IIWXXII INTERNET IDENTITY WORKSHOP 22

identitycommons working group

Book of Proceedings

www.internetidentityworkshop.com

April 26, 27 & 28 2016
Computer History Museum in Mountain View, CA

Thank you to our Notes ~ Book of Proceedings Sponsor
www.Cirrusidentity.com

Collected & Compiled by
MILLICENT BOGERT, HEIDI N SAUL AND BRADFORD WINDLEY

Notes in this book can also be found online at **http://iiw.idcommons.net/IIW_22_Notes**

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



Contents

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 12th year and is Co-produced by Kaliya Young, Phil Windley and Heidi Nobantu Saul. IIWXXIII (#23) will be October 25 – 27, 2016 in Mountain View, California at the Computer History Museum. Super Early Bird registration is open now at: https://iiw23.eventbrite.com

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

Microsoft	**Google**		**digi.me**	**Gigya**
Conference Dinner	Welcome Dinner		Tables & Power	Barista
VMWare	**Janrain**	Kantara	**AOL**	**Yubico**
BBQ Lunch	Welcome Drinks	Projectors	Afternoon Break	Afternoon Break
ForgeRock		**Cirrus Identity**	**WSO2**	**Identity.com**
Conference Reception Drinks		Book of Proceedings	Morning Break	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 for event and sponsorship information. Upcoming IIW Events in Mountain View California:

IIW XXIII #23 October 25, 26 and 27, 2016
IIW XXIX #24 May 2, 3 and 4, 2017

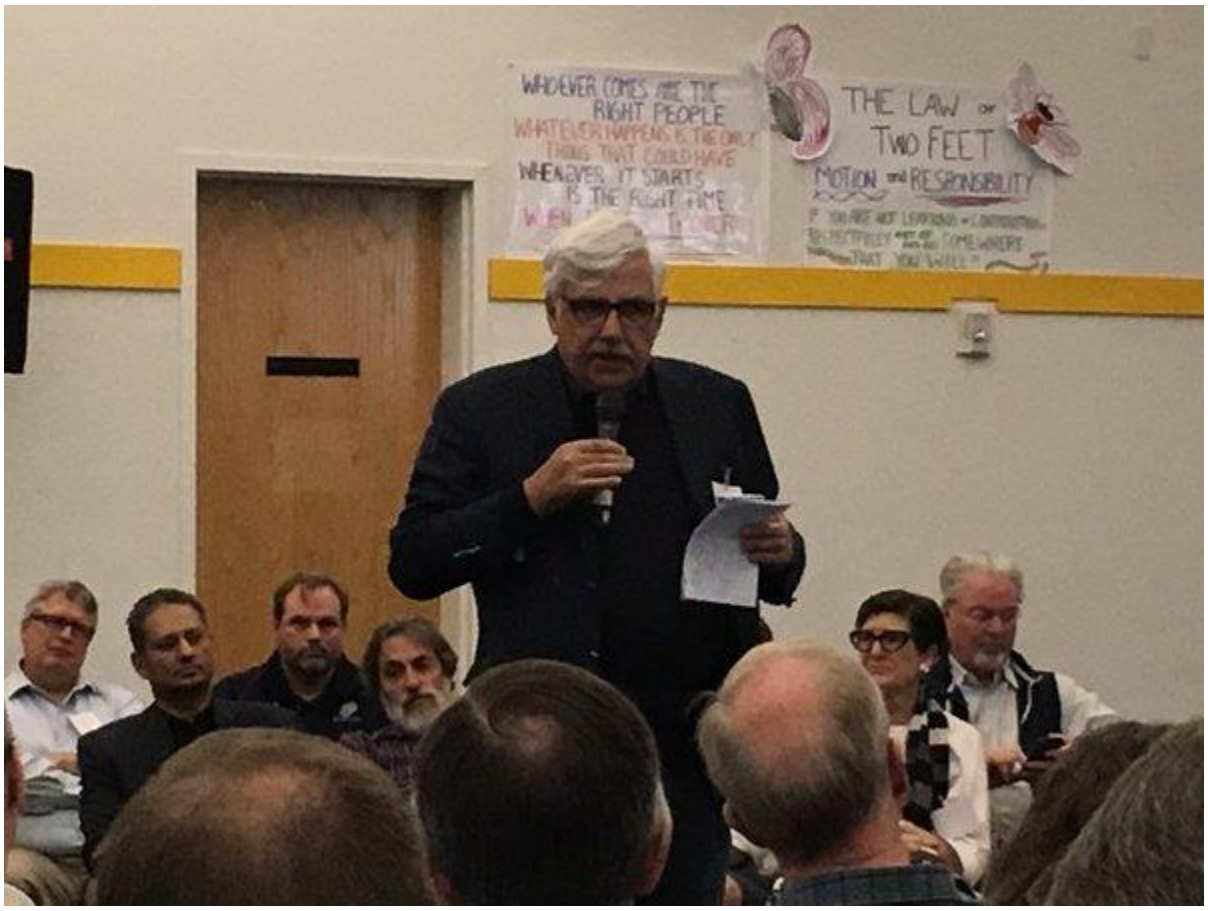
"IIW is the mecca for identity and privacy innovation. It's beneficial for newbies and it's an essential collaboration forum for the stalwart pundits who nurtured this emerging field."

Mike Schwartz
CEO Gluu

The Laws of Identity

IIW was formed around exploring what was then called "user-centric" identity. Kim Cameron's Laws of Identity were a big impetus for this focus in the early IIW meetings.

It was exciting to have Kim kick off IIW 22 with an opening keynote on Tuesday before opening circle. Kim revisited the Laws of Identity and their continued relevance over a decade after they were first coined.

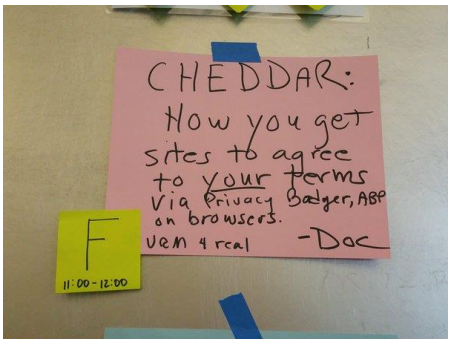


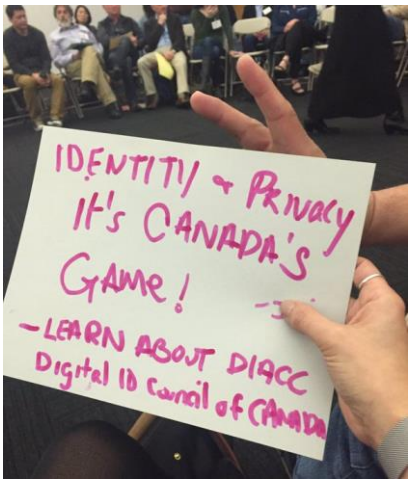
At IIW XXII we made several movies about Identity…

The Fabulous @heathervescent
and
Her Professional Film Crew
Lisa ~ Benoit ~ Lincoln ~ Terry

Organized, made-up and recorded 38 interviews with IIW folks, that will be used to create 7 individual films in addition to the primary IIW Identity Documentary. That's about 25 hours of footage

More still shots of the filming here:
https://www.dropbox.com/sh/8u9seyf04khoen5/AABaIKK2fBbZmrbzjYpQ9buRa?dl=0
pw: whoami





IIW 22 Session Topics

DAY 1 Tuesday April 26, 2016

Session 1
1A/Introduction to Blockchains
1D/IndieWeb Intro – Own Your Web Identity / Interoperate with other people + Silos
1F/CHEDDAR: How you get sites to agree to YOUR terms - VRM For Real
1G/Why do (people make) Sessions Expire? And what can we do about it?
1I/API Security Patterns BYOP
1J/Sovereign Technology

Session 2
2A/What is Sovereign Identity?
2B/Personal Data Ecosystem Consortium (trade ass) What can we do for you? What can you do for us?
2C/UMA = User Managed Access 101!
2F/Blockstack: The Global Identity Database
2G/C-DAD Cross-Domain Application Deployment "simple federation" (for enterprise apps)

Session 3
3A/Universal Compiler Demo
3B/Multi Party Delegation –It's not UMA ….Yet!
3C/Why Won't Blockechain save the world? Gaps? What's an alternative?/What Doesn't go on blockchain?
3D/Plugging Identiity Components into AAD B2C to get access to relying parties
3E/SCIM Interop Discussion
3F/My Device My Data ~ My Data My Device

Session 4
4A/JLINC Protocol for Data Sharing Chain of Custody
4B/The Hard Problems of Storing Identity Information
4C/My Things Are Me! Who backs claims for my things?

4D/Modern Identity Initiative [Working Title] A thought on using the ICANN/IANA model for hosting personal identity
4F/OpenID Connect WS / Mix-up & Cut-n-Paste Mitigation Discussion
4G/Towards a Common Ontology for Personal Data Interoperability ~ Or just a Pipe Dream?
4I/Scalable Consent – Effective, informed, revocable, *.* multiprotocol consent + attribute release, UI, infrastructure, informed content
4J/Constructive Notice – What Must We Do?

Session 5
5A/Consent Receipts – 101 & Update – Closing the loop with users
5B/R & D Funding for your Project! (Identity and Privacy) Come hear how you can get it.
5C/Identity and Payments – ACH, Blockchain, Credit, Debit, P2P
5D/Blockchain Consensus Protocols
5F/UX Design of Identity Systems
5G/Open ID Connect hint on the URL – fight IP "authentication' change EZproxy!
5I/SCIM & OpenID Connect: From Co-existence to Harmony
5J/Anonymous Credentials – Will they ever be practical?

DAY 2 Wednesday April 27, 2016

Session 1
1A/Bridge to #Meatspace – Use cases, Tech for Transfer, and verifying Idenitity at Point of Service
1D/What if…. UMA RPT was an OpenID Connect Access Token?
1G/PDEC How can we help you? (Personal Data Ecosystem)
1I/Black Box Algorithms & "Personalized" Services
1J/Body of Knowledge for 'Idenity Professionals – What Domains do we need?

