the Dictionary section of the XDI Core 1.0 spec (see link above) and also this page of the XDI TC wiki:

<https://wiki.oasis-open.org/xdi/XdiDictionaryPatterns>

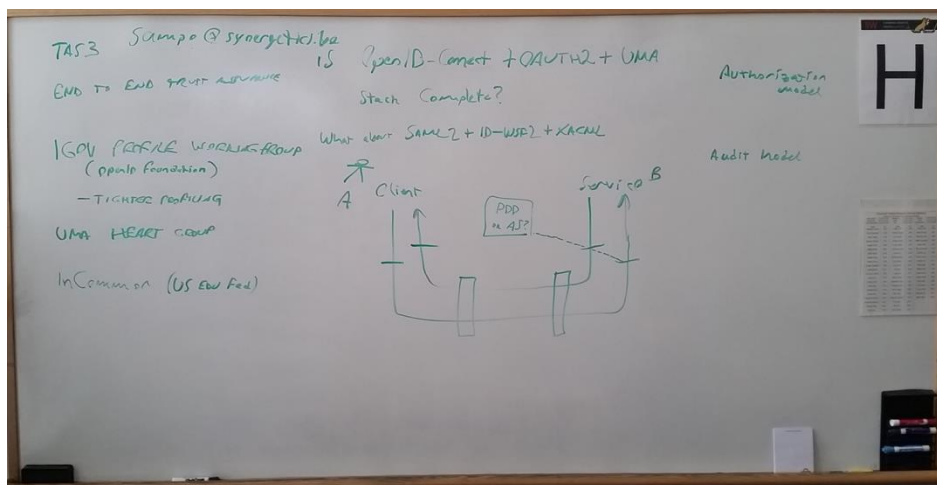
## ***Is OIDC+OAUTH2+UMA complete? What about SAML2+ID-WSF2+XACML?***

**Tuesday 4H**

**Convener:** Sambo

**Notes-taker(s):** Sambo

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



Efforts to profile and orchestrate use of protocols

IGOV Profile Working Group (under OpenID foundation)

UMA HEART group

InCommon (US educational federation)

Trusted Architecture for Securely Sharing Services (TAS3) and End-to-end Trust Assurance (Synergetics)

Both stacks are missing (but TAS3 architecture and E2ETA include):

- \* Tighter profiling of exactly how to use the specs (SAML tends to need less profiling, but even it does need it)
- \* New user intake
- \* New partner intake and Circle of Trust Management (or management model)
  - SAML2 metadata exchange is standardized, but there is much more to the intake
- \* Standardization of audit mechanisms
  - Digitally signed audit trail by logging the actual protocol messages can be done, but
  - Summary logs are not standardized yet
  - Frameworks standardize summary trail to automate processing the trail
  - Summary trail also facilitates transparency and visualization of audit trail to end users
- \* Standardization of legal/contractual framework
  - Clear description of how protocol actions and token fields articulate legal requirements and correspond to contractual obligations
  - Standardization of policies
- \* Claim: OpenID-Connect and SAML2 will do roughly the same job at SSO layer
  - Pairwise pseudonymization is possible, but needs to be made mandatory
- \* Claim: JSON Web Token (JWT) and SAML2 Assertion ultimately can express roughly the same things
- \* OAUTH2 is much looser specification than ID-WSF Security Mechanisms
- \* What are the service discovery methods in OAUTH+UMA? In ID-WSF there is clearly standardized discovery service
- \* Delegation supported in both stacks.
  - Binding through globally unique identifier, e.g. email (\*\*\*) describe mechanism in OAUTH+UMA)
  - People Service and pairwise pseudonymous Target Identity header in ID-WSF,
- \* UMA and XACML are trying to do roughly the same, namely move authorization decision away from the policy enforcement point (PEP), but they go very differently about it
  - UMA is generally foreseen to be able to impose a user interface in redirection games
  - UMA conveys authorization using a token
  - ID-WSF Discovery Service can in some cases also be seen similar to UMA as it, too, uses a token to convey the authorization
  - XACML does not specify any interaction mechanism, but ID-WSF interaction service does provide the capability
  - XACML does not convey authorization using a token, but rather using a Permit (or Deny) response to a web service call to the PDP
- \* Both have nascar style IdP discovery and IdP proxy is possible
- \* Web Service Discovery
  - Standard feature of ID-WSF
  - Perhaps Web Finger will do this for OAUTH2+UMA

## ***Burning Bridges and Breaking Brokers***

**Tuesday 4I**

**Convener:** Jim Fenton, Justin Richer, Paul Grassi

**Notes-taker(s):** Sarah Squire

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

Because Connect.gov is built on SAML, it is extremely helpful to minimize the number of connections between IdPs and RPs. That means that a broker in the middle who everyone connects to becomes helpful. IdPs and RPs who don't connect through the broker can talk to other IdPs and RPs through other channels, but often the ones who do go through the broker are bound by technology and policy to only talk through the broker.

OIDC makes connects between RPs and IdPs much cheaper, so that they can easily independently connect with each other. The "broker" can morph into a "trust anchor." The trust anchor is not an authorization service. The broker normally tells you who you can talk to and who you can trust. The trust anchor can help with standardized service discovery. RPs can have local policy and get further policies about unknown IdPs from the trust anchor. The trust anchor can provide whitelists and blacklists.

An RP can use a self-contained "software statement" when it dynamically registers with an IdP showing that it has certain client attributes. The trust anchor could provide that software statement.

The US government has the idea that linking and being able to trace transactions between IdPs and RPs is bad, so they came up with the idea of using a broker so that users can't be tracked and their activity can't be linked.

When you start talking about accessing government services with a digital identity, you need a higher level of privacy and security. Being about to link behaviors between behaviors, institutions, or interactions is something that many American citizens object to. Building systems that engender trust and ensure anonymity is critical to getting federal agency adoption. Creating blinding mechanisms can provide a lot more trust in the system.

Depending on what service you are using, there is a wide variety of anonymity that might be possible.

In a non-brokered model, OIDC does have a per-provider identifier (PPID) mechanism that could be used in a profile. However, colluding RPs could still use the other identifying data that's coming across the wire to track activity. To solve this problem, you can unbundle some of those attributes on a per-transaction basis.

How do we blind the IdPs about which RPs people are visiting? We shouldn't. The IdP needs to know what RPs the users are going to for security reasons. The solution is to allow users to bring their own trusted IdP. The proofing and binding can happen outside of or in parallel to these transactions.

How does the government audit independent IdPs? graylists and trustmarks.

Why are we using IdPs? Why aren't we just using two-party authentication? Like username and password? The problem with that is that federal agencies are not good at building those things, and it's not tenable for users to keep track of hundreds of usernames and passwords.

How does the trust anchor help RPs trust the IdP's assertions about important things like authentication context? RPs can send an IdP identifier through the trust anchor and the trust anchor can tell them how much an IdP is verified to be able to say - it's a trustmark.

There's nothing that says that we can't have direct OIDC connections and broker connections.

Users should be able to choose IdPs like they choose email servers - they can build their own, they can pay someone they trust, or they can use a free online service. Also like email, users can have multiple identity providers.

Is this leading to a national id card? No. If I can bind a homebrew IdP to an attribute bundle that is separate from a core identity, it means I can take that with me. The government isn't going to accept my self-asserted attributes, but there should be a mechanism to interact with a central "attribute provider," not identity provider, and bind my homebrew IdP to that so that the attribute provider can communicate verified attributes.

## ***Consent receipts in UMA***

**Tuesday 5A**

**Convener:** Sarah Squire

**Notes-taker(s):** Sarah Squire

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



Sarah Squire (playing the part of Alice), George Fletcher (playing the part of Bob), John Wunderlich (playing the part of the authorization server), and Susan Carvic(?) acted out the UMA flow with consent receipt opportunities. The pumpkin is the resource, the water bottle is the token, and the projector cap is the permission ticket.

| Data from         | Data to | Consent statement  |
|-------------------|---------|--|
| Alice (RO)        | RS      | "I, Alice, consent to store my resource with the RS and have it release my pumpkin"              |
| Alice             | AS      | "I, Alice, consent to delegate access rights to my AS" (consent directives/policy configuration) |
| RS                | AS      | "We consent to work together"  |
| AS                | RS      | "  |
| Alice             | AS+RS   | "I, Alice, consent to RS accepting AS and AS protecting RS"                                      |
| [Alice goes away] |         |  |
| Bob               | AS      | "I, Bob, consent to reveal claims to the AS" (consent potentially involving PII)                 |
| RS                | Bob     | "I, RS, consent to release the resource to Bob"  |
| RS                | AS      | "good faith notice"  |

Why can't a system just keep a log on its own? What's the point of generating a receipt for a person? The reason it's valuable is that every time the system does something, without the individual having evidence, they may get skewed in their understandings. If they end up, say, in court, they can

What's the difference between a consent receipt and a transaction receipt? Is a consent receipt just a subset of the generally useful concept of transaction receipts that are useful to humans but still machine-readable.

Is consent transactional or are there results of consents that happened earlier, such as by authorization policy? The UMA legal subgroup is trying to sort out what UMA flows count as "consent", legally defined (for whatever jurisdiction), to see if this helps. OAuth-based consent is involved to generate the PAT and AAT.

The receipt could simply be seen as a contract. Agency law, which spans jurisdictions nicely, is nicely applicable to contracts, in which you have principals, agents, third parties, and sometimes even shared brokers. Notice ("good faith" in the US?) is required before consent.

What might be a better (less confusing/more accurate) name than Consent Receipts?

- Consent Receipt References?
- Contract Receipts?
- Auditable Transaction Receipts (for the superset, including receipts about more than consent)?

How could a framework provide an answer for how to do the entire scope of receipt types? Human rights that go beyond contract have to be handled as well. Could @CommonAccord, which the UMA legal subgroup is looking at, be helpful? Its proprietor Jim Hazard has already been coding up the EU model clauses in the various languages.

How does a human get all of his or her receipts? Would a new ATR storage endpoint for ingesting receipts — which an AS or RS could expose — be useful? Should receipts be emailed? Heck, TripIt lets people forward un-machine-readable emails to a central storage place now. But not every service has asynchronous communications endpoints for the RO and/or the RqP.



## ***SCIM InterOp Discussion***

**Tuesday 5C**

**Convener:** Phil Hunt

**Notes-taker(s):** Prateek Mishra

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

General discussion about the nature of SCIM interop -

what are the expected error conditions from a SCIM request?

one goal is loosely coupled relationship between the client and the server.

But this means that clients don't know exactly what the server state is. They have to be ready for changes in user attributes. They have to be ready for variations in responses returned from the server

Kelly - SCIM 1.0 testing history - handbuilt script to test user create/delete etc.

The real challenge was that there was no way to describe required attributes, so it was difficult to communicate between client and server.

So what would be a basic test set for a SCIM 2.0 server? Probably a set of use-cases that should work against all SCIM 2.0 servers. Split into sub-sets, e.g., core, implementation of advanced features such as bulk or patch.

general discussion of the need for a standard identity api and how scim helps

Next steps: define some concrete use-case flows and work on them at the next IIW

## ***Potential Roles for Blockchain in Identity***

**Tuesday 5G**

**Convener:** Jeff Stollman

**Notes-taker(s):** Jeff Stollman

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

The purpose of the session was to explore the ways that blockchain technology could be applied to identity. I wanted to determine if the many useful features of blockchain (distributed source of truth, non-repudiable transaction log) bring value to our struggles to solve the various challenges of identity. I was fearful that in our excitement about blockchain and its capabilities we were acting like blockchain hammers looking for nails.

As we discovered there are a couple of solutions being developed that do leverage blockchain technology for identity purposes. We identified three such applications:

1. Shocard
2. World Citizen Passport
3. OneName

#### **1. Shocard** <http://www.shocard.com/>

ShoCard is an identity platform seeking to support Relying Parties in verifying the identity of a user. "The ShoCard Identity Platform is built on a [public blockchain data layer](#), so as a company we're not storing any data or keys that could be compromised. All identity data is encrypted and hashed then stored in the blockchain, where it can't be tampered with."

"ShoCard's game-changing pricing means almost no marginal cost to our customers for verifying identity. Banks and others can check identity on every transaction, virtually eliminating fraud."

#### **2. World Citizen Passport** <https://www.cryptocoinsnews.com/developer-creates-blockchain-passport-technology-based-bitcoin/>

The developer of World Citizen Passport created an open source solution that he hopes governments will take up for issuance of IDs. He doesn't appear to be interested in marketing his solution.

World Citizen Passport is a provider of a low assurance identity one's identity that currently uses social network references to attest to a person's existence. Of course, with additional vetting, the same approach could be used to capture higher levels of assurance identities.

#### **3. OneName** <https://onename.com/>

OneName is being developed by Ryan Shea who was in the session, so we spent most of the session drilling down on the particulars of his solution.

OneName allows you to choose a unique name, register it and build up a portfolio of both self-asserted and attested claims that the system can use to login and/or qualify for various services.

The name you register serves to allow others can find your blockchain ID. If you keep your password safe, no one can take this name from you.

You can link your blockchain ID and social media profiles together to prove ownership of your blockchain ID and verify it's really you.

It also allows you to share your blockchain ID on your website, social media profiles, and business cards so people can easily find you online, and link your public key to your blockchain ID to receive encrypted messages

It allows you to easily authenticate the digital signatures of other blockchain ID users and to log in to apps and websites without a password (coming soon).

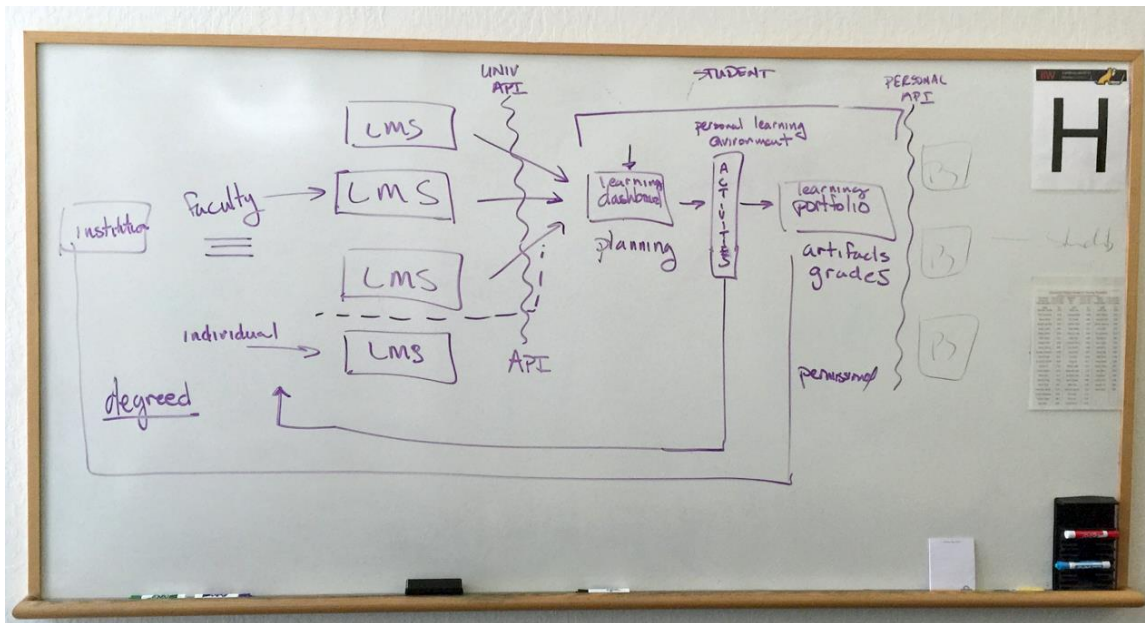
## The Personal Learning Environment

Tuesday 5H

Convener: Phil Windley

Notes-taker(s): Ben Werdmuller

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



The Personal Learning Environment is VRM for education.

A Learning Management System (LMS) is a course management system with quizzes and a gradebook. Faculty puts content into the LMS; students consume content. Occasionally students add content, eg quiz answers, but mostly the LMS is about the faculty.

In truth, Learning Management Systems aren't managing learning: they're managing course content.

In most LMS systems, anything students add disappears at the end of the term. This doesn't do the students a lot of good in terms of lifelong learning or building a portfolio of their work. They need something else.

Imagine if there were multiple Learning Management Systems that the students had to deal with. If you give faculty the choice, they won't all pick the same LMS software. (80% of faculty in practice choose one LMS, while the other 20% pick a variety of others.) So now students have multiple systems they have to interact with - but they don't want to log into a lot of them and have to manage each one in turn. Instead, it's better to give them a unified dashboard of their learning.

A student dashboard is a way for a student to see their upcoming learning activities: including but not limited to calendars; upcoming class events; notifications about their assessments.

From the dashboard, students participate in learning activities, which result in learning artifacts (pieces of work they've done and feedback on that work, grades, etc), which sit in a portfolio.

The dashboard + learning activities + the portfolio = the Personal Learning Environment.

Why distinguish between faculty and students? One reason is that the activities of students and faculty in an institution are markedly different. But one could certainly have a personal LMS that other individuals interact with.

The PLE could also potentially contain informal "paths" of learning, with peer certification of accomplishments, that could be shared between individuals. Startups like Degreed and Gibbon are working on this kind of technology, although are concentrating on corporate HR training rather than crowdsourced courses.

Every student gets their own PLE: it's not one big monolithic piece of software. Each student could potentially use their own version or select their own vendor. Students can potentially take their PLE with them when they graduate.

The PLE might have links to external tools that are used as part of the learning activities. Similarly, the portfolio may be a collection of links to resources actually stored on services like Dropbox, Google Drive, YouTube, etc etc. The value is in collecting these artifacts in the context of the student's learning. (Could there be value in providing a marketplace for both tools and places to store artifacts? This freedom of tools, loosely joined via the student's dashboard, could also free faculty to use the teaching tools and Learning Management Systems of their choice.)

A student's portfolio of artifacts and grades could flow back to the institution, with student permission, for accreditation.

One interesting missing piece: the mismatches in what the students have on graduation and what they need to learn to get a job are not captured as feedback that returns to faculty.

The ultimate goal of a PLE is to support lifelong learning.

BYU is starting a pilot of Domain of One's Own, a project that gives every student their own domain name and web hosting. They can install a selection of applications including WordPress and Known, install subdomains, and use it as their personal space. After graduation, the institution would prefer that students host their PLE elsewhere, so that the overhead of hosting is outsourced.

The PLE may turn out to be the largest deployment of the VRM model to real users.

## Wednesday October 28

### *Vectors of Trust*

Wednesday 1A

Convener: Justin Richer

Notes-taker(s): Jim Fenton

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

Authentication, Proofing

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

'Vectors of Trust' - many people hate the term but haven't gotten any better suggestions  
A vector in the mathematical sense -- not physics

Currently an IETF Internet-Draft -- looking to go through individual submission track to RFC

Candidate components:

Proofing  
Credential  
Management  
Assertion

Each has levels associated with it  
e.g. P0 = self-asserted, P3 = contractual relationship

In ID token, a new claim, e.g.,  
"vot": "P2.C3.M2.A1"

This will accommodate strong pseudonymity, e.g., "P0.C4.M2.A3"  
Context for this: "vtr":"https://.../"

Some elements can be repeated...perhaps if more things are being used to increase trust  
So multifactor authentication might be P0.C2.C3.A3 (perhaps a password and a FIDO token)  
or alternatively perhaps a P0.C4.A3

Trying to strike a balance between expressivity and excessive complexity for relying parties. Needs to be "stupidly easy" for RPs to process.

VoT does not define an ordering for values within a category, but a given "vtr" may specify that they are ordered.

## ***Re-delegation and Revocation with OAuth 2***

**Wednesday 1C**

**Convener:** Alan Karp

**Notes-taker(s):** Alan Karp

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

The motivating example is company A contracting with company B to allow employees of A to use services provided by B. Today, we federate identities so that the identities of A's users appear in B's environment. There are many problems with this approach that we can avoid by an approach called Federated Access Management (FACCM). However, FACCM requires that we create delegation chains, but there are no standards for doing that with OAuth.

In FACCM, company B gives company A a token with a scope of all the permissions covered by the contract. Company A delegates a subscope token to one of its employees, say a manager, who further delegate a sub-scope token to a user. When that user submits a request with this token, some party on the receiving side verifies that the request is authorized by the token and that the delegation is proper.

There are currently no standards specifying how to build such delegation chains. In this session we discussed three options.

1. Alice, the holder of an access token, can present that token to the Authorization Service (AS) and request a new token with a subscope. Alice can then give that token to Bob. Bob can further delegate to Carol using the same process. The AS keeps track of the delegation chain and revokes any tokens downstream from a revoked token.

2. The token is a JWT specifying a scope and a public signing key. It can only be used in a request signed by the corresponding private signing key. Alice, the holder of such a token, can create a new token that includes a potentially one-off public key she gets from Bob. She proves the delegation is valid by including a copy of her token in the metadata. Bob's request can be validated by checking that the request and each nested token is properly signed and that all delegations are valid subscopes. Tokens are revoked by telling the verifier not to honor a token with a specific GUID or any tokens delegated from it.

3. This proposal is not fully spelled out. The basic idea is to use hashes of tokens and metadata instead of signed JWTs. Other than that, the basic mechanism is the same as in #2.

We produced a table of advantages and disadvantages.

#1

Advantages: Close to OAuth standard and flows.

Disadvantages: Must be able to reach AS to delegate, metadata separate from token

#2

Advantages: Don't need to reach AS to delegate, can include lots of metadata, well understood because it's like what was done with SAML.

Disadvantages: Signing complexity, size of tokens, verification cost



#3

Advantages: Don't need to reach AS to delegate, size more flexible than JWT because no standard for mandatory fields

Disadvantages: cost of hash, size of tokens, verification cost

We ended with a vote. Only three of the seven people present voted, but they all voted for #3. I didn't vote, but I would have picked #1.

## ***International Perspectives***

**Wednesday 1D**

**Convener:** Bruce Nash

**Notes-taker(s):** Francisco Corella

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

The session surveyed nationwide identity schemes in several countries.

In Norway, banks issue PKI credentials that are used by 80% of the adult population for online authentication to commercial and government sites. They are data, not physical cards.

Banks also issue credentials in Denmark.

In Estonia, the government issues credentials to its citizens and to foreigners. A foreigner can apply for an e-resident credential without visiting the country.

In the UK commercial identity providers are authorized by the government to issue credentials. Attributes are asserted by citizens and verified by the government with yes/no answers. But enrollment is cumbersome and the system is not widely used.

In Spain the government issues chip cards that can be used online for multiple purposes using card readers.

In the US and Canada, government relying parties use private sector identity providers. A broker is used to hide identity providers and relying parties from each other.

The EU is working on a EU-wide identity system called STORK, which should be ready in 2016 or 2017.

## ***Blockchain Use Case: (not bitcoin, not identity centric) Distributed Ledgers***

**Wednesday 1E**

**Convener:** Dave Sanford, Kevin Cox

**Notes-taker(s):** Kevin Cox

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

From Kevin Cox – Blockchain and Welcomer:

<http://www.welcomer.me/welcomer/blog/2015/9/21/blockchains-and-welcomer>

Kevin Cox indicated that there might be lots of better ways to create a distributed ledger. Also there might be specific criteria to identify and differentiate the benefits of decentralization.

There are distributed ledger technologies that pre-date the blockchain, which typically have centralized permission and might or might not be more vulnerable. In particular, Kevin referred to the Interplanetary File System (IPFS) which is part of the ‘permanent web’. Kevin indicated that he thought the content addressable nature underneath IPFS could create some of the same advantages.

IPFS intends to link to blockchain at some point. The certificate transparency database at Google is similar to blockchain.

ERIS is a version of Ethereum without tokens which support smart contracts – focusing more on the checks and balance automation within the contract, than on simply title or value transfer.

Voting systems can be based on block chain – but has to be tailored for the right type of transparency, e.g. want to know what the Senator voted for, don’t want to know what Senator I voted for.

Blockchain may have been used to solve a problem called “homomorphic” encryption: A way to encrypt data such that it can be shared with a third party and used in computations without it ever being decrypted. This would allow untrusted computers to accurately run computations on sensitive data without putting the data at risk of hacker breaches or surveillance.

The reason banks are looking at permission based blockchain systems – is because they want a walled garden and the system would be cheaper to operate – while providing transparency and possibly faster convergence than current systems.

Some talk about ‘supply chain integrity’ uses for blockchain systems.

## **Identity Film**

Wednesday 1F

Convener: Kaliya

Notes-taker(s): Jim Pasquale

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

create a virtual board to hold the film and work on raising the money figuring out the financing.

The Film could be:

- Past \* Present \* Future
- 5 Years out
- a 7-10 mini-documentary that gives historical context extended elevator speech

Protocol Story / Competitors

Doc wrote up on the board the work of Scott Meredith

Protagonist(s)

Somebody or a cause audience identifiers with

Problem

conflict that keeps people watching or turning pages

Key: Things get worse but there must be movement toward resolution

Classic Hero's Journey

Is our story more like Luke Skywalker OR Obi Wan Kanobi

*people talked about it and we thought Obi Wan - the wise sage.*

The Hero is humanity

The enemy is the faceless machine we accidentally created

Moral conflict with @google and other large enterprises named in Terms and Conditions May Apply

Not the people - we don't know anyone at Google who is not a good person

they aren't the wretched hive scum of villainy

BIG OTHER / non-ominous

There is a spiritual side to IIW - many of the people have some sort of lens towards what we are doing that is spiritual.

The #nymwars

Parker Palmer worked with Obama to Train the Trainers in story telling - your story about how you got involved in the campaign and what you care about.

Pledges are needed

Kelly F said he would be willing to have some help coming from BYU. It would need to have some educational aspect to help employees understand topics in ID capabilities.

## Story (via Scott Meredith)

- 1) Protagonist(s)
  - somebody or a cause the audience identifies with
- 2) Problem
  - conflict that keeps people watching or turning pages.
  - Key: Things get worse. But there must be
- 3) Movement toward resolution

## OpenID Connect Certification: the view from the trenches

Wednesday 1H

Convener: Roshi Chandrashekhar & William Denniss

Notes-taker(s): William Denniss

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

OpenIDConnect Certification: The View From The Trenches

1. A general idea of where we started -- even though we helped write the spec, and we generally believed that the amount of work required to comply with the spec would be somewhat trivial, our bleeding-edge implementation with active users led to many challenges.

| Revision history<br>March 4, 8:54 AM |                            |   |   |                |              |                |
|--------------------------------------|----------------------------|---|---|----------------|--------------|----------------|
|                                      |                            |   |   |                |              |                |
|                                      | A                          | B   | C   | D              | E            | F              |
| 1                                    | Test Number                | Link to test Metadata   | Link to Screenshots, if any   | Clear Cookies? | Requires Re: | Failed/Passed  |
| 2                                    | OP-Response-code           | <a href="https://docs.google.com/a/google.com/document/d/1ZIWt">https://docs.google.com/a/google.com/document/d/1ZIWt</a> |   | No             |              | P              |
| 3                                    | OP-Response-Missing        | <a href="https://docs.google.com/a/c">https://docs.google.com/a/c</a>   | <a href="https://drive.google.com/a/google.com/document/d/1ZIWt">https://drive.google.com/a/google.com/document/d/1ZIWt</a> | No             |              | P              |
| 4                                    | OP-Response-form_post      | <a href="https://docs.google.com/a/google.com/document/d/1ZIWt">https://docs.google.com/a/google.com/document/d/1ZIWt</a> |   | No             |              | F              |
| 5                                    | OP-IDToken-Signature       | <a href="https://docs.google.com/a/google.com/document/d/1ZIWt">https://docs.google.com/a/google.com/document/d/1ZIWt</a> |   | No             |              | P              |
| 6                                    | OP-IDToken-kid             | <a href="https://docs.google.com/a/google.com/document/d/1ZIWt">https://docs.google.com/a/google.com/document/d/1ZIWt</a> |   | No             |              | P              |
| 7                                    | OP-IDToken-nonce-code      | <a href="https://docs.google.com/a/google.com/document/d/1ZIWt">https://docs.google.com/a/google.com/document/d/1ZIWt</a> |   | No             |              | P              |
| 8                                    | OP-IDToken-max_age=1       | <a href="https://docs.google.com/a/c">https://docs.google.com/a/c</a>   | <a href="https://drive.google.com/a/google.com/document/d/1ZIWt">https://drive.google.com/a/google.com/document/d/1ZIWt</a> | No             | Yes          | F              |
| 9                                    | OP-IDToken-max_age=1000    | <a href="https://docs.google.com/a/c">https://docs.google.com/a/c</a>   | Needed  | No             |              | F              |
| 10                                   | OP-UserInfo-Endpoint       | <a href="https://docs.google.com/a/google.com/document/d/1ZIWt">https://docs.google.com/a/google.com/document/d/1ZIWt</a> |   | No             |              | P              |
| 11                                   | OP-UserInfo-Header         | <a href="https://docs.google.com/a/c">https://docs.google.com/a/c</a>   | Not available   | No             |              | F              |
| 12                                   | OP-UserInfo-Body           | <a href="https://docs.google.com/a/c">https://docs.google.com/a/c</a>   | Not available   | No             |              | F              |
| 13                                   | OP-UserInfo-Enc            | <a href="https://docs.google.com/a/google.com/document/d/1ZIWt">https://docs.google.com/a/google.com/document/d/1ZIWt</a> |   | No             |              | Partial Result |
| 14                                   | OP-UserInfo-SigEnc         | <a href="https://docs.google.com/a/google.com/document/d/1ZIWt">https://docs.google.com/a/google.com/document/d/1ZIWt</a> |   | No             |              | Partial Result |
| 15                                   | OP-nonce-NoReq-code        | <a href="https://docs.google.com/a/google.com/document/d/1ZIWt">https://docs.google.com/a/google.com/document/d/1ZIWt</a> |   | No             |              | P              |
| 16                                   | OP-scope-profile           | <a href="https://docs.google.com/a/google.com/document/d/1ZIWt">https://docs.google.com/a/google.com/document/d/1ZIWt</a> |   | No             |              | P              |
| 17                                   | OP-scope-email             | <a href="https://docs.google.com/a/google.com/document/d/1ZIWt">https://docs.google.com/a/google.com/document/d/1ZIWt</a> |   | No             |              | P              |
| 18                                   | OP-scope-address           | <a href="https://docs.google.com/a/c">https://docs.google.com/a/c</a>   | <a href="https://drive.google.com/a/google.com/document/d/1ZIWt">https://drive.google.com/a/google.com/document/d/1ZIWt</a> | No             |              | F              |
| 19                                   | OP-scope-phone             | <a href="https://docs.google.com/a/c">https://docs.google.com/a/c</a>   | Needed  | No             |              | F              |
| 20                                   | OP-scope-All               | <a href="https://docs.google.com/a/c">https://docs.google.com/a/c</a>   | Needed  | No             |              | F              |
| 21                                   | OP-display-page            | <a href="https://docs.google.com/a/google.com/document/d/1ZIWt">https://docs.google.com/a/google.com/document/d/1ZIWt</a> |   | Yes            |              | P              |
| 22                                   | OP-display-popup           | <a href="https://docs.google.com/a/google.com/document/d/1ZIWt">https://docs.google.com/a/google.com/document/d/1ZIWt</a> |   | Yes            |              | P              |
| 23                                   | OP-prompt-login            | <a href="https://docs.google.com/a/c">https://docs.google.com/a/c</a>   | <a href="https://drive.google.com/a/google.com/document/d/1ZIWt">https://drive.google.com/a/google.com/document/d/1ZIWt</a> | No             |              |                |
| 24                                   | OP-prompt-none-NotLoggedIn | <a href="https://docs.google.com/a/c">https://docs.google.com/a/c</a>   | Not available   | Yes            |              | F              |