Session 2
2A/Signed Consent (on a chain)
2C/Monolith to Microservices – Securing w/OAuth, OpenID Connect, JWT
2G/E.R.A.S.M.U.S. – proposal for Emergency.Responder.Authentication.System for.Mobile Users
2I/Sovereign Identity AND Lending
2J/Practical UMA – curl commands etc…
Session 3
3A/Sovereign Identity – (Part Two) How is it enabled by the blockchain.
3C/$1M Does Your Project Stack Up? Come find out ☺
3D/Identity & Privacy: It's Canada's Game!
3G/I Just Bought Your Smart House, Now What?
3I/OpenID Connect RP Testing
3J/So you are the professor…what is the curriculum for Introduction to Identity Management

Session 4
4A/Identity Events = RISC, LogOut, Revocations
4C/Demo Hour Redux
4D/OIDF – EAP Use Cases

4E/People's Digital Identity Life Cycle
4F/CHEDDAR Implementation 'on server" + "on client"
4G/Trust Frameworks Explained – in 20 min.
4I/Privacy: Confusion of Identities in our Daily Life
4J/UMA + JLINC – Signed contracts on a Blockchain?

Session 5
5A/Bridge to #Meatspace #2
5C/Personal API's @ BYU
5D/Password Manager API's
5F/OIDC Identity Federation
5G/Common Ontology for Personal Data Interoperability – (Part 2) The What and How
5I/Identity for the next 1.5 Billion!!
5K/UMA Legal

DAY 3 Thursday April 28, 2016

Session 1
1A/Continuous Client "Authentication" for API's
1F/Sovereign Identity Part 3: What are the Challenges?
1I/ Consent & User Rights – GDPR 101
1H/SimpleSAMLphp - Project Overview & Roadmap

Session 2
2C/Identity in Ten Hundred Words
2D/Ecosystem Maps: - Org History, Protocol Family Tree, The Neighbors & Other Maps
2F/Sovereign Identity on Your CellPhone with YOTI
2G/S.A.L.S. – Launching Soon = IDESG/ID Ecosystem Steering Group
2H/SimpleSAMLphp Use Cases. How are orgs using SSP?

Session 3
3A/Fixing Marketing + Service with VRM – intent casting & personal API's
3C/Protocols for Sovereign Technology
3F/Weaponized Biometrics? Revocable Biometrics –
3H/SimpleSAMLphp –Code dive + How can you contribute?
Session 4 / Working Lunch
4F/OTTO – Open.Trust.Taxonomy.Operators – For Federation
4G/ID2020 Design Shop Planning / for May 21-22
4H/SimpleSAML php Nearterm Roadmap – feature requests,who wants to build what?

Session 5
5A/So You Want To Run A Standards Group
5C/Service Chaining with ZBAC / JWT Assertion Prodile vs STS for the Rest of Us
5F/Home Environmental Data, SPIMES & Engineered Privacy
5G/Token Based Federations
5H/Simple SAML php More Building!

Tuesday April 26

Introduction to Blockchains

Tuesday 1A
Convener: Muneeb Ali
Notes-taker(s): Muneeb Ali

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:

Blockchain primer

From Blockstack – Identity on blockchain
Define the problem –
Decentralized consensus
Consensus is hard in computer science – 1000 computers trying to agree on something – e.g., 2 operations over 1000 computers without central controller

Trying to solve simple problem on agreeing on the state of the system

There are different ways to do it.
Have nodes – have protocol to establish the leader election – decides what is next action.
Protocols can only tolerate certain number of malicious nodes.

Blockchains are another way to do consensus – hard to tamper

Blockchain is a file – can download it – it was 15 gigs, now 45 gigs
Presents the genesis block – start of time Time=0
Physical structure of file – time is divided into blocks – genesis block launched in 2008.

Bitcoin blockchain s largest blockchain 0 references here are to bitcoin.

Blocks are written on the blockchain as time passes. Same production network working to produce additional blocks. All data preserved in the blockchain itself.
Within each block – have transactions represented.

Now talk about the network
If you are a node and want to connect to Blockchain
There are two types of nodes – simple node that not want to be a leader (called a miner)
Miner is a leader that gets to form the next block.

If not want to participate – just a simple node.

Every node connects on average to 8 other nodes – full broadcast to all other nodes. Full expression of all transactions you hear about to your network.

When new blocks are announced – hear about the new blocks

Nodes that decide to be miners (leader election participants) are trying to solve the hard computer puzzle
The puzzle is

1. take hash of last block plus some other information and rapidly calculating new hashes
2. If the result has a certain number of 00000s in the beginning, Hash is deterministic but completely random.
3. After certain amount of tries will get solution with number of zeros.

Miners are in a race to hit the hash that is the solution to the prior block – everyone on the network can verify the success.

The number of 0000 solve for is variable by how much computing power is on the system. If there are more miners, increase the difficulty level.

0000 are just a way to define space.

2 incentives – Miners get the fee that is imposed on the transactions in the block they worked on. 2 – Protocol is used to introduce new currency into the system.

Currency gives the incentives for people to be part of the network.
Every new block releases new currency into the system.

New currency is incentive in the front end. Total is 21million bitcoins, so may be self sustaining at that time.

Most important thing to remember – process of doing hard computations – things that were written to the blockchain earlier become more and more security. So attacker seeking to alter transaction written in block 5 blocks old, would need to rewrite the hashes of the past. Problem is that it is computationally intensive.

Once you get 6 levels – probability of rewriting is close to 0. Average is one block every 10-40 minutes. If wait a couple of hours, no one can change the chain.

If changed it – every person would realize it – because would change all history and would see it. [Equivalent of neighborhood watch].

Fork in the network happen, but they are not that deep. If have a deep fork, everyone can want to put a hard stop in the system. Even if attacker is successful, they would have to bring in computational power every time to keep up.

51% issue – Blockchain works as long as no one party has 51 % of the hashing power. Some fraud enabled with 51%. Have 100% transparency on the system also so that helps with neighborhood watch. Forks are indecisions, but they are seen.

What is being done to prevent mining pools getting together and colluding to more than 51%. Theoretically possible, but history suggests that they don't have the incentive to collude, since it would put their interests at risk [Like Moral hazard – Alan Greenspan expressed surprise that leaders of financial organizations would drive companies into the ground.].

Older thinking was to fork the bitcoin blockchain for other purposes, but now have separate blockchain.

Security is about hashing power and the reliability of the network.

It is all about incentives.

What are consequences of the forks? Usually ignore it, because usually resolved by the 6th block down.

Main blockchain – bitcoin blockchain – can peg other systems on top of it (not forks, but cross reference to other. Bitcoin is solving a very hard problem – once do that, can build on top of that. System that is using a system of functionality can use blockchain.

Longest chain rule – if there is a conflict with blocks mined – the longest chain always wins – since it represents most computational power. Computational sovereignty

In blockstack – information only shows encryption for identity system.

Side chains are different than separate normative cross referenced chains.
Are side chains different than forking?

Censorship resistance – principle that everyone is equal – no one can stop it.

No one can stop you from being a node or a miner.

Powerful property – but has complications – people who want to censor.

Also, to have Censorship resistance – also have **fungibility** – one dime is like any other. Same as bitcoin – how have fungibility.

Censorship resistance is problem when have a concentration of miners – might have 51% group.

What are worse case scenarios that can happen.

If have collusion or state actor interrupting – would hit pause on system. Could go back to see "what block can you trust" and then start a new blockchain from there. Can "re-route" – announce that migrate to other blockchain and migrate other information to a new blockchain. How migrate – Own something with a private key – can migrate it then.

There are different kinds of chains
They like idea of single global blockchain.

But there are other models –

e.g., Federated system - can start blockchain with identified parties – 4 parties can decide to have round robin leader election. Still get history, auditability, but don't get decentralization.

Can have own private space, but not have all the benefits.

Virtual chain – sits on top of other larger chain – normatively cross references it. Certain operations not listed in the main blockchain – introduce new functionality in chain – transactions announced in bitcoin – for servers can construct a

Registration fees for names can be given to miners.

Proof of publication and proof of existence are simplest things to put in first.

Very firm time of when the event happened – can prove it.

Get real history from the proof of existence and proof of publication.

Differences of virtual chains

Blockchain is a state machine – changes state from block to block – put difficult to introduce new functionality. Virtual chain introduces new functionality.

Side chain is just another blockchain. Not branched from the same root, but pegged in some way to the main side chain.

Side chain is one way (or 2 way) pegged. Like currency relationship where currency is convertible to another.

Turning to practice and uses
Don't' have to trust other parties, can use blockchain and not dependent on another company.

Moves trust out of the network, into the process.

Blockchain allows self sovereign identity.

Intro to Indieweb

Tuesday 1D
Convener: Kevin Marks
Notes-taker(s): Tom Brown

Tags for the session - technology discussed/ideas considered:

#indieweb

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

where I go everyday has been subsumed by apps and silos

(your page on someone else's domain is sometimes still a reasonable option)

want to connect to identities in other places (this is my twitter, facebook, etc) - indieauth

trick - link to one of these silos that already has an auth server. rel-me link to your own site.

(twitter puts in the rel-me tag)
→ www.indieauth.com

indieweb reader: www.https://woodwind.xyz/

brid.gy finds responses in silos and sends them to your website

<link rel="webmention" href="webmention.herokuapp.com" />

w3c working draft: http://webmention.net/draft/

https://silo.pub - allows you to use one of the silos as your micropub endpoint

user friendly indieweb: https://withknown.com

https://quill.p3k.io/

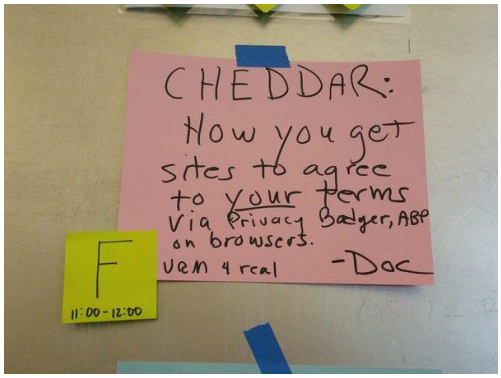
C.H.E.D.D.A.R. VRM 4 Real

Tuesday 1F
Convener: Doc Searls
Notes-taker(s): tweet compilation

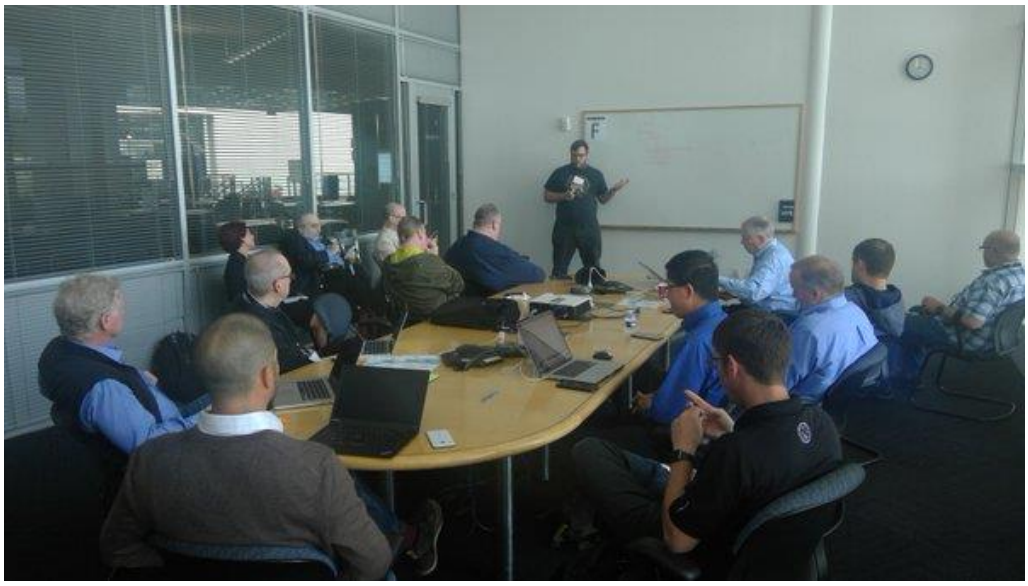
Tags for the session - technology discussed/ideas considered:

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

#iiw CHEDDAR session on a proposal for reducing ad tracking and ad fraud
http://blog.aloodo.org/posts/new-acronym/



@dmarti is the source of CHEDDAR proposal - see http://blog.aloodo.org/posts/new-acronym/ … #VRM #**IIW** Group discussion starts at IIW



Why Do (People Make) Sessions Expire?

Tuesday 1G
Convener: William Denniss, Guidin Kong
Notes-taker(s): Jim Fenton

Tags for the session - technology discussed/ideas considered:
Reauthentication ~ Session management ~ Cookies

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

Lively discussion of the reasons that sites/applications expire sessions. About 40 people present.

- Garbage collection
- Remind users of their passwords
- Lack of session revocation
- Compliance, e.g., PCI
- Customer recommendations
- OWASP recommendation
- Habit
- Lack of continuous authentication
- User walk-away (and walk-up by someone unauthorized)
- Undetected changes in user authorization (user fired from job, etc.)

Some issues:

- Lack of trust in user agent
- Lack of reliable identification of user agent (currently self-asserted)
- Caching of credentials by user agent unbeknownst to relying parties
- Lack of single logout
- Fixed vs. mobile uses (no session expiration for mobile)
- Can't detect user activity

Interesting factoid: Apple reports that typical users unlock their phones 80 times a day.

Sovereign Technology

Tuesday 1J
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:

Sovereign Technology (e.g.: has no privacy policy)
Components

1. Policy Assertions (e.g.: DNT)
2. Authentication (e.g.: FIDO)

3. Longitudinal Notification Endpoint (e.g.: email address)
4. Non-repudiable Link (e.g.: biometric)
5. White-List of IDPs (for Requesting Party claims)
6. Backup and Recovery (e.g.: m of n)
7. Delegation (e.g. parent of a minor)

8. Competence tests (e.g.: partial delegation to a minor)

Next step: Associate protocols with each of the 8 components.

What is Sovereign Identity?

Tuesday 2A
Convener: Drummond Reed, Christopher Allen, Phil Windley
Notes-taker(s): Drummond Reed & Scott David

Tags for the session - technology discussed/ideas considered:

sovereign identity, digital identity, blockchain, policy

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

its not about Facebook or other social logins
its not about asymmetric power
its not just about legal identity or citizenship / but that could be one use
its not perfect
it can address the refugee use case
it is not a single identity
it can be contextual
it doesn't have a administrative authority
it can run in parallel with other authority systems
it gives the individual control
it cannot be taken away
UN is thinking of tracking everyone to explain self-sovereign identity -
Why , why now?
Christopher Allen blog: http://lifewithalacrity.com
Phil Windley blog: http://wiindley.com
ID2020 - http://id2020summit.org
Web of Trust http://weboftrust.info — https://github.com/weboftrustinfo
IRespond - http://irespond.org
Suggestions
practical exercise of foundation - fairly straight forward summary of the current world issues.
how do you make it compelling
other terms
identifier
own agency and self determination
rebooting web of trust - experts on blockchain CTO of a major CA talked about a summary

could be called self sovereign identifier? to deal with the multiple entities?
anil john
Do we have to solve the refugee problem with sovereign identity? Can we just solve for the US for now?
what does it mean to be a person? what are the human rights of a person in the 21st century
censorship - resistant / power-resistant
1 billion undocumented identities

Notes from Scott David:

What is self-sovereign identity? And why?

Is it something new – different than user-centric identity? What is the difference?

What difference might it make?

Why should we care: Concern with co-option and market hegemony.

How begin to talk about something that allows a difference and prevent a power attacks.

Power imbalances in the system to be addressed.

Different language of needs now.

Merge the institutional and the individual needs and views on the issue.

10 principles of Christopher Allen – in Github – meant for comment and for further work. Leading to white paper from community of blockchain and identity people –

vision. https://www.lifewithalacrity.com

Phil Windley wrote a response http://windley.com Phil thinking about ID2020 summit – provide legal identity to 1.8 billion people who don't have identity currently.

Most people don't think about what life would be like without a legal identity for things like passports, getting kids into school.

Civil registration started in 1700s in France. Civil registration is basis for much other identity and social benefits. Control of identity is based on fact that can produce a piece of paper that others cannot produce.

Phil thought about Christopher's blog post – Civil registration conflates two concepts: identify individual for lots of things that happen legally, and going to say that person is a citizen (part of nation state). Most legal identity systems don't separate out citizenship and legal identity, and that can be a challenges as long as those are conflated. Self-sovereign identity may permit separation of identity from citizenship.

Possible that governments could accept a self sovereign identity system as basis for identity, and then write claims against identity that could be part of system.

Identity is nothing by self – it is the claims that mean everything.

Critical not to let the perfect get in the way of the good.

Systems that we are trying to fix/replace is not perfect either, so the solutions can be better without being perfect.

Need to articulate and use cases to help tease this out.

Loss of rights if not have identity.

Commonwealth nations as use case – have trust issues, but have much in common.

Q: Why is it singular? Why not self-sovereign identities (plural)?

It was clarified that it is not intended to suggest single identity.

Advocacy for switching to "identifier," rather than identity.

Independence from other entities or context is a good reason to use identifier as a term.

Concern with "sovereignty" may be issue for existing sovereigns.

Note history:

Federated

User centric

Self sovereign

What is the difference of identity and identifiers.

Identity is about correlation

Identifiers is different.

People can correlate you any way they want.

Back to self sovereign identity

Desire to blend policy, technical, etc. all into one issue.

Question is whether you mean – adoption rates will depend on people believing the assertion. How make it compelling for service provider or relying party to be certain of the usefulness of the identity.

Lots of technology allows for avoidance of correlation – cryptography and blockchain, e.g.,

Consider who is going to trust this – want to relate to the policy makers that in absence of an identity issuer, can people be empowered to represent a persistent entity that someone can interact with.

Practical issues – ID2020 is aimed at unidentified people – solving that is important.

But there are other identity problems that are not solved by current systems. What will change so that not have to mail a birth certificate to get a passport. Question of what will replace it. It is a broader problem than just undocumented folks.

Also, self-sovereign identity system could run in parallel with existing systems and could run together for a while.

ID2020 concerns with taking the most exposed people earth, and introducing further challenges. Can result in additional exposures to people who are already at risk. In other cases can get by without being perfect, but here if mess up, can destroy people's lives.

Return to Chris' principles: Need data minimization and other control so that can reduce bad nation state actor harm.

Can mitigate the challenge –

Notion of execution – for ID2020 – want to connect up resources of tech folks with

UN community. UN community is inexperienced in identity issues. NGOs will b there and they are in need of solutions.

OIX will create white paper after ID2020.

Day after ID2020 event, there will be a facilitated workshop: information is at web of trust. http://weboftrust.info

Suggestion that best handles are in refugees and healthcare. That is a discreet use case.

User centric – term is less useful than self-sovereign identity.

What does declaration of human rights look like in the 21 st century.

Need for guidance on the issue. What mean to be a person, what it have.

Sovereigns don't ask for permission. Develop it and be confident that don't need to ask for permission for the "sovereignty"

It is a 15 year effort. Raise awareness and consciousness for support for it. www.evernym.com - sovereign identity on a permissioned blockchain. Stumbled into the issue while solving way to send message without knowing contact information. Novel solution to that issue that realized had broader application. When realized that blockchain was there, made the connection.

Sovereign identity – ultimate authority in a particular sphere. Autonomous is similar. Identity not given by government or company, or be taken away.

To close:

Following is Material on the board during the session:

Resources – see above for other links:

https://www.lifewithalacrity.com

https://windley.com

https://weboftrust.info and github.com/weboftrustinfoevernym.com

Suggestions

1 Do a summary of current work and why sovereign ID

2. How do you make it compelling?

3. How does it relate to fundamental human rights

Its not Facebook or other social logins

Its not asymmetric power

Its not just legal identity or citizenship (but could be one use)

Its not perfect

It can address the refugee use case

Its is not a single identity

It can be contextual

It does not have an administrative authority

It can run in parallel with existing systems

It gives the individual control

It does not need to ask for permission.

UMA 101 (User Managed Access)

Tuesday 2C
Convener: Eve Maler
Notes-taker(s): Eve Maler

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

We reviewed the individual and enterprise motivations for User-Managed Access, use cases coming from health, Internet of Things, and additional corners, and discussed the UMA architecture, as expressed in the attached diagram. For more information, interested parties are invited to visit the Kantara UMA Work Group wiki home page at http://tinyurl.com/umawg, where they can find information on joining the group, implementations, case studies, and more.

Blockstack: The Global Identity Database

Tuesday 2F
Convener: Ryan Shea & Jude Nelson
Notes-taker(s): Guy Lepage / Ryan Shea

Tags for the session - technology discussed/ideas considered:

#blockstack, #blockchain, #database, #pki, #dns,

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

(The room was filled)

Who here knows what Blockstack is? No one
Why are you here? Seems most interesting

What type of blockchain are you using?

Ryan gave a quick overview of what blockchains are and what core services they provide.

Then, Ryan got into how Blockstack can operate on any blockchain but how and why the current Blockstack network operates on the Bitcoin blockchain.
- It's the most secure
- There's only really one strong, secure blockchain at the moment

Jude gave an overview of the Blocsktack architecture.