| 1  | Test Number                | Link to test Metadata   | Link to Screenshots, If any   | Clear Cookies? | Requires Re | Failed/Passed |
|----|----------------------------|---|---|----------------|-------------|---------------|
| 2  | OP-Response-code           | <a href="https://drive.google.com/open?id=0B6O-QtutCORCaEw5V">https://drive.google.com/open?id=0B6O-QtutCORCaEw5V</a>       |   | No             |             | P             |
| 3  | OP-Response-Missing        |   |   | No             |             | P             |
| 4  | OP-IDToken-Signature       | <a href="https://docs.google.com/a/google.com/document/d/1ZIWu7">https://docs.google.com/a/google.com/document/d/1ZIWu7</a> |   | No             |             | P             |
| 5  | OP-IDToken-kid             | <a href="https://docs.google.com/a/google.com/document/d/1ZIWu7">https://docs.google.com/a/google.com/document/d/1ZIWu7</a> |   | No             |             | P             |
| 6  | OP-IDToken-nonce-code      | <a href="https://docs.google.com/a/google.com/document/d/1ZIWu7">https://docs.google.com/a/google.com/document/d/1ZIWu7</a> |   | No             |             | P             |
| 7  | OP-IDToken-max_age=1       | <a href="https://docs.google.com/a/g">https://docs.google.com/a/g</a>   | <a href="https://drive.google.com/a/goo">https://drive.google.com/a/goo</a> | No             | Yes         | P             |
| 8  | OP-IDToken-max_age=1000    | <a href="https://docs.google.com/a/g">https://docs.google.com/a/g</a>   | Needed  | No             |             | P             |
| 9  | OP-UserInfo-Endpoint       | <a href="https://docs.google.com/a/google.com/document/d/1ZIWu7">https://docs.google.com/a/google.com/document/d/1ZIWu7</a> |   | No             |             | P             |
| 10 | OP-UserInfo-Header         | <a href="https://docs.google.com/a/g">https://docs.google.com/a/g</a>   | Not available   | No             |             | P             |
| 11 | OP-UserInfo-Body           | <a href="https://docs.google.com/a/g">https://docs.google.com/a/g</a>   | Not available   | No             |             | P             |
| 12 | OP-nonce-NoReq-code        | <a href="https://docs.google.com/a/google.com/document/d/1ZIWu7">https://docs.google.com/a/google.com/document/d/1ZIWu7</a> |   | No             |             | P             |
| 13 | OP-scope-profile           | <a href="https://docs.google.com/a/google.com/document/d/1ZIWu7">https://docs.google.com/a/google.com/document/d/1ZIWu7</a> |   | No             |             | P             |
| 14 | OP-scope-email             | <a href="https://docs.google.com/a/google.com/document/d/1ZIWu7">https://docs.google.com/a/google.com/document/d/1ZIWu7</a> |   | No             |             | P             |
| 15 | OP-scope-address           | <a href="https://docs.google.com/a/google.com/document/d/1ZIWu7">https://docs.google.com/a/google.com/document/d/1ZIWu7</a> |   | No             |             | P             |
| 16 | OP-scope-phone             | <a href="https://docs.google.com/a/google.com/document/d/1ZIWu7">https://docs.google.com/a/google.com/document/d/1ZIWu7</a> |   | No             |             | P             |
| 17 | OP-scope-All               | <a href="https://docs.google.com/a/google.com/document/d/1ZIWu7">https://docs.google.com/a/google.com/document/d/1ZIWu7</a> |   | No             |             | P             |
| 18 | OP-display-page            | <a href="https://docs.google.com/a/google.com/document/d/1ZIWu7">https://docs.google.com/a/google.com/document/d/1ZIWu7</a> |   | Yes            |             | P             |
| 19 | OP-display-popup           | <a href="https://docs.google.com/a/google.com/document/d/1ZIWu7">https://docs.google.com/a/google.com/document/d/1ZIWu7</a> |   | Yes            |             | P             |
| 20 | OP-prompt-login            | <a href="https://docs.google.com/a/g">https://docs.google.com/a/g</a>   | Needed  | No             |             | P             |
| 21 | OP-prompt-none-NotLoggedIn | <a href="https://docs.google.com/a/g">https://docs.google.com/a/g</a>   | Not available   | Yes            |             | P             |
| 22 | OP-prompt-none-LoggedIn    | <a href="https://docs.google.com/a/google.com/document/d/1ZIWu7">https://docs.google.com/a/google.com/document/d/1ZIWu7</a> |   | No             |             | P             |
| 23 | OP-Req-NotUnderstood       | <a href="https://docs.google.com/a/google.com/document/d/1ZIWu7">https://docs.google.com/a/google.com/document/d/1ZIWu7</a> |   | No             |             | P             |

- Backwards-incompatible changes like changing the issuer and adding “nonce” to id-tokens meant that we’d run into issues with clients who relied on our existing behavior. This can be solved by versioning our endpoints and supporting both the non-spec-compliant and compliant ones. However, it still leads to tricky issues like this:  
<http://stackoverflow.com/questions/29916637/validating-google-oauth-id-token-received-from-oauth2-v4-token>
- Speaking of validation, there are a number of client libraries that still only expect the OLD Google issuer, even though the spec had an exception for Google’s issuer and stated that developers should handle both issuers that started with the schema and that did not.  
[http://openid.net/specs/openid-connect-core-1\\_0.html#GoogleIss](http://openid.net/specs/openid-connect-core-1_0.html#GoogleIss)
- Discovery Document  
versioning - Since it’s hard-coded, there isn’t a way to version this. So we relied on  
<http://stackoverflow.com/questions/29830503/google-is-updating-their-openid-connect-implementation-to-be-fully-spec-compliant/29830504#29830504>  
caching - The general cache time for static documents like this one was 7 days, and we needed to be sure we could bring that down to ensure that anybody who saw a problem could report it quickly enough for us to point them to either StackOverflow or roll back.
- Endpoints that may be out of scope of just OpenIDConnect Spec Compliance  
Providing spec-compliant claim names at TokenInfo  
Supporting spec compliant issuer values for ID Tokens issued as a result of assertions

There was an interesting discussion that followed about best practices while working towards spec compliance.

Link to Google.doc:

<https://docs.google.com/document/d/1hUPY2PCYJpeT5ocWDz5PvLvkgRKLdQ53pJYWL0KuE54/edit#>



## Non-Person Entities

Wednesday 11

Convener: Dan

Notes-taker(s): Susan David

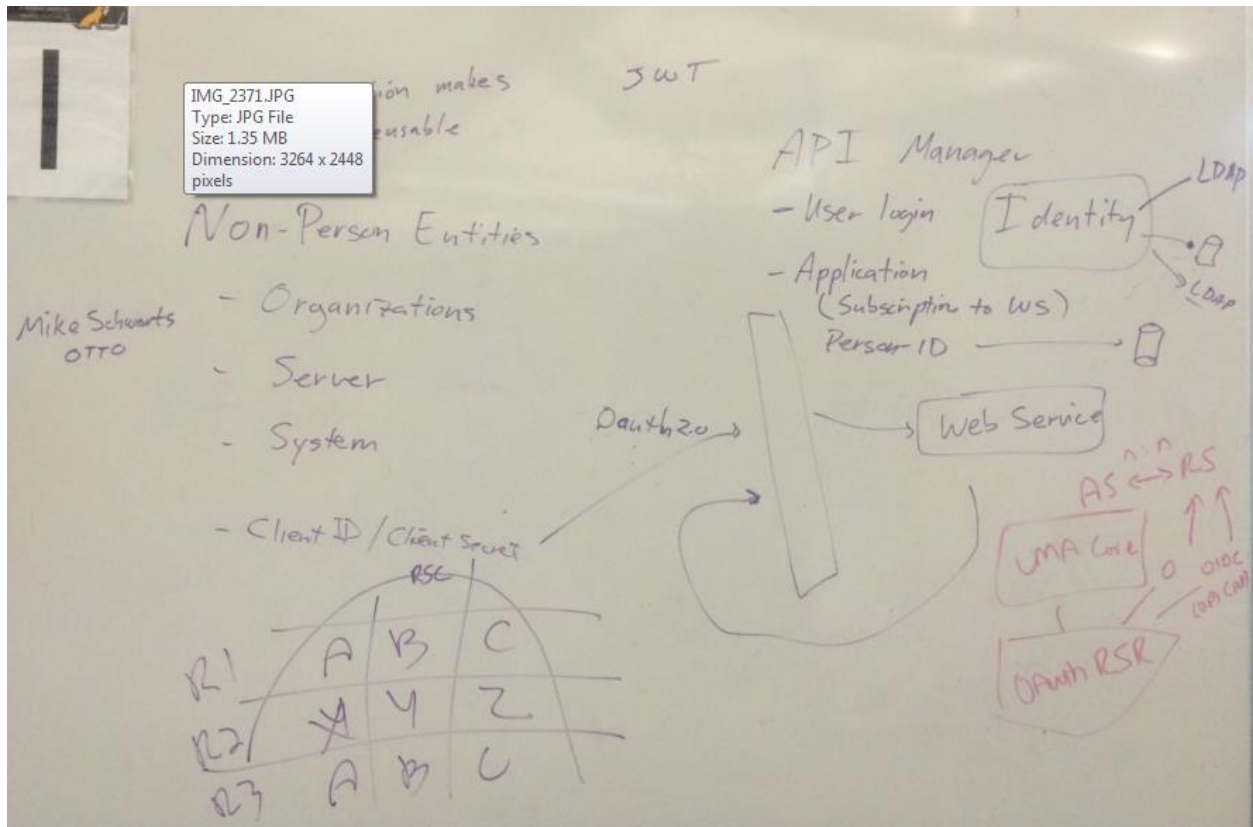
Tags for the session - technology discussed/ideas considered:

Non-Person Entities, Authentication, Things, Ownership, API Management

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

What Non-Person Entities are there?

- Organizations
- Server
- System
- Applications



Had to create "non-people" people.

Ws02 – can set up webservices and subscribe to them.

API Manager:

- User Login – receives bearer token
- Application subscribes to WS –

Administrators don't want to have non-person entities in the LDAP, so NPEs not in LDAP, and don't get a login.

Want to tie application login to person ID that ties into datastore.

So if I authenticated to the API Manager, build JWT with identity information.

Goal: each non person entity to have their own Client ID and Person ID and store in JWT and pass along to web service – how do others deal with this?

Many API managers come with tools for managing client credentials of non-persons.

WSO2 – works better when it runs everything. WSO2 can talk to multiple credential stores.

Covisent: just set up a series of APIs for managing non-person identities. Handles authentication of things, how to exchange authorizations. Seeing things on the outside/things on the inside.

Are there proxy/delegation solutions .

“If a product is good at doing something – let it”

IT needs to stamp out the impulse to customize/build their own. If you want more modularity/reuse – incentivize it.

APIs force reuse - (Documentation makes APIs reusable)

Okana (used to be SOA software) created a function to translate WSDL, RAML, Swagger – last week.

Push to have application credentials stored in LDAP – single source of identity is the desire. Need standard schema for things.

Do JWT tokens get used to authenticate to other things? - yes – this has become common currency. (JSON Web Token)

Gateway can do any needed transformations.

Open Trust Taxonomy for OAuth (Mark Schwartz) – OAuth federations [\\this](#) could be used by API platforms.

Dynamic Onboarding: UMA might be something to look at:

UMA has two specs:

UMA Core: loosely couples AS and RS

UMA Resource Set Registration (RSR) : OIDC: OP and 3<sup>rd</sup> party attribute providers

- Federated authorization

If you have services, and want them to use your authorization service: this would be a way to do this.

SaaS: We can SSO onto SaaS, but what we really want is for them to provide Federated Authorization (Dynamic Entitlements) Imagine having the Scopes brought to every service within the Token. Scopes make entitlements reusable (Scope grained access control, by taking federated authorization approach).

Are Scopes standardized? No – entirely unstandardized (causing a fight). Now they are just keywords. UMA tried to standardize them by making them Http verbs – fell apart. However, can make them be URLs – User URL has to be resolvable. AS has to be able to grab it, so that the user can set policy.

Scopes: (A,B,C..) all in RSC. UMA: A,B,C will be registered against resources (R1, R2, R3): Resources can be end points, information – think of it as nouns and verbs.

## ***Multi-Protocol, end2end Trust Assured Frameworks for Personal Data Ecosystems***

**Wednesday 2A**

**Convener:** Luk Vervenne

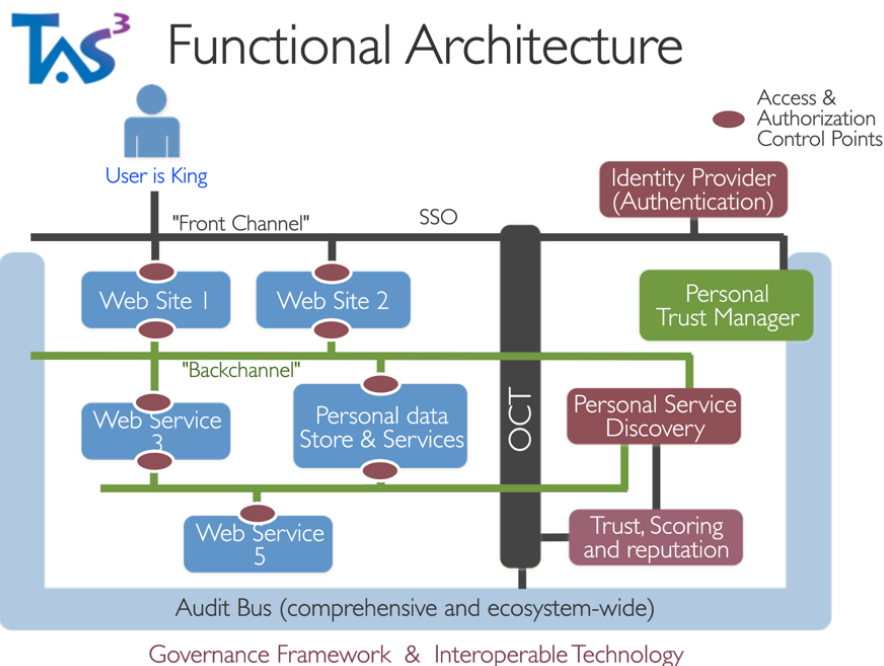
**Notes-taker(s):** LaVonne Reimer & Luk Vervenne

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

This team has been grappling with rubber meets the road pragmatism, innovation meeting real use cases coupled with strong regulatory regimes

TAS3.eu = Trusted architecture for securely shared services

- Individual as empowered stakeholder
- End to end trust assurance and trust perception
- Bring analytics to the data--democratization of analytics services



Personal data as big data using Virtual personal data stores by virtue of

- Cell-level data security allowing.
- ABAC + RBAC + CBAC policy management in a big data setting

Ecosystem is managed by:

- Techno-legal-contractual framework
- Separation of concern governance

Multi-protocol stack = Open architecture using translatable

- SAML + IDWSF SSO layer
- OIDC + Kantara UMA

Personal trust manager: user can see “who asked for his data, did they got it or why not?”

Support for delegation, breaking the glass principles, ...

High-level architecture with front- and back channel

Throughout the architecture, every component has client & server access & authorisation control points that send their audit summary data to an audit bus.

<http://www.ft.com/cms/s/0/5fd7d8a8-28e5-11e2-b92c-00144feabdc0.html>

Estimates cited in Financial Times personal data is going to be worth \$1T -- it's a valuation rather than assertion of revenues to be addressed. Ad tech is 10% of this and going down. So the conclusion is there is value to be gleaned that isn't all about ad tech. We need to get persons leveraging these data to begin to bring some of that value into the economy.

Eg healthcare insurance (the Netherlands) example:

Risk balancing that goes beyond just the claims filed with them. Such as unemployment and other records they cannot get because of data privacy. The alternative is that insurers let go of the data, leave it in the PDS of care recipients, and organize privacy preserving analytics retrieving the insights they need rather than the data.

Europe is setting up a “personal information management” industry association.

Mostly SMEs, start-ups and university departments.

Big ICT companies too entrenched in enterprise. Don't see it yet.

Trying to join forces on architecture to enhance their impact.

EU commission gave out \$2B to big companies for big data research and optimization.

What's at stake is continuing to exploit personal data.

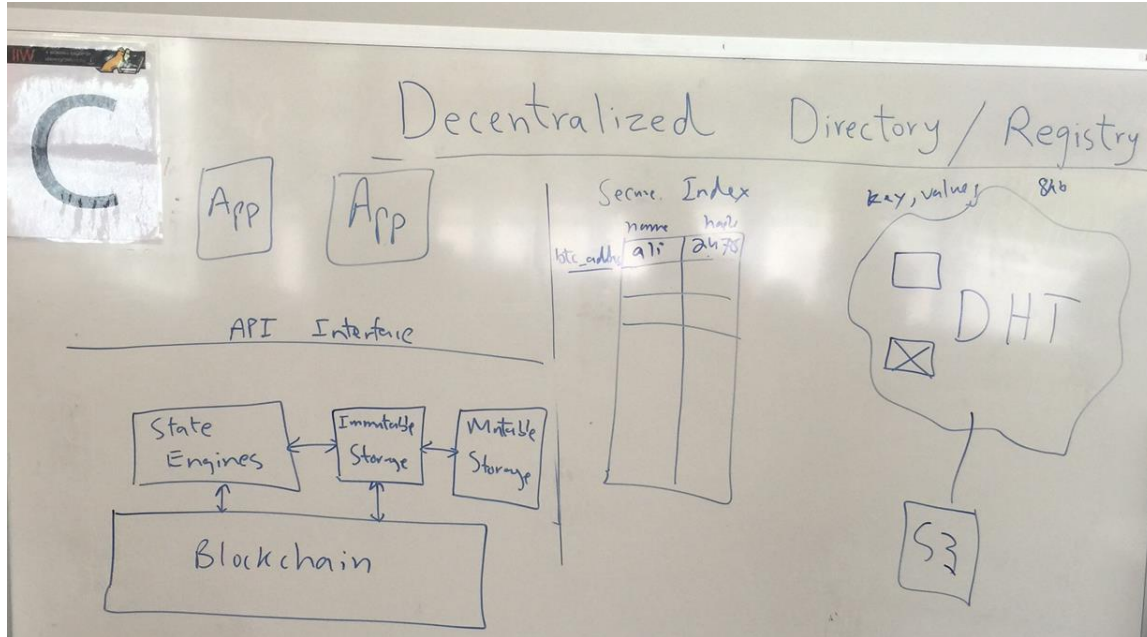
## Decentralized Directories/Registry (using Blockchain)

Wednesday 2C

Convener: Muneeb Ali

Notes-taker(s): Muneeb Ali

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



And the session basically covered this:

<https://github.com/WebOfTrustInfo/rebooting-the-web-of-trust/blob/master/topics-and-advance-readings/Secure-Naming-on-the-Blockchain.md>

## Ethereum: a general purpose Blockchain

Wednesday 2E

Convener: Aaron Davis

Notes-taker(s): Dave Sanford

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

Aaron asked if this is what was wanted – and gave a tutorial starting with some basics on blockchain followed by how Ethereum uses blockchain.