Note: Even more people coming in.
Note: People seemed to really like that they can run their own server locally.

Explanation of who the Blockstack community is:

- Companies like Blockstack Labs, Openbazaar, Mine, etc.
- Explained that you can think of blockstack as a new ecosystem

Question: "So everything is being stored onto the blockchain?"

What is the fundamental value prop?
- Ownership
- Federation
- This put self-sovereign identity within reach
- Global
- Trusted
- Verified
- Difficult to be taken down
- Secure

"It's the sovereign identity we've been talking about for the past 10 years"
- Unknown IIW veteran

Why would someone want a permanent id?
- Root long
- Persona

Each namespace has it's own name pricing rules and name expiration rules.

Can you talk about some use cases?
- Onename.com for identity management and single sign-on
- Openbazaar is using naming of the stores and id
- Developer Operations
- We are now working with Microsoft
- Question: is this going to be passport v2?

William King
- Is there going to be a Blocsktack Server that we can use?

C-DAD: Cross Domain Application Deployment

Tuesday 2G
Convener: Dick Hardt
Notes-taker(s): Ritwick Dhar

Tags for the session - technology discussed/ideas considered:

How to simplify/automate SaaS app registration and setup with IdPs

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

Sample problem statement: How do app developers using Google as IdP set up AWS (as a SaaS app)

without creating brand new identities in AWS, without cutting and pasting data. Define pattern for optimizing setup.
Proposed pattern:
Step 0: App registered at the IdP (bootstrap flow) - one time - (using metadata containing endpoint for discovery….)
Step 1: Admin authenticates at IdP (Google)
Step 2: Select app (AWS)
Step 3: Answer questions - what questions? - Optional
Step 4: Get redirected to magic entry point for app
Step 5: Authn @ app [OR create account] - should be OOB.
Step 6: Answer Qs
Step 7: redirect to IdP
Step 8: Tests and checks
Discussion:
Step 0: Can app ask IdP for attributes that the Idp does not want to give (phone numbers, etc)
Paul Madsen: The smarter Step 0 is, easier the other steps are? 0 informs 3 and 6… driving the UI
Shashank: Make the process smart …. collapse rest of the steps? We are not there yet - Salesforce has a good example of this.
Rachit: Can #2 be 'paste a URL, and discover App': App publishes URL? Dick: where did the URL come from?
Prateek: Step 0: describes identity requirements that surrounds the app, there's no such manifest today. That's foundational.
John Bradley: Q. on scope: Is provisioning included? Are there 3 parties here instead of 3?
Enterprise dir. may not be run by the same identity as the IdP?
The vision is:
SAML/OIDC for authentication
SCIM for provisioning
Auth for SCIM is one the things we need to set up in the steps
Paul: #5 implies admin already has an account at SaaS. We shouldn't mandate an existing pwd for the SaaS. [Q]
Where does user choose app name?
Does the service push the data, or does the admin?
#0: Admin can be aware of the URL….
In many cases, users can become aware of the app as they are using it.
Shadow IT: user sets up their own identifier into the SaaS app.
We need to figure out Step 0, 3, 6
What going on with the redirects: #4 and #7 (oauth-type flow)
The account that manages federation, should that be out of band authentication?
- break glass. No one can authenticate any more…. how do you fix it?
- say you want to change who your IdP is.
- Logging in locally at the SaaS app.
Best practices for this?
#1 #5: Should use MFA.
#5 - federating into an app doesn't preclude app again MFA. Most industry best practices usually avoid managing federation with federated identities. This is an OR operation: either use existing OR create an account. If they're not authenticating with the same IdP, doesn't the shadow IT still exist?
No, because shadow IT is completely independent. Assumption is that SCIM will deprovision admin… maybe we need a 'super-admin' role.
Above has to do with 'how do we deal with privileged accounts' - out of scope for this discussion.
SCIM could become pervasive. As we are branching out to SaaS, central directories are not possible any more. Back channel push @ change.

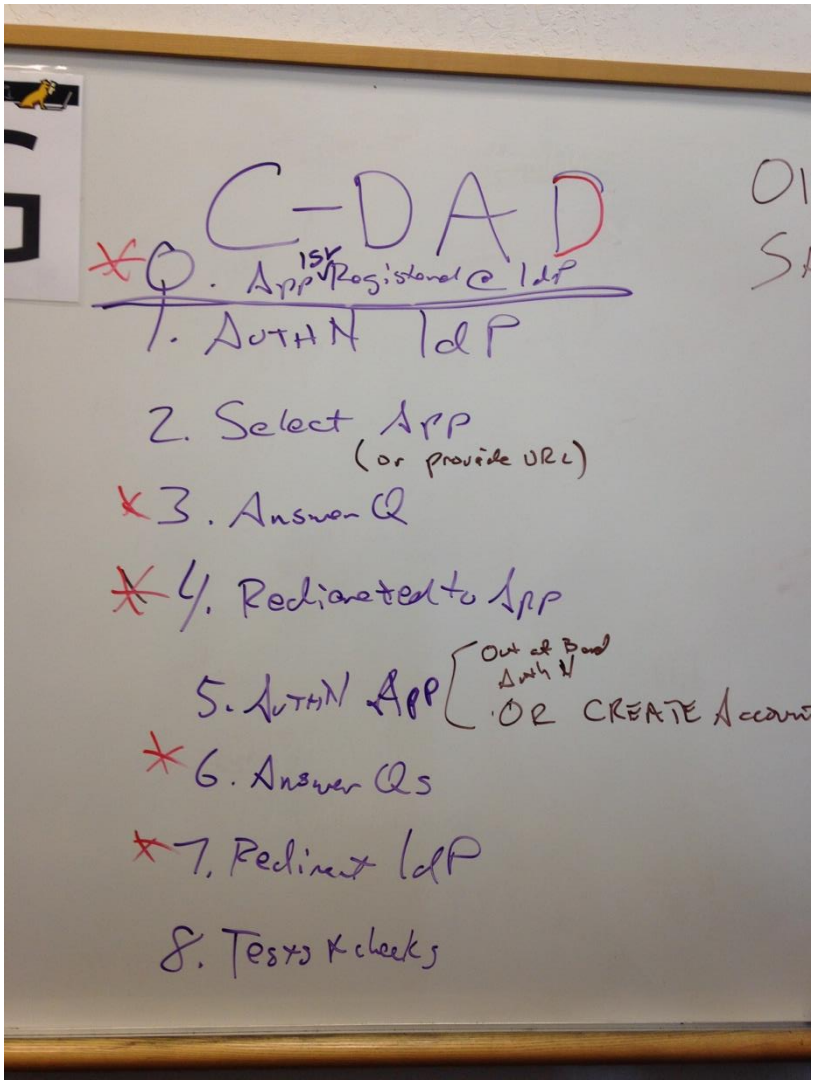
Discussion about where this belongs? OAuth? IETF?
Spin up an email list? That's the quickest. Let the ADs worry about where it goes.
Concern: OAUTH working group is going through a consolidation phase. Rechartering. May be out of scope.
Should it be OIDF? Probably is the best place? OIDF could possibly agree
Other option: Like SCIM, do it completely offsite.

Outstanding questions & observations:

Need to define Steps 0, 3 and 6 better. Step 0 is critical. Can collapse a large part of the flow.
Step 8: Each SaaS app could have a test account that the IdP can to check continuously (first as part of #8 and then over time).

Action Items:

John Bradley - will talk to Steven (Area director) about creating an email list



Universal Compiler Demo

Tuesday 3A
Convener: Scott Shelton
Notes-taker(s): Scott Shelton

Tags for the session - technology discussed/ideas considered:

#VRM, #IntentionEconomy, Internet of Things #IoT

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

Demonstrated a crowdsourced intention engine designed whose goal is to make it as easy as possible for supply and demand to communicate and interact with each other using natural language. Also demonstrated how it's possible to use that same intention technology combined with crowdsourcing to empower people to do more with their computers using natural language. It was suggested to look into Amazon's Alexa API as well.

Multi Party Delegation

Tuesday 3B
Convener: Justin Richer
Notes-taker(s): William Kim

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

MPD Not UMA

Justin Richer and team working on UMA implementation on top of MITREid-Connect project, found a lot of architectural decisions in the UMA protocol that made implementation difficult. Collected issues over 9 months of UMA implementation.

Earlier this year, took lessons learned and implemented into system--called it Multiparty Delegation (NOT compatible with UMA protocol!)

Justin: "Simplified the system, and made it more flexible at the same time".

Eve: UMA recent history. UMA 1.0 achieved acceptance March 2015. Then did 1.0.1 in December and addressed bunch of bugs. Collected non-backwards-compatible issues and 2016 roadmap for changes. Number of buckets: security, IoT, simplification, i.e. how it can be better aligned with OIDC/OAuth e.g. Can it be a true profile of OAuth 2.0?

MPD was developed with requirement that two users do not have to have accounts on the same server. Lead to "wide ecosystem" UMA use case.

Desirable to be able to cleanly place UMA on top of existing OIDC/OAuth setups, but wasn't possible with UMA 1.0.

Description of MPD flow (Notetaker's Disclaimer: may be missing parts):
Resource Owner flow.
Start by starting authentication session with Relying Party using local OIDC server. Unchecked UMA managed resources scope.
Now share resource to MPD server. First, declare the MPD server URL, which kicks off discovery and registration
Get presented with scope authorization screen with the UMA managed resource scope checked (UMA protection). Protection Access Token still there and works in the same way
Specific mechanisms of how this happens differs from UMA protocol (e.g. data structures, syntactic differences in resource set registration)
At this stage, pretty much still UMA with some syntactic changes.

UMA Discovery, OIDC Discovery, and OAuth Discovery were all different before.
Made alignments on UMA to OIDC Discovery.

Now Requesting Party shows up, and now its very different from UMA.
No AAT
If Bob already had account on the AS, then it would work, but this is the narrow ecosystem use case.
Pointer to AS and permission ticket MUST comes back in the header in MPD version to the Client.

UMA requesting resource one scope at a time, but developers would implement it just get all the scopes at once. It was entirely on the RS to make the call for what permissions it needs to ask for
George: Analogy for phone app asking for all the permissions up front vs. at run time.

Eve: 1. Multiple resource sets, each with it's own scopes -- complicates potentially what the client actually wants. 2. It's up to Alice (resource owner) to decide what get shares.

Justin: No, the AS ultimately decides which scope gets shared
Disagreement

Client requested resource.
Now AS has to do some set math, scopes that the Client has requested, and scopes that Client is authorized
Also, set of policies that apply to this authorization, each of those may have scopes.
One way to handle this is to interactively involve the requesting party,
"Claims gathering endpoint", aka interactive claims gathering endpoint. In MPD, it uses OpenID Connect and it's an RP, but doesn't necessarily need to be--just needs some some way to prove the Requesting Party. "Just go get something from the RqP".

Two ways to attach claims to a permission ticket, claims gathering endpoint or claims pushing to the endpoint.

UMA Token Profiles? Introspection vs Structured tokens

Adrian: Doesn't work with HIPAA unless the RS gives Resource Owner gets warning that Client is trying to get access.

Why Won't Blockchain Save the World?

Tuesday 3C
Convener: Maria Vachino, Christopher Allen
Notes-taker(s): Kevin Marks

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

Christopher Allen: I am deeply involved with blockchain but it is definitely overhyped. We really don't want to put identity on the blockchain - bitcoin is a permissionless system - no-one can stop you mining or transacting - on the permissioned side there are different groups that need permission for certain roles

Maria Vachino: the different consensus protocols are about who gets to be the leader: PAXOS, POET etc - blockchain it's mining

Christopher Allen: what I need to know to suggest a consensus algorithm depends on the roles and number of players

Maria Vachino: if scale is locked in at the beginning, what happens when you mis-estimate it?

Christopher Allen: if just you and I have a transaction, there's no reason to use a blockchain

Joaquin: Under your research, what did you find that blockchain wasn't suitable for?

John W: There are use cases for things that need to expire - must go away after 7 years - blockchain is too persistent

Maria Vachna: our identities do change, and we don't always want them to persist -think of refugees fleeing persecution

Christopher Allen: there may be existing signing agencies, trust agencies that you would prefer to the blockchain

John W: if one of the requirements is compliance with the right to be forgotten or deleted, a persistent history is bad - if information has to be revocable, that doesn't imply that it will delete all copies

Shen: You could use blockchain for key distribution and unique identifiers, not for storing volatile information

Maria Vachino: if a database solves it, we don't need to be told about this - what new ideas are there? - a blockchain identity is first come, first based - bankers say you can't fix a mistake or reverse a transaction - a secure blockchain needs a very high amount of traffic - it may go away if there is too much bickering

Dale: Bitcoin is based on a proof of work that is hard to game, but the work provides no value in the world. Is there one that does?

Shen: Blockstack's system is blockchain agnostic - it can work on bitcoin or other chains - you don't necessarily want work that is useful, as that makes it more gameable

Christopher Allen: blockchain can't do small trust - other things are a lot easier. zero-knowledge proofs can do a lot that don't require blockchain

John W: you can't use blockchain for ephemeral trust the same way that you can with OTR

Jack: where rely on an oracle you can't use blockchain as it adds an external dependency - say I have a website and I want future blocks to depend on that site - if that is removed blocks can't be validated

Christopher Allen: we understand problems with very large like bitcoin and things under 50 where paxos works but there are edges - anything with latency requirements doesn't work on blockchain

Jason: do you rely on immutable ledger or consensus protocol? You could have a triple-signed receipt to reveal proof

Christopher Allen: if you need to revert a transaction a year ago, you can't

Kevin Marks: you can revert by creating a mirror transaction but it leaves a record.

Christopher Allen: if you are logging a history, you can do things like certificate transparency rather than a blockchain.

Jack: turing complete computation is not necessary for the blockchain, but you can just log the verification

Jim Fenton: reading the board I see that blockchain is not good for small, trust, medium trust or large trust

John Best: I work with ledgers all the time, and a big issue is converting from one to another if you take it from a go forward basis, migrating onto a blockchain means you don't have a creation history

John W: I have seen the size of storage be an issue so I am worried about the ever-growing size of the chain

Christopher Allen: with Segregated Witness we are moving the signatures away from the transactions to use less data - there are models where you mark a point in time and forget everything before that and move on - the root of this capability is to have a ledger; if you have something done with a ledger it might be a candidate

Jason: if you have a distributed consensus you could just store hashes

Christopher Allen: there are a lot of things implied by identity that don't belong on the blockchain - we're working to making sure that you can't put anything human readable in the blockchain itself

Drummond Reed: there are different kinds of blockchains that have different properties

Ryan Shea: you could replicate ICANN in blockchain by having a federated namespace that you delegate through for domains

Jack: what we are getting at here is the blockchain microkernel - what is the minimal thing we need for the blockchain to exist - I care about how big blocks are and how fast they propagate, and the federation model; we can simulate anything else

Christopher Allen: other forms of leader election have problems when the parties are changing a lot - eg Stellar is vulnerable to changes

John W: if you roll your own encryption it's usually a bad idea; is the same true of a blockchain

Andy: last iiw the argument was blockchains was for everything, now we're seeing skepticism which is interesting

Maria Vachino: that was why I proposed this

Andy: What are the things that you can get with the blockchain that other tools provide

Christopher Allen: don't be on the bleeding edge of blockchain; there are lots of things you can do without that - with 8 parties you could ahave a round robin consensus model and still have a blockchain ledger - if someone comes up with something better than proof of work we'll shift over

Kevin Marks: Blockchain is not provably collusion resistant - the 2013 fork resolution was solved by collusion

Joaquin: is blockchain resistant to bad implementations?

Christopher Allen: there's 7 billion dollars of reward if you can crack bitcoin

Kevin Marks: well, there's the ability destroy 7 billion dollars if you crack bitcoin; you don't get them

Christopher Allen: bitcoin is arguably antifragile as it absorbs a lot of attacks

Ryan Shea: what blockchains are bad at is like what databases are bad at - they need to be part of a system. some people have talked about storing data in the blockchain - that has always been a bad idea

Christopher Allen: there are things created in blockchain that don't have to be used in it - multisig and hd signature are examples - Merkle Trees are cool

Cross-Domain Identity Management: SCIM Interop Discussion

Tuesday 3E
Convener: Phil Hunt
Notes-taker(s): Phil Hunt & Prateek Mishra

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

A number of people came to hear about SCIM Interop. We discussed that an interop is being held next Month and concluding at the Cloud Identity Summit in New Orleans on Monday June 6: https://www.cloudidentitysummit.com/en/events.html

The interop is following the format that was carried out for SCIM 1 but updated for SCIM 2. Participants will arrange with each other to test each other's clients and servers over the month of May and report back on their findings.

Long term we discussed that we would like to see an organization like OpenID Foundation take on a certification process along the lines that OpenID Connect has already done.

We had some general Q&A, who is implementing, and talked about some of the new work regarding provisioning events. More about that on Wednesday.

We had some really good discussion on the issue of "soft" or "tombstone" deletes and the paradoxical issues that some service providers are mandated never to destroy data while others must destroy it. In enterprises, there are particular problem with employees that return to work and previous authorizations are lost when new identifiers are issued or used.
For more information see the proposal from Morteza Ansari at:
https://tools.ietf.org/html/draft-ansari-scim-soft-delete-00

Those that are interested in working on Soft Delete, or participating in the SCIM Interop are invited to join the SCIM mailing list and let the group know. See: https://www.ietf.org/mailman/listinfo/scim

Notes From: Prateek Mishra
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

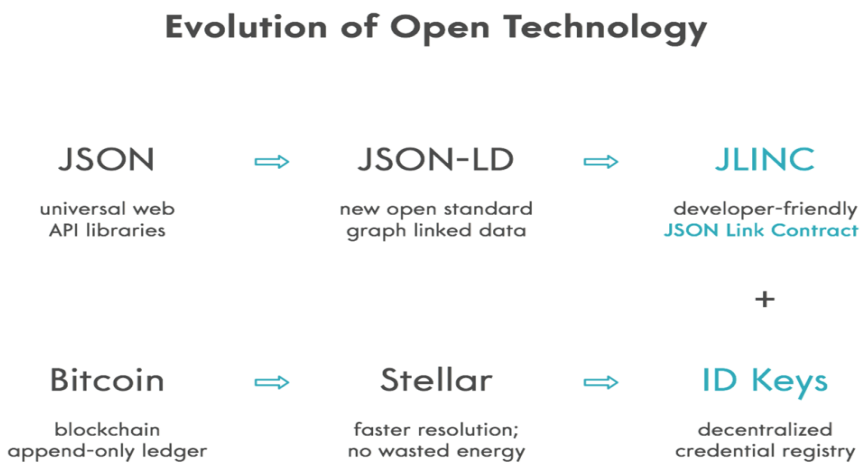
Kelly - SCIM 1.0 testing history - hand built script to test user create/delete etc. The real challenge was that there was no way to describe required attributes, so it was difficult to communicate between client and server. So what would be a basic test set for a SCIM 2.0 server? Probably a set of use-cases 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

JLINC Protocol for Data Sharing Chain of Custody

Tuesday 4A
Convener: Victor Grey, Jim Fournier
Notes-taker(s): Jim Fournier

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:



JLINC Technology integration

- JSON-LD –– provides a graph model with libraries in JSON.
- Public-key cryptography –– provides a secure credential token using 25519 elliptic curve keys.
- Blockchain –– Stellar, provides a clean, fast, blockchain to use for a distributed registry for public keys.
- IPFS –– provides a distributed file system for contracts where the pointers to the data are each a hash on the chain.
- JSON web tokens –– provide a universal standard way to pass strings in the header.
- **ID Keys API** api.idkeys.net
- Create a new account
- Four account information APIs
- Get a signature on a JWT
- Send a REF payment
- Following the slides, played animations linked at the bottom of JLINCLabs.com
- Extensive discussion with Adrian of UMA model vs the model illustrated in the VRM animated cartoon followed.

The Hard Problems of Storing Identity Information

Tuesday 4B
Convener: Muneeb Ali, Jude Nelson
Notes-taker(s): Jude Nelson

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

Hard Problems:
- Where you keep data?
- How you keep data?
- Who is to keep my identity data?

Identity is a subset of a user's private and public data. These problems should motivate systems designs for storage.

- PKI - enforces the "who" of storage
- User-controlled storage - enforces the "how" of storage
- jurisdictions, trust domains, admin domains - constrain the "who" and the "how" of storage; must be visible to the user and taken into consideration by the storage system.

Takeaways from the above:
The "who" and the "how" of storage is data-dependent. Users, not the application nor the storage provider(s), are the ones who are most affected by who stores their data, and how they store it. Storage systems of the future need to be built to let the user control both aspects of storage directly, without having to rely on the application to do so. If we do this, then applications cannot be data silos--users would bring their own storage to the application, and the application would only be able to write to the user's storage with the user's consent. It's worth mentioning that this is not only beneficial to the user, but also to the application--because the application no longer hosts user data, it is no longer responsible for keeping it available, and no longer needs to run extra servers to do so.