While the blockchain algorithm can act as a platform that provides “a single source of truth” without centralized control – there are many possible:

- Data structures
- Consensus mechanisms

Blockchain acts as a reverse linked set of blocks with each block leading back to the first or 'genesis' block. The blockchain is more than a distributed ledger – it is a living programming system and the blockchain represents the state of the system including every block and every transaction.

For bitcoin, miners submit timestamps and everyone has to agree on the state of the system. The longest blockchain wins.

Consensus – for any system we need a way for the system to make changes to state – from any participant – and converge to an agreed state, at least for some known point in the past. For a private blockchain the owner(s) decide. For public block chains – this involves 'proof of work'.

Along with transactors, the main actors are miners – which act as validators.

While the bitcoin machine is primarily programmed to support financial transactions – Ethereum is a distributed programming machine – a computer containing disk and programs. It uses the basic blockchain features:

- Transparency
- Mutability
- Consensus

And may be able to support lots of governance functions. It supports key revocation. There is a quote out there – “If bitcoin is magic Internet money, maybe Ethereum is magic Internet governance” – although there is lots of work to do, to see if it can get there.

For Ethereum – autonomous programs exist, but cannot initiate a transaction. These programs do have an address, code and their code and storage is written into the blockchain.

Clearly Ethereum can do lots of programming which would not be efficient as it would simply be better to run it on a stand-alone computer. It is not for heavy computation or heavy data, as many minors have to each run all the code.

Ethereum has a block time of about 17 seconds – however it takes about the same amount of time (perhaps an hour ~ 600 blocks) for consensus to be reached on a block, as with bitcoin.

Ethereum is good for write access management and keeping track of tokens and as a betting platform. Every op code has a fee, so you can run an infinite loop if you want to pay for it. If the transaction doesn't complete you still pay for processing. Ethereum predictive markets have been created.

Ethereum supports contracts (and proxy contracts? Not sure what that is). Typically the first person 'wins'. Contracts have APIs associated with them and a valid address.



## ***Beyond Ad Blocking***

**Wednesday 2F**

**Convener: Doc**

**Notes-taker(s): Judi and Doc**

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

ad blocking, revolution, RSS, Ghostery, Lumascape, tracking, advertising, #NoAds, #DNT, do not track, inner voice, user pain, #SafeAds (tweeted, face booked, blogged) #SaeAd (on an advertisement)

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

LUMAscapes show how complex the current adtech plumbing is.

Google Trend searches make a convincing case that tracking has driven ad blocking. It isn't just shitty and annoying ads.

While ad blockers are popular, the biggest, Adblock Plus, is not taking the right lead with its "acceptable ads" program.

The press is hypocritical in their disdain for ad blockers while running so many trackers that burden the users.

Thus the popularity of ad blockers is huge....:

200 million people currently using ad blocking in their browsers. With this action, they're saying "no ads" and "do not track." (Also, it amounts to the largest #boycott or #blockade in human history.)

People often think that when they block ads, they're blocking tracking as well (and vice versa) This isn't necessarily so. There are cases where people want #SafeAds but don't get them. Or when they block tracking and in effect ruin their experience of a site because so much of the site is based on tracking, even though the ads may not be based on tracking. (e.g. when using the EFF's privacy badger)

People also don't know what the sliders in Privacy Badger, Ghostery and others actually control. And Ghostery has >500 different tracking companies that can be opted out of. Crazy.

The 200M people got the attention of Verge, other big companies. Mozilla thinks of the web as an ecosystem. Worst case is that some big sites go full-on silos, start an escalating war. Main difference between safe and unsafe ads: tracking. Safe isn't based on tracking, unsafe is. (For today. Later, when ads are permission based by individuals, some tracking may be allowed — but the individual is in charge of that.)

Doc's proposal: Step 1: what about popularizing #SafeAds. Make it a trend. Step 2: Verge and other advertisers will be open to working with #SafeAds, as will be advertisers, who have already demonstrated that they're willing to put code and symbols on ads. So ads will start to say "#SafeAd," in response to user pressure. Step 3: Person-driven programmatic (VRM).

When we can get the #SafeAds movement large enough, Step 2 and 3 will follow.

Until then, we're still using AdBlockers until the movement works...

Other factors...

Big advertisers aren't feeling the pain.

Small bloggers need their networks to make advertising work for them.

Are there examples of opt-in that is working? No examples today.

Start to align the incentives in the right direction. No incentive today, though most of the pipe is there.

Bullies tend to win, and no big players are open to experimenting (yet).

George Fletcher of AOL: Until #safeads gets popular, people will continue to run ad blockers. Once popularity happens, however, the existing system will adapt.

FedEx as an example, they work with ad agencies, which work with everything in the LUMAScape. But #SafeAds would be desirable for them.

Source: <<http://blogs.law.harvard.edu/doc/2015/09/24/the-adblock-war-series/>>

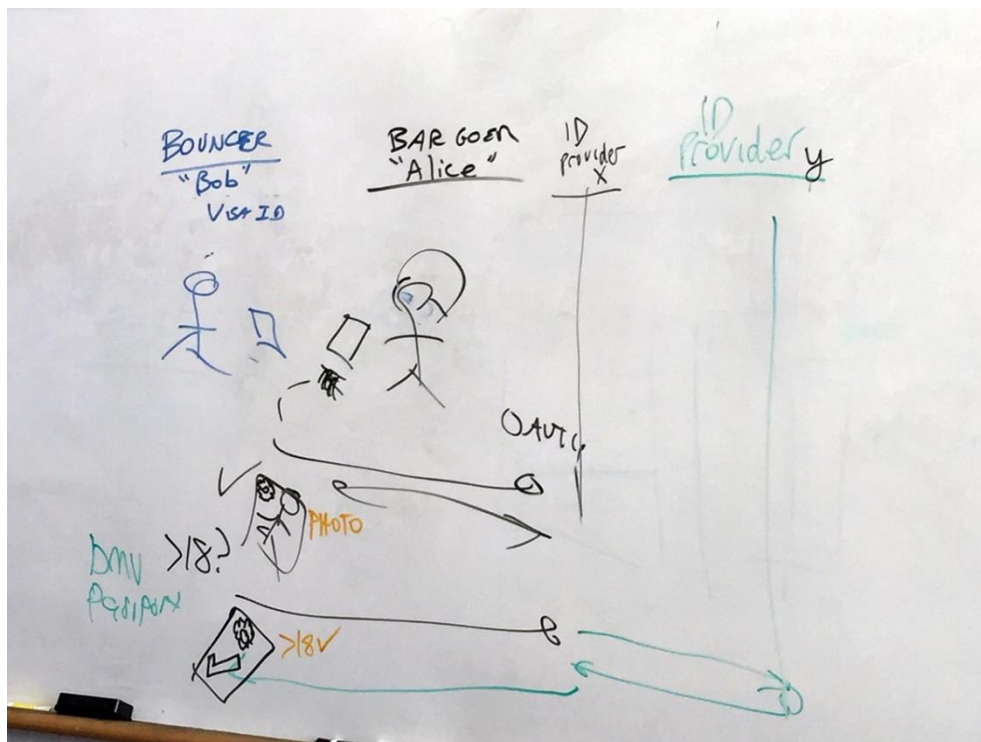
## Selective Disclosure

Wednesday 2G

Convener: Christopher Allen

Notes-taker(s): Jim Pasquale

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



## ***Post Password World***

Wednesday 2J

Convener: Dick Hardt

Notes-taker(s): Brennan Lee

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

How many people have ideas about post-password world?

### **1. Unguessable URL**

prototyped as a bookmark-able token URL

add part of the unique URL to the header

if you erase the bookmark, you need to re-gen the key

Dick - I don't like that idea, issues

### **2. Phone-based**

2-factor authentication through phone Yubikey

biometrics aren't very secure.

apple pay is an "in the wild" example of using post password

the combination of hardware, safe biometric authentication, tokenization.

identity proof - when I registered the card on the device, banks weren't doing identity proofing

identity proof - my bank has identified me to perform transactions.

to replace the password, you will have to

### **3. Fido/UAF**

<https://fidoalliance.org/assets/downloads/FIDO-U2F-UAF-Tutorial-v1.pdf>

**QUESTION: Why do we need to solve the password problem?**

### **4. Client Certs**

**QUESTION: Should we have passwords in 10 years?**

### **5. ID in browser**

Sign in to browser once then browser brokers authentication for the user.

## 6. Trusted Signals

My wireless network knows who I am so it can authenticate me.

## 7. Behavior (History)

My history indicates (probably) who I am

## 8. ID + location on Map

Plug in my ID and pick a point on a map to authenticate you are who you are

## 9. Microchip / Temp Tattoo / Taking a Pill with a Signal

**COMMENT: We can solve recovery and not solve passwords?**

Is everyone comfortable with how Credit Cards handle authentication? (NO!)

## 10. Public Key Authentication

[https://en.wikipedia.org/wiki/Public-key\\_cryptography](https://en.wikipedia.org/wiki/Public-key_cryptography)

## 11. Google Authentication / Ubikey / BioMetrics

Biometrics are fragile. They are good as an additional factor. They are problematic if they are the single factor.

**COMMENT: "Our current central IDP is our Mail system"**

Banks are bad

Root-independent identity source to build upon

### Desirable characteristics of post-password auth system

- Low Cost
- X-Device - App brokers sign
- As reliable as passwords
- Recovery must be better than current patterns
- Something in the auth mechanism must be revokable.
- Continual Authentication
- Security Gradient

### Further Reading:

**"A Quest To Replace Passwords - Joseph Bonneau"**

[http://www.jbonneau.com/doc/BHOS12-IEEEESP-quest\\_to\\_replace\\_passwords.pdf](http://www.jbonneau.com/doc/BHOS12-IEEEESP-quest_to_replace_passwords.pdf)

## ***Trust ~ Elevation with UMA and Connect***

**Wednesday 3A**

**Convener:** Mike Schwartz

**Notes-taker(s):** Mike Schwartz

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

Mike presented slides that he developed for an OWASP chapter meeting in August.

- Video (from OWASP): <http://www.gluu.co/trustel-owasp-2015>
- Prezi: <http://www.gluu.co/trust-el-prezi>
- Slides: <http://www.gluu.co/trust-el-slideshow>

## ***U2F Update***

**Wednesday 3C**

**Convener:** John, Jerrod, Stina

**Notes-taker(s):** John Fontana

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

It is public key crypto

Benefits over the OTP, prove this is a real person.

don't need third-party service.

I can log in to bank, gov. school. No secret is shared.

New set of encryption secretes when you login.

Can allow high scale, high privacy security.

There is no one controlling the global scale of identity.

Code is open and free.

Works with Chrome' we're working with Mozilla for them to adopt U2F

Building ecosystem with many authenticators.

Will be choices for all sorts of servers, services, biometrics, authenticators,

There is a registration process and authentication process

You can have many challenges in each session, not just initial login

The FIDO stack can be built into any software, it is now prominent in browsers, Chrome, Mozilla working on it.

What about mobile.

Mobile is about apps, a mobile app could do software key gen, and that app will basically be your fido client and your authenticator.

The future state is that the platform will provide the plumbing,

Apple is not on board at all now. Their support would be app level support and not device level support.

Phishing and man in middle in the protection.

Origin is important, the client can verify where the response comes from. It fights re-direction.

Application specific keys layer on top.

OTP notion today is symmetric. If every server does symmetric, you will have a mountain of codes. Independent of passwords look at strong two-factor today.

Device cloning – protection against this.

Registration and device attestation.

Need to have bit to store public key and verify this is device you want to work with

So in the protocol we have attestation, relying party can decide which authenticators to trust.

Maybe this authenticator has secure element, transports over USB, I make assumptions what this authenticator can do ...

You can trust vendors that produce the device, registration, once you have bound keys, can do bootstrap sessions on new devices.

Registration is critical, you can go bootstrap other things. You bootstrap a secure account to device and you can use it everywhere.

Adding u2f support

Clients are there.

Critical thing for U2F public keys for those devices.



Q: How do you validate a hardware device?

FIDO has certified devices, that is one area. You can check signatures.

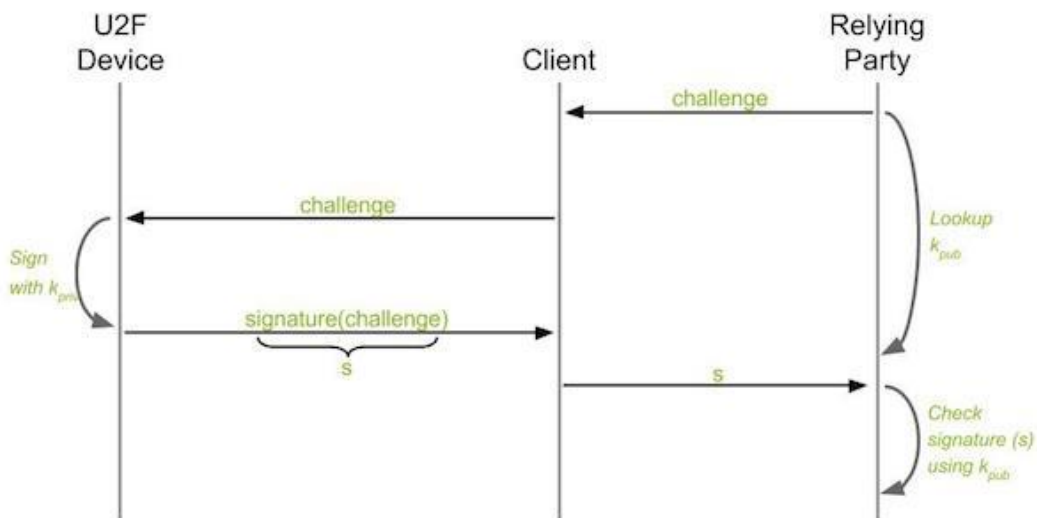
As ecosystem grows. We see platform support as key.

U2F final specs are one year out, industry leadership is needed for evolution.

We know public Key crypto works, the industry failed at first with too much infrastructure. Now that is gone with this. And we need to get it baked into platforms

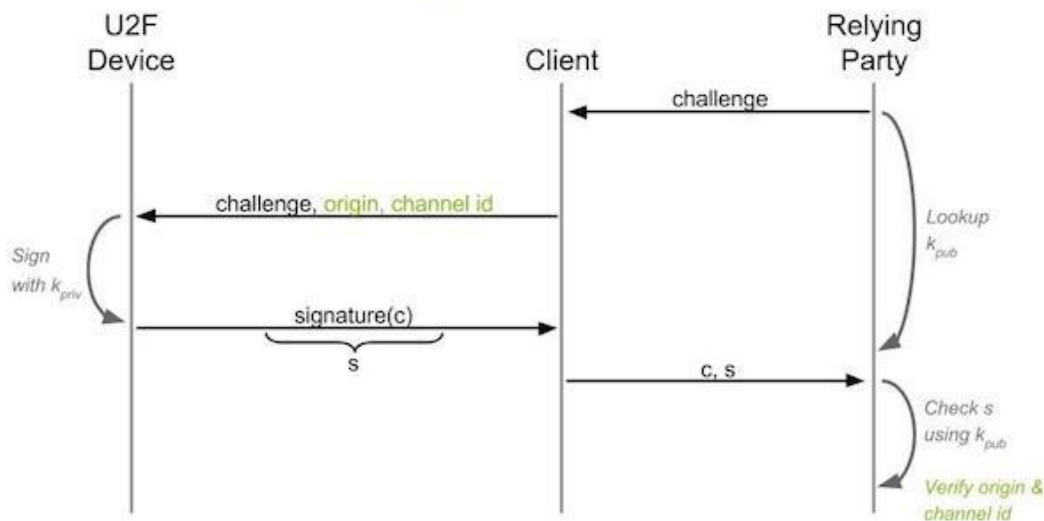
## PROTOCOL DESIGN

### Authentication



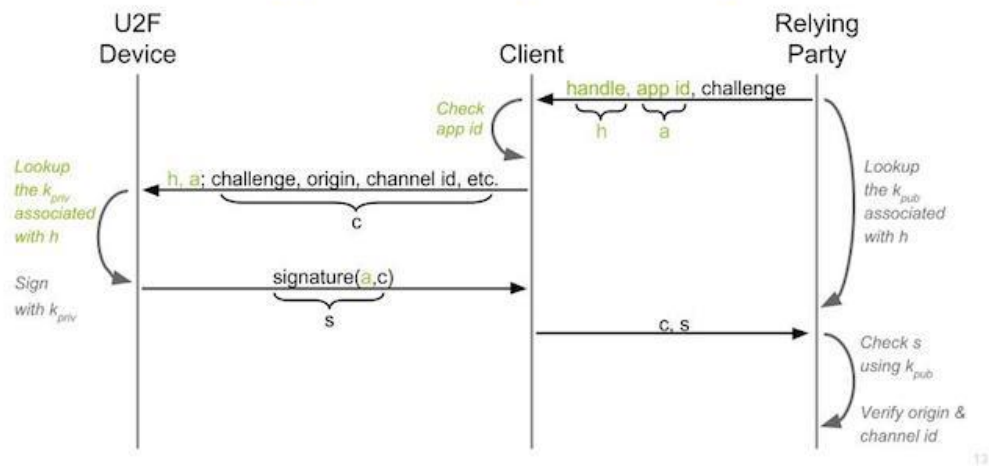
11

### Phishing/MitM Protection

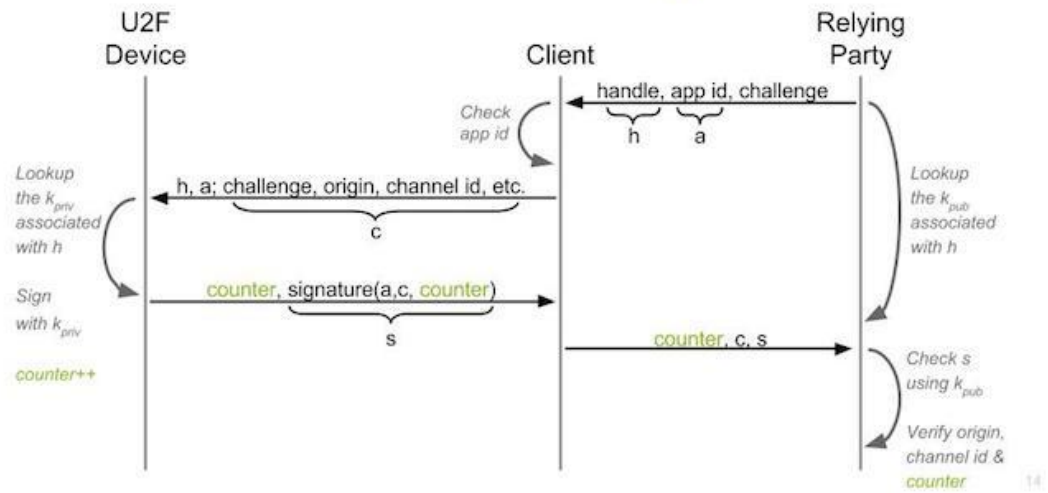


12

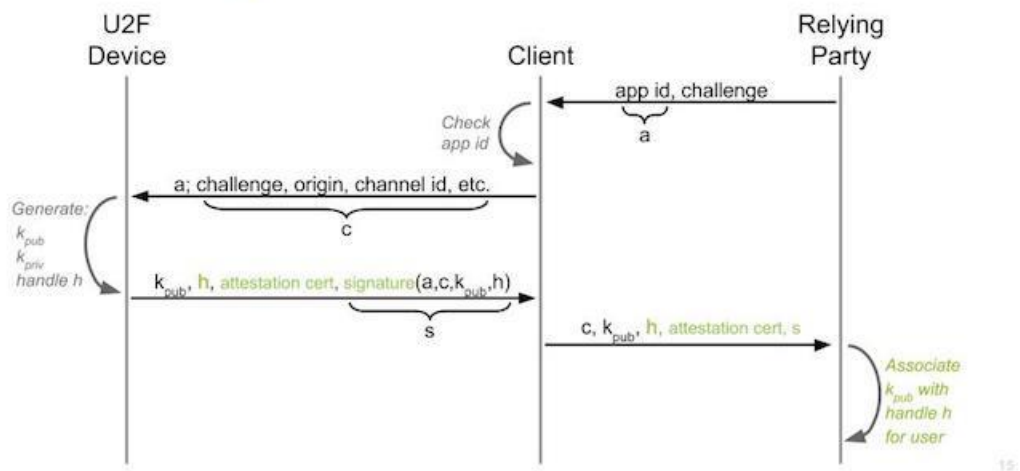
## Application-Specific Keys



## Device Cloning



## Registration + Device Attestation



## ***Blockchain Auth: Passwords login w/blockchain using JSON web tokens***

Wednesday 3D

Convener: Ryan Shea

Notes-taker(s): Ryan Shea

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

#blockchain #JSON

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

An authentication flow with Blockchain Auth looks like this:

1. the app creates a signed authentication request and delivers it to the user
2. the user's client verifies the authenticity of the request
3. the user's client compiles information for an authentication response
  1. it grabs the challenge inside of the request
  2. it looks at the permissions and pulls together the necessary data to deliver
4. the user's client creates a signed authentication response with the compiled information
5. the user's client sends a message to the app's server with both the app-produced authentication request and the user-produced authentication response
6. the app looks at the request and response and performs a few checks
  1. "hey, this auth request was really signed by me"
  2. "hey, this auth response was really signed by the user who claims to have produced the token"
  3. "hey, the request and response have the same challenge"
7. the app logs the user in

Blockchain Auth does not require third party identity providers. In a sense, the blockchain is the identity provider. It has the directory of identities.

There are two types of auth responses - pseudo-anonymous auth responses and identified auth responses.

With pseudo-anonymous auth responses, only a persistent public key is specified, as well as optional private information. No blockchain ID, and by extension public profile, is provided by the user.

With identified auth responses, the user additionally provides a blockchain ID, as well as evidence that they are the owner of said blockchain ID.

Quote: It looks like this is looking to replace OpenID Connect. I'm just trying to call a spade a spade

## ***Book Preview: OAuth 2 in Action***

**Wednesday 3F**

**Convener:** Justin Richer

**Notes-taker(s):** Justin

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

We discussed the forthcoming book, OAuth 2 In Action, by Justin Richer and Antonio Sanso from Manning Publications.

The book can be pre-ordered online at <https://www.manning.com/books/oauth-2-in-action/>

A discount code was provided to attendees

## ***Citizen Data Schema***

**Wednesday 3G**

**Convener:** David Kelts

**Notes-taker(s):** David Kelts

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

- Proposed a common data model for SCIM/JWTs/OIDC that would represent "Citizen" users
- Feedback was to create "Citizen" as a new schema with RESTful endpoint parallel to "User"
- All data elements appear to be complete
- Discussed the models for lists of breeder documents, verification performed, and status value

## ***Blockchain & UMA: Two Great Tastes ...Do they go together?***

Wednesday 3J

Convener: Aaron & Eve Maler

Notes-taker(s): Eve Maler

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

Attending: Aaron Davis, Eve Maler, Darius Donlap, Joe Andrieu, Adrian Gropper, Jin Wen, LaVonne Reimer, Mark Dobrinic, Heather Vescent, Christopher Allen, Joachin Miller, Shailesh

The proposition: Are there opportunities to use blockchain and UMA together for the greater good?

The discussion: Some properties of blockchain: Proof of existence by virtue of being on the chain at a point in time, and thus non-repudiation. This is like an audit log entry, and thus it acts like a receipt! The information on the chain "public" and out in the open.

Some properties of UMA: Protection (central) of resources (that are distributed). All the parts of the UMA flow are "private".

Is there tension between them therefore? Not necessarily. Hashes of the relevant information can go on the chain. However, blockchains are long-lived vs. (say) bearer tokens, whose risk of being exposed is often partly through time-to-live strategy. Could you cut old stuff off the chain/ Yes, but you can't delete those parts from all copies of the distributed chain. Opportunities to use blockchain and UMA together that we identified so far:

1. Could post legal obligations/consent receipts/auditable transaction receipts on the chain. We liked this one a lot and thought it had the most immediate application. Blockchain implementations such as Ethereum, Enigma, etc. build non-repudiation with revocation and non-correlation in. This makes the "receipts" able to act like really flexible contract records.
2. Could layer blockchain-based DRM and licensing solutions on top of resources once UMA-based access is granted. Ethereum is doing work that has DRM and licensing implications.
3. Could leverage provenance proofs in enforcing purpose-of-use limitations in UMA-based chained downstream chaining, which normally wouldn't really be able to fully propagate these limitations in the "soft" (business-legal) realm. This would be like applying "chain-link confidentiality" at a technical layer; see this paper: [http://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=2045818](http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2045818) Again, Thereum is doing work on provenance solutions, e.g. for supply chain use cases in medicine.
4. Finally, could use blockchain-based reputation data, which is typically desired to be public anyway, for UMA trust elevation processes prior to authorizing a requesting party for access and also for dynamic client registration. It may be early days for this. The example given was that in the health realm, CMS exposes data through the FHIR API and wants to release access to anyone using a qualified OAuth client app by reputation.

Apparently we fell prey to Noah's Law! "Any conversation about decentralization eventually evolves into a conversation about reputation." <https://twitter.com/christophera/status/654106382967304192> It's been suggested that people interested in this topic are UNAnitarian blockheads. :-)

## ***Societies of Things***

**Wednesday 4C**

**Convener:** Phil Windley

**Notes-taker(s):** Phil Windley

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

### **# Observation**

- \* Social animals form dynamic relationships to accomplish goals without central planning
- \* This is what we want out of a useful Internet of Things

### **# Goals:**

- \* ZeroConf - interact without owner programming, etc.
- \* Independent - thrive in environments where we encounter and interact other independent agents—even when those agents are potentially harmful or even malicious

### **# Culture and Societies**

- \* Cultures are default decision systems
- \* Gharajedaghi defines civilization as follows:

...civilization is the emergent outcome of the interaction between culture (the software) and technology. Technology is universal, proliferating with no resistance, whereas cultures are local, resisting change with tenacity.

### **# Example: My Electric Car**

As a small example of this, consider the following example: suppose I buy an electric car. The car needs to negotiate charging times with the air conditioner, home entertainment system, and so on. The charging time might change every day. There are several hard problems in that scenario, but the one I want to focus on is group forming. Several things need to happen:

- \* The car must know that it belongs to me. Or, more generally, it has to know its place in the world.
- \* The car must be able to discover societies with a cultural fit (e.g. that there's a group of things that also belong to me and care about power management.)
- \* Other things in that society must be able to dynamically evaluate the trustworthiness of the car.
- \* Members of the group (including the car) must be able to adjust their interactions with each other on the basis of their individual calculations of trustworthiness.
- \* The car may encounter other devices that misrepresent themselves and their intentions (whether due to fault or outright maliciousness).
- \* Occasionally, unexpected, even unforeseen events will happen (e.g. a power outage). The car will have to adapt.

We could extend this situation to a group of devices that don't all belong to the same owner too. For example, I'm at my friend's house and want to charge the car.



## # Principles

- \* Decentralized and heterarchical
- \* Dynamic
- \* Event-driven and reactive
- \* Robust, perhaps anti-fragile
- \* Trust building
- \* Safety over security (protect rather than prevent)

## # Trustworthy spaces

- \* conceptual
- \* discoverable culture (we do power management negotiation, car's self-image aligns with this)
- \* default policies
- \* join and leave at will
- \* reputation - provenance and reciprocity

Culture provides a means for devices that are introduced to a household to self organize around common interests.

## # Picos

- \* Arbiters
- \* Legal can't override to achieve goals. Culture can be
- \* vulnerability tradeoff and trust
- \* translation between signals and protocols from different devices

## ***OpenID Connect RP Certification Hands-On***

**Wednesday 4D**

**Convener:** Roland Hedberg

**Notes-taker(s):** Mike Jones

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

In Attendance: Roland Hedberg, Edmund Jay, Mike Jones, Sascha Preibisch, Sampo Kellomäki  
William Denniss, Nov Matak, Sarah Squire, Mark Mucha, Greg Haverkamp

Roland went over the RP testing tool and how to use it

Documentation is at [https://dirg.org.umu.se/static/oictest/how\\_to\\_use\\_rp\\_test.html](https://dirg.org.umu.se/static/oictest/how_to_use_rp_test.html)

The code is at <https://github.com/rohe/oidctest/>

Can only test RPs that can use OP configuration discovery information

Path specifies behavior of test OP

Uses IP address of RP as correlation handle for requests

Logs at /log/<RP IP-address>/<id>

Logs are currently just appended to and not cleared

William Denniss asked for a way to clear a log

test\_rp/rp/cflows.py - Test configuration for Roland's RP code that he is using to test the tests

test\_rp/op/static/pathmap.py - Paths defining tests to run

Edmund Jay showed us running RP tests for his implementation

His test tool is at <https://connect.openid4.us:5443/phpRp>

A redirect\_uri used by his RP: <https://connect.openid4.us:5443/phpRp/index.php/implicit>

A log: [https://rp.certification.openid.net:8080/log/67.180.145.30/rp-id\\_token-bad\\_asym\\_sig\\_rs256](https://rp.certification.openid.net:8080/log/67.180.145.30/rp-id_token-bad_asym_sig_rs256)

An issuer: [https://rp.certification.openid.net:8080/rp-id\\_token-bad\\_asym\\_sig\\_rs256](https://rp.certification.openid.net:8080/rp-id_token-bad_asym_sig_rs256)

## ***Who Cares About Our Personal Data? Mapping Innovations and Showing the way...***

**Wednesday 4E**

**Convener:** Kaliya Hamlin, LaVonne

**Notes-taker(s):** LaVonne

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

Our goal was to generate discussion around mapping the personal data ecosystem. We were interested in learning about innovative projects, research, and businesses/startups addressing needs and/or filling in gaps in the ecosystem.

We opened the session asking people why they came

Digi.me talked about the Personal Data Economy and creating the "Internet of Me" - meaning anything where you are in the center.

He also talked about engaging large consumer packaged goods companies.

Doc shared that he had 10 tera bites of data - that there was a use value to this that was greater than a sales value. Commentary was also made that the only people currently buying it were messing it up. Look what happened with Big Data? McKinsey and IBM sort of swooped in.

There are some really Big Rat Holes sucked into a vortex.

Big Verticals such as Quantified Self

What is the Distribution? How do we get mass adoption?

95% of businesses are SMES (small and medium sized enterprises)

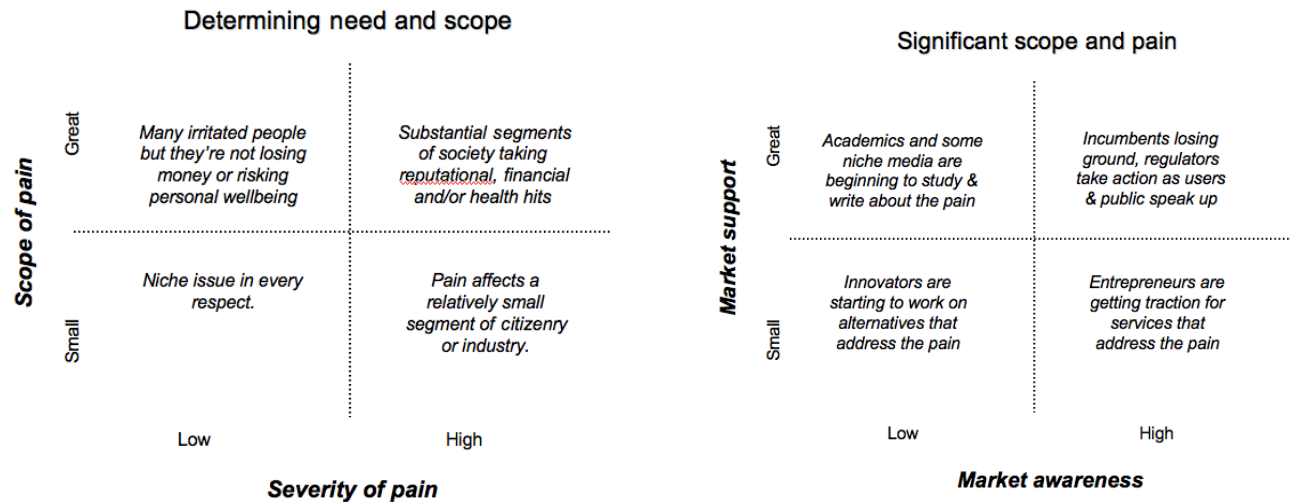
Exponential Growth in Alternative that is the more about exploitation of Personal Data than enabling people to access value from their data.

We need better ways of innovating around and deriving value from data (that honor the core principles of the personal data ecosystem).

Data ---> Info ---> Knowledge ---> Insight

Joe Andrieu raised the point that there is a big difference in the social contract between people/institutions and exchange value.

LaVonne outlined two matrices that innovators and entrepreneurs might use to understand where there are market opportunities. The first chart might be a starting point. It doesn't mean that someone innovating in an area where the issue is annoyance rather than financial pain but could be helpful in thinking about filling in the ecosystem overall. The second chart suggests you've identified which of the four quadrants in the first chart you're going to address. The second chart helps you figure out who your allies are and whether the timing is ripe to enter the market. Again, it doesn't mean you don't take action if urgency and strategic allies aren't available, just that it may be slower going and require more capital.



Julian described how he identified target markets for Digi.me by presenting the future vision for how personal data works and paying attention to who sits up and listens. There has been a marked change - about who sits up and listens. They must also be ready to take action and the pitch has to be sufficiently about business issues if you're pitching a business-to-business solution (presumably as compared to consumer fairness issues).