What had been missing is a scalable user-controlled storage system that can both assimilate existing storage systems into a coherent whole and give users fine-grained control over how their data is managed. Blockstack offers a way forward on this front. Its client-side tools implement storage drivers for existing storage services, which gives users the ability to select which storage services host data and control how they do so. Users can authorize external parties (applications) to read their data, and revoke permission later. We are currently accepting pull requests to add support for more drivers, and seek community feedback on how to efficiently implement storage policies that are easy for non-technical users to control

My Things are Me! Who Backs Claims for My Things?

Tuesday 4C
Convener: Andrew Hughes
Notes-taker(s): Andrew Hughes

Tags for the session - technology discussed/ideas considered:

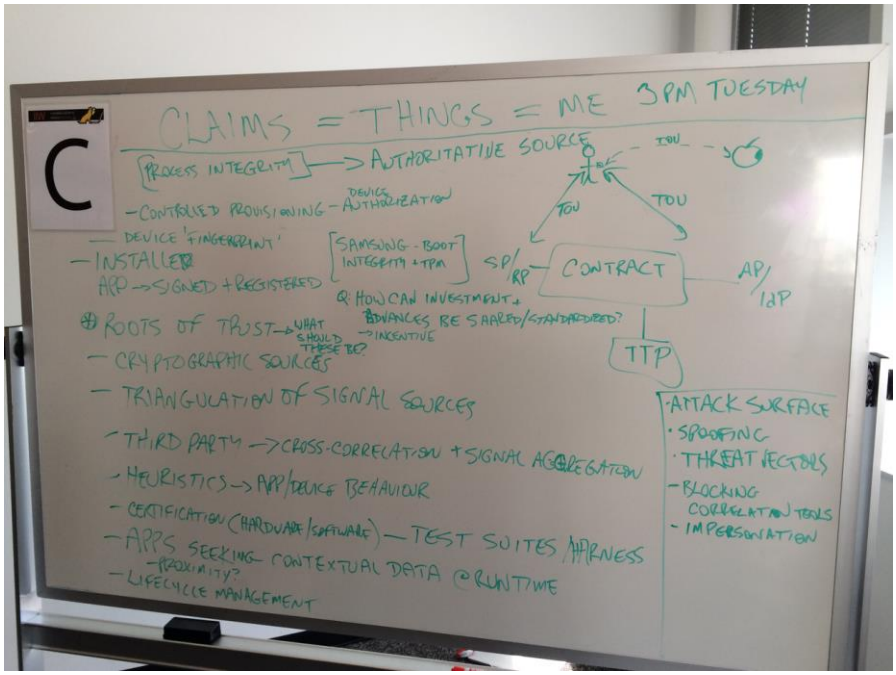
Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

This session explored the ideas around how trust frameworks and contracts can be extended to cover advancements in authentication technologies from mobile and wearables.

Essentially, how can process integrity be ensured/assured for these new technologies?
What is needed to accept claims that data from mobile/wearables is authentic and authoritative?

We discussed how authoritativeness could be reflected in contracts and trust frameworks.

The whiteboard picture is a list of potential mechanisms for establishing authenticity and authoritative data sources.

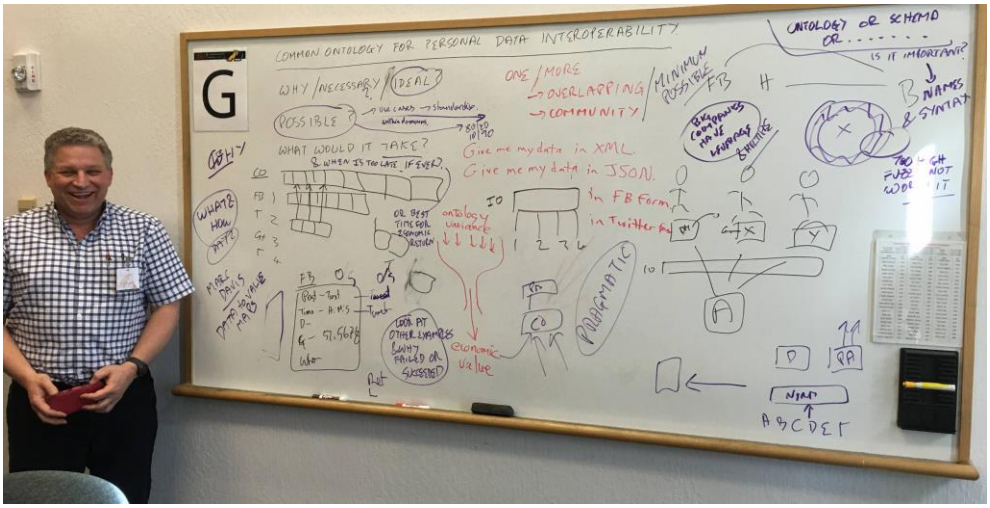


Towards a Common Ontology for Personal Data Interoperability

Tuesday 4G
Convener: Julian Ranger
Notes-taker(s): Julian Ranger

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

1. Agreed that Common Ontology was an ideal to make task easier for all, though was not a necessary requirement in that systems can cope with multiple ontologies if needed.
2. Found it amusing that in talking about a single ontology there was no agreement about whether we were talking about an ontology, a schema, a data dictionary or other term!
a. Did agree that it was about entity names & syntax whatever we call the aggregation
3. Should it be a single ontology, multiple ontologies, separate or overlapping, by community?
a. Agreed looking for minimum possible
b. Today big companies have leverage forcing all to use their ontologies, which results in many variants needing to be implemented - would like to reduce towards one for personal data exchange/use
4. In looking at a common ontology:
a. Need to be pragmatic vis perfective
b. There will be a fuzzy boundary around a core ontology where items cannot be resolved - need to live with that provided the level of fuzziness is not too high
5. A discussion on whether it was possible to create a single ontology concluded that it would be - after all many companies do this internally as they have to
6. Agreed should have a further Part 2 session at this IIW to explore what it would take to create a single ontology (or minimum set) - the What & How. Points to note:
a. Look at use cases and solve for those first
b. Look at other ontology standardization examples and why they failed or succeeded
c. Discuss "Data to Value" maps
7. In terms of timing agreed it is never too late, but best economic value is to do earlier whilst personal data exchange from/by people is in nascent stage



Scalable Consent: Effective, Informed, Revocable

Tuesday 4I
Convener: Ken Klingenstein
Notes-taker(s): Ken Klingenstein

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:

Topics

• Use cases and requirements

– Enterprise internal and federated

– Boots on the wire today

• Scalable Consent

– Architecture

– UI

– Application behavior connected to attribute

– Status

– Informed Content

• Lessons learned

The internal and federated use cases

• External consent

– Classic federated use cases:

release

• Difficult because of their often international aspects

• In the US, a significant number of "policy deciders" are not in central IT

• EU GDPR (General Data Protection Regulation) has raised the bar

• Internal consent

– Examples are the student app marketplace at

– Consent needed per requirements of data

– May involve protocols beyond SAML, including Duke and the departmental app marketplace at UW stewards, both central and distributed

OAuth and OpenId Connect

What's on the wire?

• Opaque non-correlating transient identifiers

• Opaque pair-wise persistent identifiers

• Opaque correlating persistent identifiers

Local Federation Registrations

Kim Cameron's Laws of Identity

Approaches to attribute release and consent

• Institutional policies and individual choices – End-entity categories (e.g. Research and SAML End-user consent Scholarship)

– Consent to release user's attributes

– Oriented towards IdP, transactional consent with

– Client side and server-side Shib options

• OIDC and Oauth consent

– Consent to access a user's resource

– Oriented towards RP, persistent consent with

• Multi-protocol consent infrastructure (+ Shib shim) suppression options, revocation options, Scalable Consent

• Components to create a scalable consent experience and infrastructure

– An infrastructure to deliver the capabilities and

– A user interface that enables a user to make the information to allow users and administrators manage their attribute release from their identity provider at scale effective and informed decisions about attribute release experience

– Tools for an enterprise to manage that user

• Catalyzed by an NSTIC grant from NIST, becoming part of the TIER suite

• Web site

https://spaces.internet2.edu/display/ScalableConsent/Scalable+Consent+Home

Consent Requirements

• Derived from use cases, usable privacy research, legal regulations, etc.

• Fine-grain attribute release capabilities, with use of “bundles” and “meta-attributes” as needed

• Informed consent that is hierarchical, flexible, accessible, etc, with clear, concise human-readable explanations of attributes to be sent

– Additional detail provided when needed, including which attributes are required, values of attributes, how SP will use each attribute, how long SP will keep each attribute (attribute privacy policy)

• Revocation of an attribute release policy (out of band is fine)

• Ability to convey trust marks and other guides to user

• Providing a variety of options for attribute release during future visits to the same site, including using the current settings, periodic resets or reconfirmations, out-of- band notifications, etc.

• Provide an audit interface and history to support both privacy and security

• Ability to work across protocols

• Ability to work on-line and off-line

• Support for identity portability

UI (PrivacyLens) as a paradigm

• Enabling effective and informed end-user consent

• Embraces a set of capabilities

– Hierarchical information, fine grain control, bundling, revocation of consent, flexible notifications, etc.

• Embraces a style of presentation

– Clear screens and slides

– Optional display of values being sent

– Affirmative user actions

• Integrates across use cases

– Protocol-agnostic

– On-line and off-line

– Allows a variety of information sources

• UI built on an open consent management infrastructure

– Can be replaced, skinned, etc.

Releasing an opaque identifier only

Anonymous comments

With only the opaque identifier released, individuals may post comments while preserving their anonymity within the community.

Releasing an opaque identifier and some personal information

Releasing an opaque identifier and personal information

Scalable Consent Infrastructure

Integrating organizational and individual policies

Informed Content

• The information and trust sources for Informed Consent

– The fuel that feeds informed user consent

• What do we need right now?

– MDUI (Graphic Icons) for IdP and SP

– IsRequired Attributes

– Meta attributes

• What we need soon

– Informed consent dialogues

– trustmarks - e.g. R&S, CoC, IDESG

– third party reuse and other privacy policy thinking information

Informed content dimensions

• Data fields

– Icons, required attributes, trustmarks, privacy policies, etc.