Digi.me is working to find 4 big customers who each have millions of users. They have infrastructure that can connect a bunch of verticals with a Horizontal technology and strategy.

Innovation ---> Commercial Opportunity

Julian suggests there are 500 Companies/startups currently in the Personal Data Space (ctrl-shift is on the list)

Ask companies about what they are doing - do a survey of them - What does they do? What are they targeting and why. Where is the thrust and how are they financing themselves and making money.

We talked about the telco difficulty in leveraging data. Kaliya highlighted the work of the Rethinking Personal Data Project and how it arose out of telco's trying to figure out how to "give people back their data" and then license from them to provide them value.

It was discussed how many are mentally locked-in. Julian talked about the card presentations he does <http://www.digi.me/video>

We discussed the differences between services and infrastructure.

We talked about cooperating together and working on something in common.

Talking more. Luk highlighted that we needed to be thinking about pre-competitive Cooperation.

There was interest to start scheduling regional gatherings where innovators could get together to share experiences, learn more about markets and technologies, and help the ecosystem mature and thrive.

## ***SCIM Credential Management Discussion***

**Wednesday 4H**

**Convener:** Phil Hunt - Oracle

**Notes-taker(s):** Bill Mills - Microsoft/Skype

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

SCIM, Password management, password suitability.

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

- Exploration of SCIM vs. password policy enforcement.
- Password vs. other authenticators and how to handle them
- Extending the schema to support various policy.
- Is SCIM going to be an authentication engine.
- Does SCIM become a validation engine?
- Phil: Let's look at this for lessons learned. This draft may not go forward as is.
- Using SCIM as a back channel for account event propagation is potentially interesting.

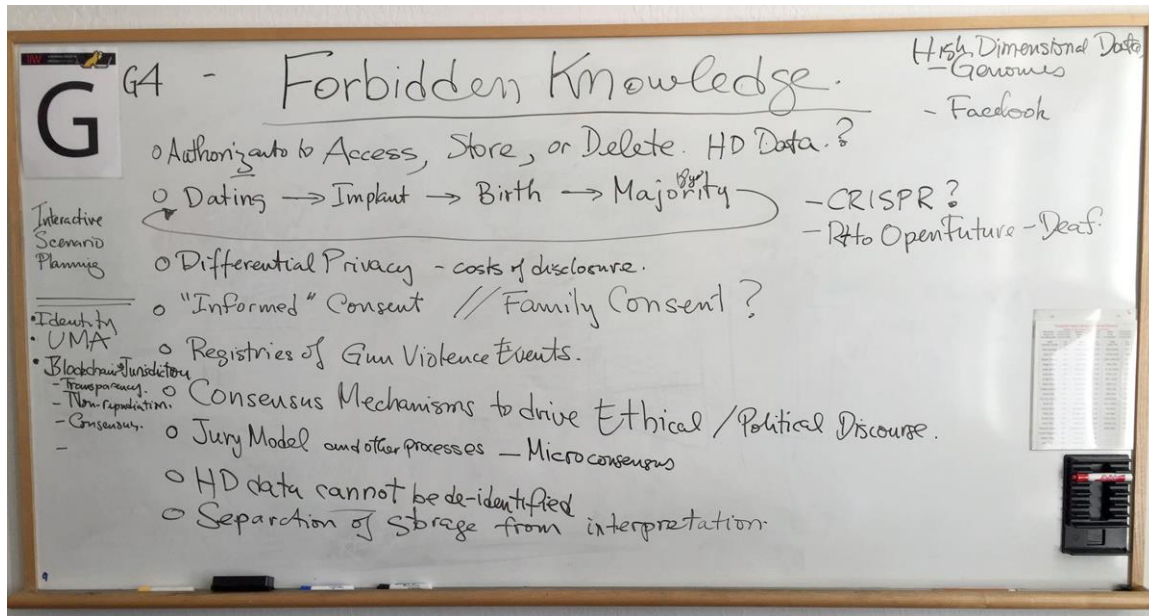
## Forbidden Knowledge

Wednesday 4G

Convener: Adrian Gropper

Notes-taker(s): Adrian Gropper

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



Genome / Facebook Data Cycle: Dating > Implantation > Birth > Majority > Dating

Separation and control of Storage, Access, and Deletion

IIW Topics to consider:

- Identity
- UMA
- Blockchain
  - Transparency
  - Non-repudiation
  - Consensus

## ***Non-Person Entities***

**Wednesday 4I**

**Convener:** Jim Fenton

**Notes-taker(s):** Susan David Carevic

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

Identity Proofing

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

Methods:

Remote:

KBA: Knowledge Based Access: questions – to assure identity – example: social security administration.

Data is out there – KBA not the best method, due to availability of data.

Trusted 3<sup>rd</sup> party certificates

Biometric + Doc Auth

Social Score/trust\ vouching for persons

Fraud signals

Virtual In-Person:

Hasn't been evaluated well – how clear must a video be, to ensure person is the same as picture in an ID card – if they are holding it up virtually.

In person:

works well, but is inconvenient for users and expensive process, but highly accurate, less scalable.

Other flavors:

Identity.com: Uses sequential upload followed by a verification process. (NetVerify). AirBnB uses NetVerify.

We need to fully understand the in-person proofing process to be able to create an alternative solution. Here is what happens during an In Person Session:

- Biometric screening
- Records check
- Proof of address, name, DoB
- Credit style audit checks
- Personal feeling if they are lying
- Interview process to verify data
- Original identity document position/showing

Proofing of data usually a government role – not sure I trust companies to do this/this role. Governments shouldn't outsource this responsibility. Personal feeling should not be criteria.

If there a better way to do Identity Proofing virtually or make Remote Identity proofing better?

- We can't count on federal agencies to do this

What can be done better to improve remote identity proofing?



- Need to consider level of assurance needed: What LOA are we trying to talk about: All of them.

What ways are there to do identity proofing remotely:

- Account activity: Answer question about recent transaction: but only binding to a Bank's log. Only proving you have access to the logs.
- Telesigning: Call API – they report on where person is/person associated with the phone number – if this matches the person using a credit card, you've verified identity.

In U.S. it all comes down to government documents?

In Canada: Office of Vital statistics

There is Federal Identity and State Identity in the U.S.

Federal Assurance Exchange: Credit bureau information.

Problem is how to verify the document remotely.

The fact that you have a drivers license, doesn't necessarily mean that it identifies you.

Telesign: Creating a full loop – if that is correlated with an ID. Problem is any PBX can emulate a telephone number.

- How can that get hijacked?
  - Because at any point you can redirect a phone number to another destination.

Does a telecom do any identity proofing before giving out a telephone number? No – just need to be able to pay.

Issuance of credential by U.S. Mail? Verification of address: They mail a code or some other information. There is also registered mail requiring a signature.

Derived Proof: Create registration process that provides sufficient binding to proof. Selfie + ID Card scan, biometric check, send to DMV – and provide a score of likelihood person is who they say they are. Are DMVs allowed to share information? - they only share an opinion, don't need to send out data.

Why is there a need to send packet to DMV? Privacy measure. More difficult to compare facial features to a copy of a card with security features over the face.

DMV is not reliable source of identity information? – yes – because we call them that.

Few other things that could be used for proofing: Trust cloud\social score. LinkedIn: Professional resume with verification of employment provides proof that someone is a real person. : concern: more than one identity: for example, for voting—need to ensure voting only once.

Closing the loop is the only way to prevent at-scale attacks.

## ***UMA: Interop Testing, ARP Use Case***

**Wednesday 5C**

**Convener:** Roland Hedberg

**Notes-taker(s):** Roland Hedberg

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

Roland described the UMA use case that he and his group are going to implement.

The setup is that we have Identity providers, IdP and AA for SAML and OP for OIDC, and there are service provider who wants information.

Which information is released to which service provider is governed by what is called attribute release policy.

This policy is set by at least two parties:

- 1) an administrator
- 2) the user who's identity information is released

Right now this is mostly done within the identity provider we are looking at putting it outside such that all identity providers could be governed from one and the same authorization server. We also would like to use a standard protocol (UMA) for doing this.

After presenting this layout a discussion was held about:

- what scopes really means,
- what kind of information that can be handled by UMA,
- the binding of several resource servers to one authorization server,
- resource set naming

and so on...

## ***Cradle to Grave***

**Wednesday 5G**

**Convener:** Akiko Orita

**Notes-taker(s):** Susan David Carevic

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

Consent, Agency Law, Notice, Transparency, Permission

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

Can we ban the word "consent" - its misleading and being abused – as a first step of the solution. An alternative might be "Notice" or "transparency"

Contract/Agreement: Responsibilities on both sides.

Are you saying that Consent is vendor driven? The way its used is being pushed by the provider.

Should we call it “rights negotiation”? In policy language it is permissions and obligations.

Notice/transparency and permission/obligation are two factors that were part of the “C” word

Who is the owner: They who have the right to delete it? Owner is a legalistic concept. What about the stuff that can’t be deleted? Officials who have my data and can’t delete it – Do they own my data or do I and they have access rights to them? If you were the owner would you have the right to tell them to delete it?

Does owner have access/use? - Disagreement of that as a definition.

Agency Law:

- Principal
- Agent (Lawyer): surrogate becomes agent
- Third parties: Get’s license
- Good Faith: quality of description of the icons
- Notice: transparency

License: Permission/obligation

Who would be the owner of a deceased person’s data – for example on facebook.

Still need to be able to give access/usage rights.

Who controls the data: vague – UMA splits control between authorization (Agent) server and resource server (Third party).

Consent: Granularity doesn’t exist: User driven by default agreement.

Gem from VRM Session: Icon: What vs. Why: Why don’t you label the icons with why you are asking for the what? – if there isn’t a reason why – no one will do it.

Owner can forcibly argue that he owns the data. Derived data: does the company who derived the data own the data, or since the derived data came from the person giving the data –does that person own it?

Businesses in UK to provide style advice: Customers give them information with their permission to use data to give them advice. They have built a “Secret” algorithm that is giving a customer value. Why should the algorithm be the customers?

Counterexample: Mayo Clinic – gives IBM Watson 1 million health records: Watson turns data into secret algorithm, which provides a diagnosis. Before IBM Watson, the algorithm would have been tested, printed in a journal. Can this algorithm be made secret, just because it’s electronic now? -- doesn’t work for medicine, law or Wikipedia. ... maybe it does work for medicine: New drug testing: patent for drug for 15-20 years.

Originating person: can I have a look at all of the data: why: understand cancer better. If we try to remove from consent all economic incentives, nothing is going to happen.

We need to get rid of identities in this: use metadata instead of identities.

## What Does “Log Out” Mean?

Wednesday 5H

Convener: Annabelle

Notes-taker(s): William Denniss

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

- By “logout” do you mean the user is clicking a “logout” button?
  - where, is it on the RP, OP?
- Can we kill logout?
- Consumer vs enterprise. Different behaviors in each environment.
- “End this session” vs “End all sessions”
- Step-up auth. Amazon has a system where you can perform sensitive actions after sign-in/reauth, that expire after a time, but the user is still logged-in and can view less sensitive features like wishlists, etc.
- Logged out / logged in – sometimes the state is carried, but users may think they’re being tracked
- User expectations vs service expectation – users might not realize that there is always a session cookie whether it’s logged out or not.
- What is the intent of logging out?
  - Is the user trying to clear all remnants of their data (e.g. internet cafe)
  - or, are they just trying to switch account
- Anecdote: Hospital app had a 15min logout policy, so they hired an intern to go around and press the control key to keep the machines logged in. As a result every terminal was always unlocked, and they had less security than if they didn’t have the logout policy.
- User question: when I logout, does it mean I’m logged out everywhere.
- When you use federated login, then you logout of the RP – you’re still logged in to the IDP! That can be a surprise.
  - By the same token, the user may be surprised if they logged into a second RP, and had to sign-in again.
  - Amazon’s IDP doesn’t save login state when you do an RP-initiated login
- Amazon’s IDP implementation has no SLO (Single Log Out) communication between the RP and IDP for logout events. One reason is that you’d have to ask to the RP to implement it, and we don’t know what experience the RP would have.
- Lock after inactivity would be better than logging out, as you wouldn’t lose the session state (e.g. Schwab).
- Desktop SSO – when you close the client, what does it mean? I just want to kill the client to avoid getting notifications that interrupt my call – but sometimes these apps will stay in the background and continue notifications.
- Session used to mean something: users were instructed to close the window when they were done, but then along came chrome
- Incognito windows and profiles – new approaches to data management, to kill all traces of a user / segregate data into the different users that share a device
- Users may need to be able to signal their intent to stay logged in
  - but then those buttons are confusing and don’t always work
- When you logout of an RP, what does that mean to the IDP session? When you logout of an IDP what does it mean to the RP?
  - do you want a “side effect” of signing-in to an RP

- Layers of logins
  - RP <- logout here and you'll get logged back automatically due to the next layer down
  - IDP
  - SSO
  - Desktop Session
- Legitimate cases for trusted logout (e.g. violated security policy) should be via the backchannel
- Should the RP have an "emergency button" to signal full logout everywhere
  - front channel spec has facilities for a user confirmation of this
- Lots of skepticism for the ability of an RP signal to log the user out of other locations. "Single sign-out works well until it doesn't"
- Should an auth context switch at the IDP (e.g. multi sign-in at Google)
  - what does that mean for RPs if the auth context switch happens at the IDP?
- How much mileage can we get to teach users to logout where they logged in?
- Device centric user experiences: why do you logout at all? Segregate data through device management, in the internet cafe situation "I want to click on one button and kill everything", not be a janitor and go around logging out everywhere

## **Security Loft**

**Wednesday 5J**

**Convener:** Mike Schwartz

**Notes-taker(s):** Mike Schwartz

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

SecurityLoft will promote software and services that support modern application identity security standards, initially OpenID Connect, UMA and SCIM.

The site will include a free certification program for the above mentioned protocols. It will also provide links to organizations offering third-party certification services.

Targeted launch date for SecurityLoft is 11/30/15. The domain will be <https://securityloft.org>  
A press release with initial participants will be announced then.

This will be a volunteer organization. Gluu will sponsor the hosting of a server. For more information, contact Gluu at <http://gluu.org/contact>

## ***Citizen ID Cards: white paper concepts/good designs***

**Wednesday 5L**

**Convener:** Kaliya Hamlin

**Notes-taker(s):** Kaliya Hamlin

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

I lead a session about the idea of writing a white paper specifically aimed at government officials (globally) [and their staffs] considering options for Citizen Cards / eID / Drivers Licenses to understand core concepts related to such cards along with outlines of good designs that have been developed (Such as British Columbia's)

A few people came - we had a good discussion but it was not as in-depth as I thought it could have been - I shared what I was doing and people agreed but I didn't gain much insight beyond where I already was. Which is fine for an open space session.

I will likely work on this in the coming months.

## Thursday October 29

### *The Permanent Web*

Wednesday 1A

Convener: Kevin Cox

Notes-taker(s): Kevin Cox

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

Link from Kevin Cox -

<http://www.welcomer.me/welcomer/blog/2015/10/26/welcomer-a-primitive-prefrontal-cortex-for-electronic-memories>

### *ABAC - Attributed Based Access Control*

Thursday 1G

Convener: Don McNeece

Notes-taker(s): Susan Carevic

Tags for the session - technology discussed/ideas considered:

Role Based Access Management, Attribute Based Access Manager, RBAC, ABAC

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

The question first came up of what is an attribute? Is it a role? Or any value associated with the user

Example Scenario was presented:

- Role based Access Control (RBAC): Roles/groups set up. User wants access to a resource. Typically, roles or groups are created for the resource to look at. Person belongs to Employee can view HR information.
- Process runs nightly to take attributes from a database and assign persons into roles based on their attributes.

Attribute Based Access Control:

Challenges:

- Agreeing on attributes and deciding what they mean across organizations is one of the most challenging parts.
  - One way: associate the role with a function: each role as an assembly with functions as opposed to membership.
- Role sprawl is the problem.

Attribute Characteristics in scenario:

- don't have to do with role, these could be contextual, such as time/location..
- Contextual information



- Authority
- Entitlement
- Applies to people and not devices.
- Attributes can negate rights as well as grant

Goal:

- What do I need to know about someone for them to be able to do X.
- Minimum set of data to be able to resolve the person..
- Need to figure out how to map attributes to privileges.

Problems with Roles (RBAC):

- assumption that there is a top down entity that can figure out what people need. Role explosion
- Delays
- Permissions to attributes (applications don't have access to attributes)
- Mapping attributes to permissions
- Reduced visibility: nothing ties to group name what people in the group are necessarily allowed to do.
- Roles invariably overprovision employees. They will most likely receive resources they don't need.
- Roles: name means different things.. imprecise.

ABAC:

- Policy
- Common Words\definitions
- Could lead to an "attribute explosion"
- Applications need to be able to understand the attributes and API of applications.

Policy:

- Trying to find a policy: does this person have permission to do this type of action.
- Policy explains what attributes are needed to be able to do it.
  - So each set of attributes are associated with a policy.
  - Each set combined is effectively a role.