– Federated agreements on syntax and semantics

– Easier for internal federations to manage

• Transports

– SAML metadata, well-known URI's, publish and

– Much to understand on the fit of transport to

• Trust management

– Vetted, self-asserted, reputation system based Lessons Learned – Consent Management

• Consent management at scale seems viable, but needs plumbing infrastructure and content

• Contractual vs non-consentable vs

• Need to guard against user habituation, oppressiveness; need to permit rubber squeeze toys

• Applications don't know how to do data minimization

– Very few are privacy-preserving; most lead with a subscribe mechanisms, etc. data to trust request for identity when, at that point, only statefulness is needed

– "You are what you release" functionality not leveraged

• Deep devils in the details

– Selective release of values from a multivalued

• The hard part will not be the infrastructure design and build but developing and maintaining the information that runs through it attribute

For more information:
https://spaces.internet2.edu/display/ScalableConsent/Scalable+Consent+Home

– Scalable Consent Overview https://work.iamtestbed.internet2.edu/drupal/

– PrivacyLens and Consent Management infrastructure

https://work.iamtestbed.internet2.edu/confluence/display/YCW/Yourtown+Community+Wiki+and+Service+Portal – Privacy-responsive and attribute aware applications

Constructive Notice: What must we do?

Tuesday 4J
Convener: Joaquin Miller
Notes-taker(s): Joaquin Miller

Tags for the session - technology discussed/ideas considered:

#constructive notice

An example of constructive notice: You load a web page, at the bottom of that page, not visible in your browser, is a link, "Terms and Conditions." You have been given constructive notice of those terms and conditions. Why? Because you could have scrolled down and seen the link.

The question for discussion: How can a person give constructive notice to a vendor of that person's conditions for continued use of a facility provided by that vendor over the internet?

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

No one came.

At dinner, convener learned from Joyce Searles, Mary Hodder, and Doc Searles that folks working on VRM have this question on their agenda.

Key fact: The doctrine of constructive notice is distinct from the contract type, contract of adhesion.

https://www.law.cornell.edu/wex/constructive_notice

https://www.law.cornell.edu/wex/adhesion_contract_contract_of_adhesion

Consent Receipts

Tuesday 5A
Convener: John Wonderliech
Notes-taker(s): Jim Fournier

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

ConsentReceipt.org

Biggest lie on the internet

Alice & Bob comments on blog

Alice wants to comment on Bob's site:
collect info

notice
submit

Bob makes commitment
How does Alice know its true?

Minimum viable set of info for receipt?

Do piracy policies protect your privacy? No
Risk management for corp

Receipt for value
follows transaction
memorialize commitment by Bob to Alice

Status of project:

JSON object notation in process

Health? In Canada depends entirely on consent

If not option to say No, its notice not consent

Should not use info for any other purpose

Same blank looks in Silicon Valley in China, why can't we just use the data?

Whats the difference between whats in receipt and privacy policy?
Evil Bob's privacy policy favors corp entirely as broadly as possible.
Nobody reads them, may or may not comply locally.
Receipt shows Alice what she agreed to. Surfaces by UX perspective
Privacy = contract of adhesion
Whats the URI in effect at the time of transaction?
Change in terms of service notice now.
Creates shared display and enforces old terms until new agreed.

In the US FTC, promise what you will, but abide by it.
If Alice doesn't agree to new policy.
Don't go back to site.

Add this to your CRM

For EU GDPR:
fine = 4% of global revenue
if marketing material is added, must be user opt-in option
now receipt shows opt-in
that can become part of CRM for Bob
mass personalization based on consent

Without receipt Bob can't currently track which terms apply to which user.
Share the terms with the user, keep a record of them, and share that with user.

Google Groupon-like example, unauthorized charge to mom's account for daughter's action.
Should have been a receipt in new paradigm.

How do I revoke consent?
GDPR says has to be as to revoke as to give.
UUID reference number, but up to Bob how to do it.
CR opens channel to do it.
In health or research one-way door, HR, internal enterprise, could simply be notice.

PIMS not getting traction yet, last pass, one pass, key pass, could add CR.

Bob could ask for proof of identity.

How different than PP?
Doesn't replace, creates communication record of actual exchange.
Information power asymmetry.

Could tie PP to Terms of Service and keep better records.

Semantic standard plugin can only happen with standard.

CR contains URL of existing PP
no crypto sig in early example
for enterprise will get more robust

creates point of agreement, protects enterprise too

now UUID on receipt
minimum viable 2 party isolated transaction
some use-cases don't want 3rd party

Goal is to address power imbalance, organizations winning, gov, corp
also compliance and human rights under GDPR

comment:
simplified ToS on a page
for start up offer vetted standard

Can help Enterprise manage risk: working example Optinon in UK

No metric for companies that want to claim that they are better on privacy.

R&D Funding for Your Project

Tuesday 5B
Convener: Colin Wallis
Notes-taker(s): Colin Wallis

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

Identity and Privacy projects (a new and much less cumbersome channel than those currently in existence). Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

file:///C:/Users/colin/Downloads/Kantara-v3template%20CCICADA%20IIW%20April%202016%20.pdf

UX Design of Identity Systems

Tuesday 5F
Convener: Guy Lepage
Notes-taker(s): Scott Fehrman

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

Current state of systems has been pretty bad
How user can take control of their identity
Typically for users that understand the technology
Current State

- OpenID
- Required to log into some identity provider, FB Login
- Need to create an account ... Provides data or reference an existing account
- Onboarding challenges
- Adopting delegated identity data, reduced the friction
- SSO ... Leveraging and initial
- Account recovery
- Level of assurance
- Level of authentication
- Limiting friction
- In enterprise, need to make other people happy, not necessarily the end-user
- In consumer its the value of the service or offering
- Do you collection data just as needed or everything at once
- Show incremental value as the relationship is built with the end user
- People that use the Forgotten Password process for infrequent logins
- Entering repetitive info

Goal ... How to improve on the experience
Different use cases ... Registration , Login, Proofing
In US no core common service for proofing
What about people that don't have access to modern technology
Balance of friction vs. value
Consent
Timing of when you ask for "something" during a process
Appropriate content
Knowledge based system to do login / access control
Respecting Identity
What's the level of assurance?

Identity & Payments

Tuesday 5C
Convener: John Best
Notes-taker(s): John Best

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

We discussed the challenges that Banks and Credit Unions face in today's payment environments , including phishing , smishing, vishing, and other account take over mechanisms. In particular we discussed how sovereign identity could help the Financial institutions reduce this kind of fraud. Scott David discussed several regulations that could prevent banks from taking advantage of sovereign identity. Some ideas that came out of the discussion

1. Family watch – the idea that sovereign identity would have a family component and allow the FI to have others in the family watch the accounts besides the account owner. This was particularly interesting as the elderly are frequently taken advantage of , so family relationships via sovereign identity could allow for emails or other messaging to be routed or copied to another individual for review before forwarding on.
2. Entity to entity communication- reviewing the remote account before funds are sent. Having sovereign identities for entities such as banks would allow communication between the banks more easily and could result in reduced ach fraud by allowing the sending bank to validate the account at the receiving bank before transacting funds.

The session closed with discussions around identity and social engineering, how to prevent social engineering with sovereign identity.

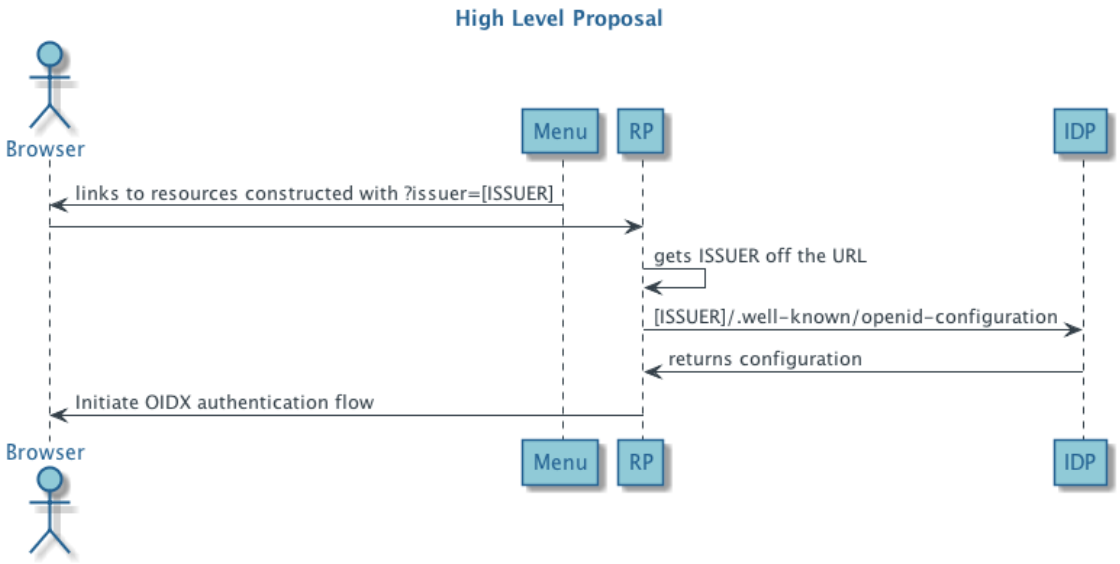
Open ID Connect

Tuesday 5G
Convener: Judith Bush
Notes-taker(s): Judith Bush

Tags for the session - technology discussed/ideas considered:

Discovery, EZproxy

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

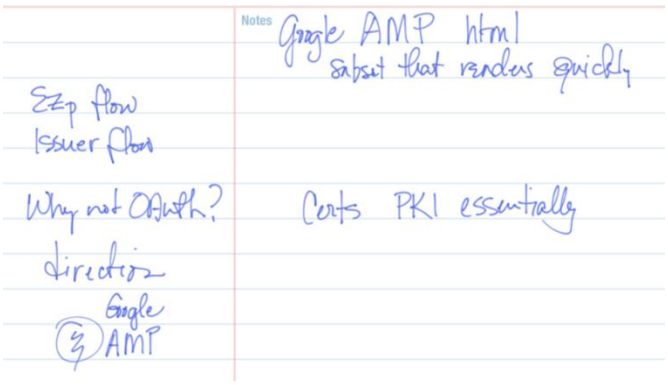


<?xml version="1.0" encoding="UTF-8" standalone="no"?>
OpenID Connect uses WebFinger[RFC7033] to locate the OpenID Provider for an End-User. Once the OpenID Provider has been identified, the configuration information for that OP is retrieved from a well-known location as a JSON document, including its OAuth 2.0 endpoint locations. "

Issuer discovery is OPTIONAL; if a Relying Party knows the OP's Issuer location through an out-of-band mechanism, it can skip this step and proceed to Section 4.

issuer
REQUIRED. URL using the https scheme with no query or fragment component that the OP asserts as its Issuer Identifier. If Issuer discovery is supported (see Section 2), this value MUST be identical to the issuer value returned by WebFinger. This also MUST be identical to the iss Claim value in ID Tokens issued from this Issuer.