Some terms and definitions:

Role: collection of permissions

Groups: collection of users

Roles can be attributes

JWT pronounced "JOTS"

Advantage of ABAC over Roles:

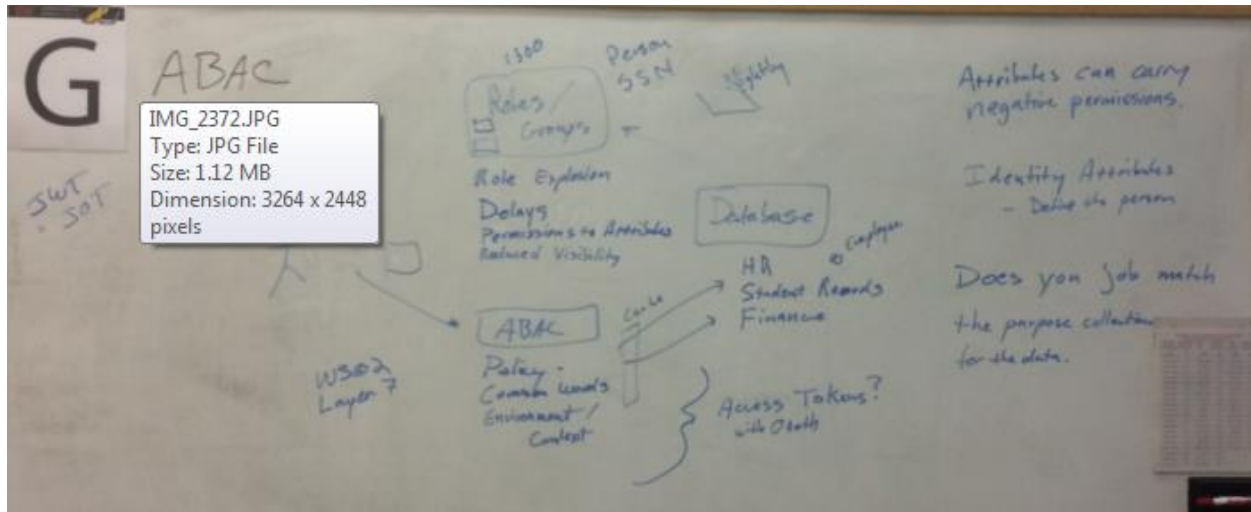
Roles have "combinatoric" explosion problem. Set of attributes don't have to be thought of as a role.

When people change jobs, they get assigned to a different set of roles..eventually, attributes need to be changed.

Recommendations:

- Delink to HR database. So that access can be based on relationships in the moment.

- Approach Alan prefers: Use your attributes roles identities to get a set of access tokens. Send the access tokens along with the request, so that the service is free from having to figure out the attribute compilations.
  - Example: Navy Ship: policy calculation on shore, and sent back to ship. Use OAuth, go to AR for access tokens and use for access decision. Access token needs to include what the token is good for/what kind of requests. Only piece to add are the contextual pieces. .. doesn't work for dynamic roles – in this case every RS becomes an AS.



## Digital Identity 2nd Edition / Non-Person Entities

Thursday 2G

Convener: Phil Windley

Notes-taker(s): Susan Carevic

Tags for the session - technology discussed/ideas considered:

Identity, Publishing, Topics

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

Some History: Began with Steve Gillmore: Podcast on Identity – after that call, decided to do an identity workshop. Book written in 2004. Mostly focused on Enterprise Digital Identity.

Will the book be written for a different audience: Yes,

Goals:

- Place where people get an introduction to digital identity as we talk about it here. A holistic approach. Shouldn't be a how-to book. Give people an idea of how identity fits into a larger picture.
- Audience: Org leaders, Product Managers, Engineers/Business side, Not for individual who is worried about their identity. Marketing

- How should gap be bridged between corporate and humanistic space: Expand to include product managers and developers.. What do customer's expect
- Should it be for policy wonks? Should be useful information to them as background information.
- There are cross-cutting areas that speak to a wide audience.
- How much should the book go into the human rights side of things?

Would be great to have a book that explains how advanced concepts of these technologies work so that decisions can be made. How should we think about the involvement of the user culturally? Think of identity –in the plural. Not necessarily in the interest of the person to link them.

By defining what the problem is, product managers will come up with different solutions. Identity potential readers, and build a matrix of what would interest them. Then they could be guided on what chapters.

Underpinning of book needs to be the policies, principles, identity proofing.. that ties everything together. Why do I care? Should come out in the book. Start with principles of Fair practices.

Topics:

- Trust Frameworks\Federations: nobody understands what trust frameworks mean – call it something different.
- Architectural models
- Protocols: different roles within OAuth, needed to understand the framework. Protocol vocabulary. Diagrams of each
- Reputation: identity in the context of the sharing economy\linking to trust.
- Set of things that a service provider would expect to conduct business.
  - Authentication Strength of token
  - Set of information
- Anil's framework!!
- Difference between payload and protocols – why does anyone care?
- Mediation to put in place to have less parts – what makes integration easier, what are the architectural components. Common underlying themes – how do current technologies measure up or handle them.
- Authorization/Access Control: slightly deeper then with first book.
  - Also about keeping track of products, not just customers.
- Relationship/convergence of payments
- Decentralized/rootless directories and ledgers (Blockchain as example)
- Defining “attribute overreach” (-- why should my refrigerator control my garage opener.)
- Shaming – should a device be able to shame someone (publicly) – won't necessarily know who the information has been shared with – shouldn't this be addressed in design?
- Real world identities – identities are complex.. what makes up an identity. Sovereign source of identity vs. government identity – connects all of these pieces: societal aspect: human questions being addressed. How should technical people think about

this, principles we want to espouse. How should companies be relating to their customers.

- How do company interactions with customers impact the company:
  - Brands issue identities about their customers: consumer isn't involved in the issuance of the identity: Brands: stitch identities together to sell more. Don't listen to what kind of a relationship that sets up.
    - Revenue extraction
    - 360 view: relationship maintenance
  - Most not very "bright" with the math/algebra. Short focused.

## OTTO Private BlockChain Help



Thursday 2H

Convener: Mike Schwartz

Notes-taker(s): Judith Bush

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

OTTO H (I think) Date: 2015-10-29

| Notes  |  |
|--|--|
| <p>XML sig broken<br/>but what about json signing</p> <ul style="list-style-type: none"><li>• RFC common indexing protocol</li><li>• Blockstack has an index search</li></ul> <p>bob.org/my/metadata</p>  <p>bob.org/my/metadata - fed1</p> <p>signed vs of /my/metadata - fed2</p> <p>Summary signed vs of</p> | <p>1 Hate XML <math>\Rightarrow</math> JSON <math>\leftarrow</math> Four requirements on top of SAML</p> <p>2 Better query</p> <p>3 scale</p> <p>4 Fed management challenge</p> <p>Link to the blockchain location<br/>Hash is blockchain One Name</p> <p>• Merkle tree/certificate</p> <p>hash in URL</p> <p>JSON Web Token for the client</p>  <p>AuthZ Request</p> <p>metadata Indices</p> <p>Software Stack</p> <p>Conclusion: Question whether the blockchain is "over kill" for solving the federation scale and management issues.</p> |

## ***The Cultural Barriers to Privacy***

**Thursday 3A**

**Convener:** Jeff Stollman

**Notes-taker(s):** Jeff Stollman

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

For my Thursday session 3A on Cultural Barriers to Privacy, I represented a study by the Ponemon Institute which highlight disparities among IT professionals based on their nationality.

The study highlights a cultural diversity that we are often trying to serve imagining that the general public is just like us. This is a risky assumption.

Here is a link to the presentation: <http://www.secureidentityconsulting.com/wp-login.php?loggedout=true>

## ***Is Identity Always On***

**Thursday 3G**

**Convener:** Vidya Jayaraman

**Notes-taker(s):** Vidya Jayaraman

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

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

In today's digital world, customers are seeking brand experiences and solutions that are simple, proactive, personal and efficient. In order to meet these customer needs, the key is to identify customers in that specific context, and use machine learning techniques to progressively build on that customer knowledge and needs. It can be viewed as five steps as shown in the attached illustration:

- Identify – this may be a customer-specified identifier like – name, address, email, phone, social or device-rendered such as cookie, IP address, device ID, etc.
- Context Filter – this step drives most of the personalization as this records all context signals with the identifier at every instance. Signals can be as far as we want to go. Examples of signals include, location, time of day, duration of visit, length of scroll, frequency of use, etc.
- Profile – this is where we use machine learning to compare signals across a broader group of identities and develop profiles at an aggregate basis for segmentation and targeting purposes
- Map – this is picking the solutions and communications based on the aggregate profile
- Serve – this is rendering the solutions and communications using contextual signals to personalize the delivery of the experience

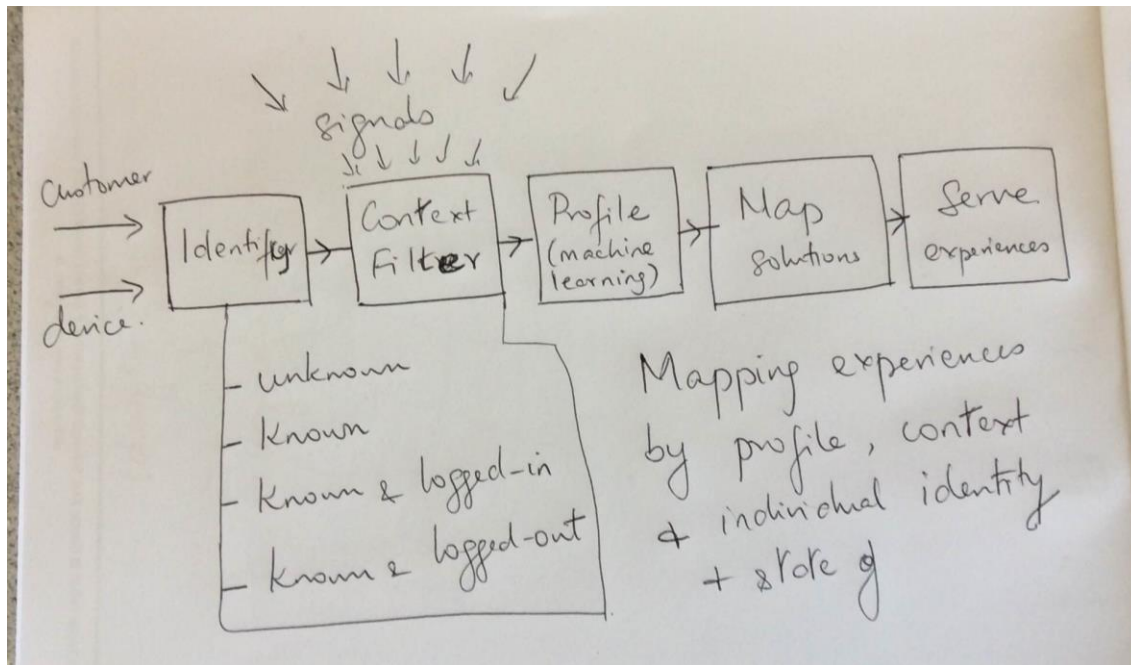
### Key discussion points/Take away:

At least four different states of customer identification exists:

- Unknown (no identifier)
- Known (generic customer or device identifier, e.g. cookie, IP address, device ID)
- Known Logged-in (customer identified, e.g. account number, username)
- Known Logged-out (customer identified but has signaled a lower engagement state, e.g. reverts back to cookie/device ID but additional info is available)
- Some points to keep in mind during implementation:
- Identification is fluid and contextual (e.g. work vs. personal identity)
- Signals are implicit and gathered; hence requires careful use of signals to avoid unintended consequences/awkward customer experiences
- Balancing the use of contextual signals (guess work) and 1<sup>st</sup> party inputs to be proactive; use this to differentiate the journey for different states of identification
- Logged out states still carry the customer identity/identifiers. So 'log out' by customer is a signal to the company that the customer is changing states. So the experience should flex based on that signal.

It was a very informative session for me and thought you might also find it interesting. I'll be happy if anyone wants to discuss this any further.

Thank you, Vidya





## **Blockchain Governance**

**Thursday 3H**

**Convener:** Dave Shepard

**Notes-taker(s):** Guy Onename

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

Magic internet governance

——> Voting |——> Anonymity

——> Consensus |——> Pseudonymity

Auditing

Blockchain

1. Immutable system of record

2. Ordered

3. Consensus mechanisms

4. Permissionless

Bad actors make system anti-fragile

Decentralized/authority-less

What is the overall cost for maintaining the bitcoin blockchain?

[Christopher Allan]

- There is a transaction fee

[whiteboard]

Amount of bitcoin miners receive is;

—————

:arrow\_lower\_right:

25BTC (12.5BTC in 2016)

which gets cut in half every 4 years

- Bitcoin value is not going up which is causing a problem

[Dave Shepard]

If you want blockchain based governance systems. You get transparency and no humans can mess around with it.

[whiteboard]

- Transparency

——> Automated

[Christopher Allan]

Permissionless blockchains - systems are baked in to the system such as Ethereum

Permissioned blockchains - relying on the miners/consensus mechanism

There are hybrid model Permissioned and Permissionless blockchains

Sidechained blockchains are tied to Permissioned blockchains

Sidechains are pegged at a certain price and will always be the same

Can you change parameters of a blockchain?

Lightcoin is the second largest blockchain

Proof of stake

-Stellar

--- Governance

--- Proof of stake

— Proven

[Jude Nelson]

Permissionless is set at a extremely high price

[Kaliya]

Let's not forget about governance out side of the technology

[Dave Shepard]

[whiteboard]

space —> voting/consensus

Turkey has created a taxi system that uses voting system for the union. Bitcoin could be used for something like that.

Ordering is necessary to achieve consensus

- blockchain has to be solve the ordering problem then the consensus problem

[Christopher Allan]

Don't need to have perfect consensus

Voting on the blockchain might be too soon

- Too difficult due to algorithm faults

Bitcoin is a public ledger. You can see the transaction but not the person doing the transaction (unless you're a very large state actor). Hashes are used once per transaction.

UREA was making currency for governance

Paxos has been proven correct. [Jude Nelson] there's a paper on it.

[Christopher Allan]

I believe there is not a proven governance model for all blockchains

- There's a huge risk to the community if there is a "hard fork"

- They do not like federated systems

- It reminds me about Kaliya's complaint which is why white male's version of identity. Blockchain Identity has a lot to offer to this community.

[Mehdi - Oauth]

Augur uses crowd bets to produce predictions of war for example.

[Christopher Allan]

- There are various versions of consensus - 100% consensus, consensus +1, etc.

- If we can get a large sufficient group of people to vote, we can use that to get a better voting system

lifewithalacrity - Christopher Allan's Blog (edited)

## **Customer Funding**

**Thursday 4G**

**Convener:** Kevin Cox

**Notes-taker(s):** Kevin Cox

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

Link to a blog post by Kevin Cox

The Implications of Giving Customers Control Over Their Online Information

How Crowd Funding Came of Age

<http://kevinrosscox.me/2014/07/07/has-crowd-funding-come-of-age/>

## ***OIDC Federation for Higher Ed***

**Thursday 4H**

**Convener:** Roland Hedberg

**Notes-taker(s):** Roland Hedberg

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

Roland described four problems that he thought should be addressed before OIDC can be used in a Higher Ed Identity federation.

### 1) Attributes

The set of attributes provided in the OIDC standard are not sufficient so someone preferably REFEDS (<https://refeds.org>) should do that.

### 2) Scopes

A number of scopes should be registered:

- a) To signal that Higher Ed attributes are expected from the UserInfo endpoint, this could be named 'edu'
- b) scopes that matches the entity categories that are used in Higher Ed identity federations.

### 3) Allow for semi-static client registration

Right now there are two choices for client registration, static or dynamic.

We would like to have something in-between where the RP can send some information (in the form of software statements) during client registration that allows the OP to know who the RP belongs to and what it is allowed to do/see.

### 4) Allow for off-line verification of 'documents' that are sent around.

Things like provider configuration, client registration and client/provider keys are now just JSON documents. There ought to be ways of signing these such that anyone disregarding how it was received can verify the correctness of the document.

Discussion followed.

## ***Beyoncé as a Service***

**Thursday 5A**

**Convener:** Justin Richer, Christopher Allen

**Notes-taker(s):** Justin R, Christopher A (paper)

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

PDF of notes : <http://kantarainitiative.org/confluence/download/attachments/17760302/beyonce-as-a-service-session.pdf?api=v2>

### **Here are the new lyrics to the song Justin performed in closing circle on Thursday**

All the public people! (All the public people!)  
All the public people! (All the public people!)  
All the public people! (All the public people!)  
All the public people!  
Now put your side up.

Every night I verify in my bed,  
Lost in a fairytale.  
Can you hold my tail and be my guide?

Agents filled with keys cover your skies.  
What kinda dream is this?  
You could be a distributed chain or an immutable block.  
Either way I don't wanna link without you.

Coins, we run this motha (yeah!)  
Coins, we run this motha (yeah!)  
Coins, we run this motha (yeah!)  
Coins, we run this motha (yeah!)  
COINS!

Yes! So transparent right now,  
Most incredibly transparent.  
Oh! So transparent. Oh! So transparent.  
Yes! So transparent right now.

All the agents who are independent,  
Throw your head at me!  
All the agents who makin' money,  
Throw your head at me!  
All the agents who truly feel secure,  
Throw your head at me!

Tonight I'll be your transparent hash.  
I'm callin' all my coins.  
I know you want my purple tail.  
Tonight I'll be your transparent hash  
I'm callin' all my coins.

Who run the world? Coins, we run this motha - yeah!  
Who run this motha? Coins, we run this motha - yeah!  
Who run the world? Coins, we run this motha - yeah!

## ***Cradle to Grave***

**Wednesday 5G**

**Convener:** Akiko Orita

**Notes-taker(s):** Susan David Carevic

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

Consent, Agency Law, Notice, Transparency, Permission

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

Can we ban the word “consent” - its misleading and being abused – as a first step of the solution. An alternative might be “Notice” or “transparency”

Contract/Agreement: Responsibilities on both sides.

Are you saying that Consent is vendor driven? The way its used is being pushed by the provider.

Should we call it “rights negotiation”? In policy language it is permissions and obligations.

Notice/transparence and permission/obligation are two factors that were part of the “C” word

Who is the owner: They who have the right to delete it? Owner is a legalistic concept. What about the stuff that can’t be deleted? Officials who have my data and can’t delete it – Do they own my data or do I and they have access rights to them? If you were the owner would you have the right to tell them to delete it?

Does owner have access/use? - Disagreement of that as a definition.

Agency Law:

- Principal
- Agent (Lawyer): surrogate becomes agent
- Third parties: Get’s license
- Good Faith: quality of description of the icons
- Notice: transparency

License: Permission/obligation

Who would be the owner of a deceased person’s data – for example on facebook.

Still need to be able to give access/usage rights.

Who controls the data: vague – UMA splits control between authorization (Agent) server and resource server (Third party).

Consent: Granularity doesn’t exist: User driven by default agreement.

Gem from VRM Session: Icon: What vs. Why: Why don’t you label the icons with why you are asking for the what? – if there isn’t a reason why – no one will do it.

Owner can forcibly argue that he owns the data. Derived data: does the company who derived the data own the data, or since the derived data came from the person giving the data –does that person own it?

Businesses in UK to provide style advice: Customers give them information with their permission to use data to give them advice. They have built a “Secret” algorithm that is giving a customer value. Why should the algorithm be the customers?

Counterexample: Mayo Clinic – gives IBM Watson 1 million health records: Watson turns data into secret algorithm, which provides a diagnosis. Before IBM Watson, the algorithm would have been tested, printed in a journal. Can this algorithm be made secret, just because it’s electronic now? -- doesn’t work for medicine, law or Wikipedia. ... maybe it does work for medicine: New drug testing: patent for drug for 15-20 years.

Originating person: can I have a look at all of the data: why: understand cancer better. If we try to remove from consent all economic incentives, nothing is going to happen.

We need to get rid of identities in this: use metadata instead of identities.

## ***What Does “Log Out” Mean?***

**Wednesday 5H**

**Convener:** Annabelle

**Notes-taker(s):** William Denniss

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

- By “logout” do you mean the user is clicking a “logout” button?
  - where, is it on the RP, OP?
- Can we kill logout?
- Consumer vs enterprise. Different behaviors in each environment.
- “End this session” vs “End all sessions”
- Step-up auth. Amazon has a system where you can perform sensitive actions after sign-in/reauth, that expire after a time, but the user is still logged-in and can view less sensitive features like wishlists, etc.
- Logged out / logged in – sometimes the state is carried, but users may think they’re being tracked
- User expectations vs service expectation – users might not realize that there is always a session cookie whether it’s logged out or not.
- What is the intent of logging out?
  - Is the user trying to clear all remnants of their data (e.g. internet cafe)
  - or, are they just trying to switch account
- Anecdote: Hospital app had a 15min logout policy, so they hired an intern to go around and press the control key to keep the machines logged in. As a result every terminal was always unlocked, and they had less security than if they didn’t have the logout policy.
- User question: when I logout, does it mean I’m logged out everywhere.
- When you use federated login, then you logout of the RP – you’re still logged in to the IDP! That can be a surprise.
  - By the same token, the user may be surprised if they logged into a second RP, and had to sign-in again.
  - Amazon’s IDP doesn’t save login state when you do an RP-initiated login

- Amazon's IDP implementation has no SLO (Single Log Out) communication between the RP and IDP for logout events. One reason is that you'd have to ask the RP to implement it, and we don't know what experience the RP would have.
- Lock after inactivity would be better than logging out, as you wouldn't lose the session state (e.g. Schwab).
- Desktop SSO – when you close the client, what does it mean? I just want to kill the client to avoid getting notifications that interrupt my call – but sometimes these apps will stay in the background and continue notifications.
- Session used to mean something: users were instructed to close the window when they were done, but then along came chrome
- Incognito windows and profiles – new approaches to data management, to kill all traces of a user / segregate data into the different users that share a device
- Users may need to be able to signal their intent to stay logged in
  - but then those buttons are confusing and don't always work
- When you logout of an RP, what does that mean to the IDP session? When you logout of an IDP what does it mean to the RP?
  - do you want a “side effect” of signing-in to an RP
- Layers of logins
  - RP <- logout here and you'll get logged back automatically due to the next layer down
  - IDP
  - SSO
  - Desktop Session
- Legitimate cases for trusted logout (e.g. violated security policy) should be via the backchannel
- Should the RP have an “emergency button” to signal full logout everywhere
  - front channel spec has facilities for a user confirmation of this
- Lots of skepticism for the ability of an RP signal to log the user out of other locations. “Single sign-out works well until it doesn't”
- Should an auth context switch at the IDP (e.g. multi sign-in at Google)
  - what does that mean for RPs if the auth context switch happens at the IDP?
- How much mileage can we get to teach users to logout where they logged in?
- Device centric user experiences: why do you logout at all? Segregate data through device management, in the internet cafe situation “I want to click on one button and kill everything”, not be a janitor and go around logging out everywhere



## ***What's Next for IIW***

Thursday 5F

Convener: Doc Searls

Notes-taker(s): Kaliya H

Tags for the session - technology discussed/ideas considered:

#IIW #Identity #InternetIdentityWorkshop

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

Attendance grew since IIW20 when it was at a low of 135 and, we could grow by 40-60 people. We talked about ideas for outreach and spreading the word.

Be Supportive of more Local Connection between events

IIDinners -> leading into IIW thinking about topics for IIW

They can be an opportunity to connect with other related niches

Privacy

Privacy Lawyers

Security

IoT

AdTech

AdBlocking

Blockchain

GamesNight? - the women in Seattle already do this

Identity Conference Evangelism, word of mouth -> people invite new people

¥ Ping

¥ Forge Rock

¥ Gartner IAM

¥ DIDW2?

Developer Events

API Days - have an ID track OR RESTfest

Indiewebify.net / Ben – Known & Kevin Marks

Meetup Groups we could reach out to.

LinkedIn Groups focused on IAM and maybe blogging there.

Pods/Groups coming from other countries together

Japanese organizes by framing it as a IdM specialist study trip to silicon valley

What could make this more compelling visiting companies on Friday/Monday

Survey - leading questions

Host a monthly Twitter Chat? (idea since the event that Kaliya had) Here is an example of how they work/mechanics from ChangeMakers

<https://www.changemakers.com/blog/fabricofchange-twitter-chat>

Explaining better what happens and what goes on at IIW.

- The topic is so broad some people "should be here" but don't know
- Who is at IIW - High level thinkers who are visionary.
- Why are they here? They Love the unconference format and the Dynamic it brings.
- Create a WordCloud from the Book of Proceedings.

As topics come in can we curate them?

MindMap Past and current events

Who people are like "speakers" presented

Use a Panel Picker Like tool to input ideas for sessions

Ideas to broaden participation

Fellowship Program from sponsors for attendees.

Cousin Events

European Workshop for Trust and Identity (Austria/Europe)

Identity North (Canada)

AustralAsia???

Social Event around IIW Pre/Post

Women's Spa Day? (Kaliya has thought of this on the weekend before or after)

Consider Pre-event with "speakers"

## Thank You to All the Fabulous Notes-takers!

There were 95 distinct sessions called and held. We received notes and/or white board shots for 77 of these sessions. Thanks to those of you who submitted notes and information!

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

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



## Demo Hour



### IIW XX #21 Community Sharing / DEMO LIST Wednesday October 28, 2015 brought to you by



1. **Identity Changes in Windows 10 Desktop and Mobile:** Vicky Milton  
URL: <http://www.microsoft.com/en-us/windows>  
Personal and work identities co-exist in Windows 10, yet they don't co-mingle. Learn how these identities work together to drive new experiences.
2. **WelcomeAboard by Welcomer:** Kevin Cox  
URL: [www.welcomer.me](http://www.welcomer.me) & [www.welcomeaboard.me](http://www.welcomeaboard.me)  
WelcomeAboard gives individuals their own linked electronic copy of the data from any form they fill out for any organization whether employers, suppliers, cooperatives, conference organizers, governments, etc.
3. **Blockstore:** Muneeb Ali and Jude Nelson  
URL: <https://github.com/blockstack/blockstore>  
Blockstore enables human-readable name registrations on the Bitcoin blockchain, along with the ability to store associated data in external datastores. You can use it to register globally unique names, associate data with those names, and transfer them between Bitcoin addresses.
4. **Blockchain Auth:** Ryan Shea  
URL: <http://www.blockchainauth.org>  
Blockchain Auth is a blockchain ID authentication protocol that supports generating, decoding and verifying auth request and auth response tokens. The Blockchain Auth protocol can be used as a decentralized alternative to passwords and Single Sign On systems that rely on third party identity providers.
5. **Consent and Information Sharing Work Group of the Kantara Initiative:** John Wunderlich  
URL: <http://consentreceipt.org/> & <https://kantarainitiative.org/groups/ciswg/>  
This demo will present a high level review of the proposed standard for consent receipts to enable users and service providers to have a method to agree on and record consent & notice. The demo will include showing how the work group has provided a generator page and api to allow anyone to provide Kantara compliant consent receipts.

6. **Danube Tech - XDI, FreedomBox:** Markus Sabadello  
URL: <http://danubetech.com/>  
The OASIS XDI TC is finally releasing its first Committee Draft specification, and FreedomBox is now at version 0.6. Come see what this means! (Secret Tip: Maybe there's even some cool blockchain stuff hidden inside?)
7. **digi.me -current PC/Mac and iOS version application:** Jim Pasquale & Julian Ranger  
URL: <http://digi.me> for product and <http://digi.me/video> for vision  
The demonstration of [digi.me](http://digi.me) will show what users can do when they own and control their own data on their own devices(s), initially with their social data of up to twenty aggregated accounts that are fully curated - providing peace of mind, flashback perspectives on social interactions with likes and comments and photos, universal search, customizable widgets for building collections, creating journals, empowering individuals to make better decisions.
8. **Covisint IoT Platform for Managing Identity of Things:** John Gleeson  
URL: [www.covisint.com](http://www.covisint.com)  
Our demonstration will show how to unlock the value of the IoT by connecting people, processes, systems and things. We will show how enabling those interactions gives enterprises the power to connect more deeply with customers and drive greater collaboration within the value chain.
9. **ForgeRock OpenUMA open-source project for User-Managed Access (UMA):** Eve Maler  
URL: <https://forgerock.org/openuma/>  
In the Internet of Things, the number of data sources that reveal our doings, and the sheer volume of data generated, will overwhelm our ability to control and share it all – unless we have help. That's where UMA and OpenUMA come in.
10. **MetaMask, demoing the "Ethereum" blockchain:** Aaron Davis  
URL: <https://metamask.io/> & <https://ethereum.org/>  
Ethereum is a decentralized platform that runs applications exactly as programmed without any possibility of downtime, censorship, fraud or third party interference. With identity built in at the protocol layer, it is shifts of control back into the hands of the user.
11. **Faster Modular Exponentiation in JavaScript:** Karen Lewison, Francisco Corella /Pomcor  
URL: <http://pomcor.com/2015/10/25/faster-modular-exponentiation-in-javascript/>  
We will demonstrate a modular exponentiation algorithm implemented in JavaScript, which is many times faster than the one in the Stanford JavaScript Crypto Library (SJCL), and can greatly facilitate the use of cryptographic authentication in web applications.
12. **FIDO U2F for Mobile:** Stina Eherensvard, John Fontana, Jerrod Chong, Yubico  
URL: <https://www.yubico.com/applications/fido/>  
**FIDO U2F - open authentication standard** After support in Gmail, Dropbox and GitHub, a million USB devices deployed with users, NFC and Bluetooth in beta, U2F public key authentication is now expanding to also include a mobile password- and tokenless user experience.
13. **passQi 2 with Two Factor:** David Eyes  
URL: <https://www.passqi.com/>  
Demo of passQi 2 with both TOTP & passQi 2 Factor Authentication along with Apple Watch support Store credentials in your phone (not in cloud) and automate login.

**The IIWXXI Demo List can also be found here**

[http://iiw.idcommons.net/IIW\\_21\\_Demo%27s](http://iiw.idcommons.net/IIW_21_Demo%27s)

**More Photo's of the Demo Hour can be found here**

<https://www.flickr.com/photos/docsearls/albums/72157659234919203>



## IIWXX #21 Photos by Doc

Links to Doc's Fabulous Photos of IIWXXI

Doc Day 1: <https://www.flickr.com/photos/docsearls/albums/72157661374994272>

Doc Day 2: <https://www.flickr.com/photos/docsearls/albums/72157659234919203>

Doc Day 3: <https://www.flickr.com/photos/docsearls/albums/72157661562244366>

Book of Proceedings Photos taken and provided by:  
Doc Searls and Heidi Nobantu Saul



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

William Heath  
Chairman Mydex CI

## Thank You to digi.me

Thank you to Digi.me for co-sponsoring this compilation of notes from the workshop ~ <http://get.digi.me/video/>

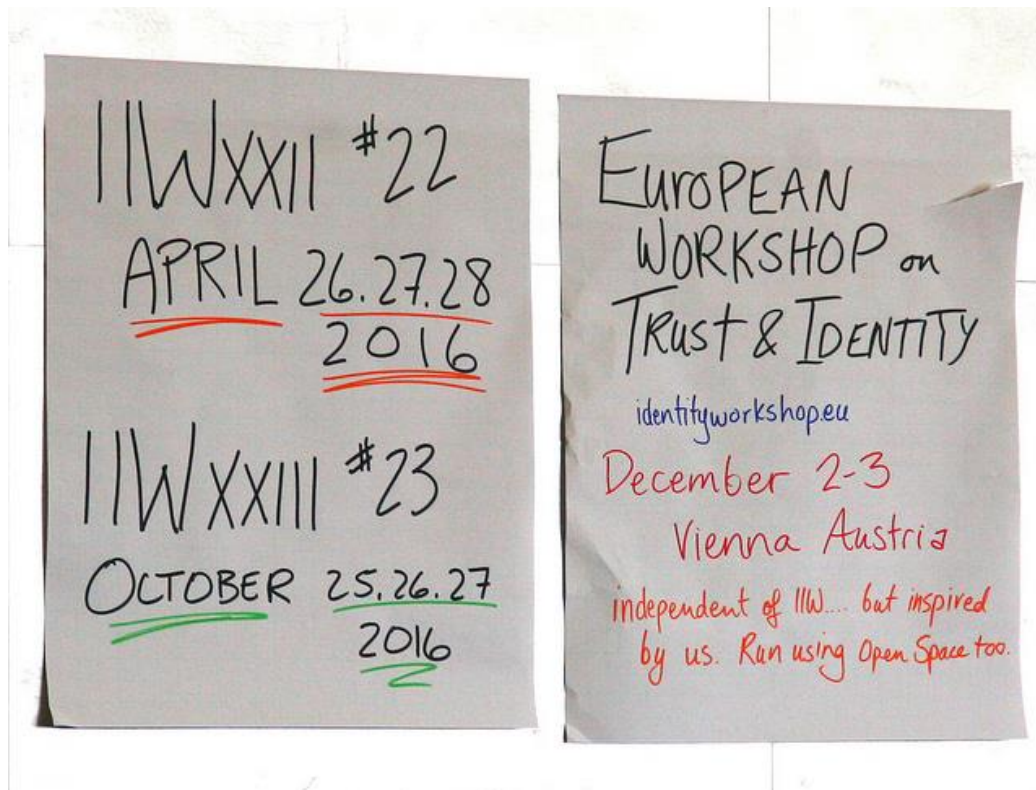


# See you April 26, 27, 28 2016 for IIWXXII

The 22<sup>nd</sup> Internet Identity Workshop

[www.InternetIdentityWorkshop.com](http://www.InternetIdentityWorkshop.com)

**Register Here!**



Thank you to our IIWXXI Sponsors