* Oauth flows don't match the library flow model
* Will look into Google's AMP protocol



SCIM & Open ID Connect

Tuesday 5I
Convener: Prateek Mishra
Notes-taker(s): Mike Schwartz

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

SCIM - System for Cross Domain Identity Management Specs are here: http://simplecloud.info
Provides schema for use objects, for example:

{"id": "12345680", "username": "joe", etc.}

REST API's for user and group management.

OpenID Connect provides for federated authentication, and provides user_claims

Why can't we use SCIM schema in OpenID Flows?

OpenID has a "profile callback mechanism", i.e. user_info endpoint.

Using the information coming back from OpenID Connect, an relying party may implement "Just in-time" JIT provisioning

OpenID Connect defines its own (different schema) for a person (does not define groups or roles).

Mike Schwartz pointed out that OpenID Connect is used to enable a person to authorize the release of attributes about himself, whereas SCIM is used by the enterprise to provision users in a SaaS.

Phil Hunt pointed out that OpenID Connect is generally delivering simple attribute value pairs, SCIM is better at conveying complex attribute values.

Use Case: An enterprise with a directory service needs work with a SaaS Provider. The SaaS Service provides a SCIM endpoint to enable the enterprise to provision user and group information. SaaS

service needs to advertise its scim endpoints via a Manifest. Does the SaaS need to do JIT? Or Bulk provisioning? JIT does not support de-provisioning.

Prateek says Oracle is interested to start a working group about this problem so it can solve their internal SaaS and industry SaaS issues.

Phil has published a SCIM discovery Spec: https://tools.ietf.org/html/draft-hunt-scim-discovery-00

There is also SCIM configuration endpoint: https://tools.ietf.org/html/rfc7644#section-4
Prateek says the business problem is that SCIM lacks coherent security that makes it a real standard across many service providers.

Anonymous Credentials: Will they ever be practical?

Tuesday 5J
Convener: Francisco Corella & Karen Lewison
Notes-taker(s): Karen Lewison

Tags for the session - technology discussed/ideas considered:

Anonymous credentials, U-Prove, Idemix, unlinkability, Javascript local storage, Javascript service workers, IndexedDB API

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

Anonymous credentials, which provide varying degrees of unlinkability, include U-Prove, Idemix, other methods of providing zero-knowledge proofs, blinding techniques, group signatures.

One difficulty with implementing anonymous credentials is storage of the credential, as exemplified by Microsoft's implementation of U-Prove, which stored the credentials in a Windows native app, making it platform-specific. Now, credentials issued by web apps can be stored in browser local storage accessible through the IndexedDB API. Possession of the credential can be proved by an offline front end of the issuer via a JavaScript service worker, without involvement of the issuer back end, avoiding linkability by timing correlation.

Other problems with anonymous credentials are: complexity of the cryptographic algorithms; revocation, in that a traditional revocation list precludes unlinkability; U-Prove had no solution, Idemix used very short term credentials that are valid for only a few hours; there is the possibility of timing correlation on reissuance, if credentials are "picked up" after a gap of several issuance cycles; instead, IBM is now implementing dynamic accumulators. Last is the prevention of credential sharing, which is a difficult human engineering problem.

Wednesday April 27

Bridge to #Meatspace 1

Wednesday 1A
Convener: David Kelts & Anil John
Notes-taker(s): Scott David

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

Pre.imminary questions and Credit card is an example

Question whether physical space is merely type of information space that is embodied – we solve many problems today by bridging the continuum. Information encoded in physicality. May make it easier to bridge. How is it presented. How do it in a way that not exclude technology people. How be inclusive. What you are, what you have, and what you know. This is blended in the case of cyborgs.

Are we talking about info space to meatspace, or vice versa

Bridging digital identity into physical world

Three categories

Note

Use cases
Age based Purchase

Border Crossing
In-Store Pickup
Enroll for Account/Bank

Implantable defribrulators (inplants without user interfaces, only connections)
FDA issue, prescription, license subscriber, individual control

Metabolism as a service

Emergency responders – ability to effect the intelligent systems that are present there

Patient ID at POS

ATM Usage

Banking

Connecting physical presence at a terminal with Border crossing, ATM electronic activity there.

Break glass mechanism is emergency room.

Cyborgs

Contract signing

Bridge to #meatspace (technoloiges)
Biometrics – Nonrevocable, but there are use cases where they can still be useful. There are security and privacy implications of that. Biometric is great way to do step up authentication, but if done in way that provides the biometric to another outside of the control of the data subject, then a problem of revocation. There is a class of revocable biometrics. Square payment use case – wifi – automatically sends your picture to restaurant – they can compare. Also, a drivers license – has a picture, which is a form of biometric identification that works in the non-digital space. They work well in the analog space. Like card is present system – face is present system.

Touch ID – still can use biometric because combined with another one. Many are too quick to dismiss biometric, in those settings in which also need to be "present" to use it. "I am here" doing this authentication so it is part of the ceremony.
Multiple factors in a serial fashion can help address it (Hybrid technoloiges).

Chip cards
Implantable secure element

RFID chips

QR scans – Put JSON in QR code –

Tokenization Tech

What know/have/are bridges – when inplant

What do if no technology available (refugee example)

Transmit channels – NFC is channel – data can go across it. Protocol is there to transmit information. Can you also include an identity protocol in it. Discussion of difference of channel and protocol.

Transmit protocols – how share information, how jump start ecosystem.
Iris scans read at 35 feet

What are the effective real world protocols that are in use today – if want to drive adoption, they need to be at least as simple as what have today.

Security and Privacy
Inclusiveness of non-ID holders - Spoofability
Policies that ensure trust
Strength of Authentication after presentation
Thin line between authentication and authorization
Inability to change IRIS scan

Need to consider life cycle - How to unbind the credentials is important – right to be forgotten legislation type issues.

What class can be used remotely versus in person

Attacks between the secure element and the channel is an issue.

Authentication is going to get solved – how present the credential and get started.

Lots of meat behavior – the selfie – During the Haiti crisis – quickly bootstrap the picture taken into security context.

Even if have biometrics that can match – still policy reasons that might not use them – Such as banks not accepting certain biometrics and other credentials. Entity that is receiving the credentials has its own policies

Different biometrics can have inconsistent results.

What is entropy that is binding data.

We didn't get to the protocols for conveying information

What if…UMA RPT Was An OpenID Connect Access Token?

Wednesday 1D
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:

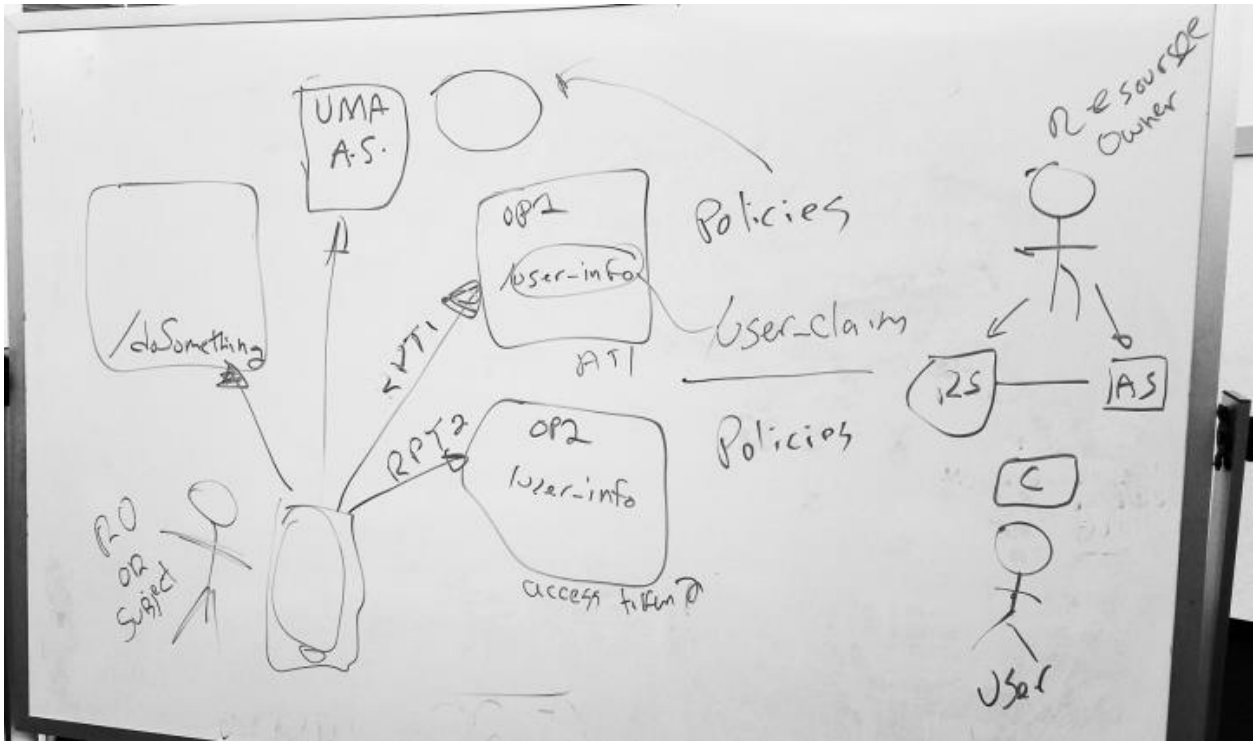
Mike Schwartz of Gluu provided a high level overview of UMA and OpenID Connect.

The idea he proposed was what if an UMA RPT token could be used to protect the OpenID Connect user_info endpoint, instead of an OpenID Connect access token. He posted a similar idea here http://gluu.co/oauth-identity

George Fletcher of AOL suggested that this might not be necessary, because perhaps you could use OAuth2 to issue all the necessary scopes, and then use the refresh token to downscope the token to the required OpenID Connect scopes. However, that aside, it still seems like OpenID Connect falls a little short for this purpose: providing a solution for distribute user claims aggregation.

There seemed to be consensus that this might not be a bad idea. However, it would not be the user_info endpoint, but a similar endpoint that also provides user claims (but is not the user_info endpoint).

Unfortunately however, Mike pointed out that he doesn't have time to embark on such an effort. But maybe someone else does?

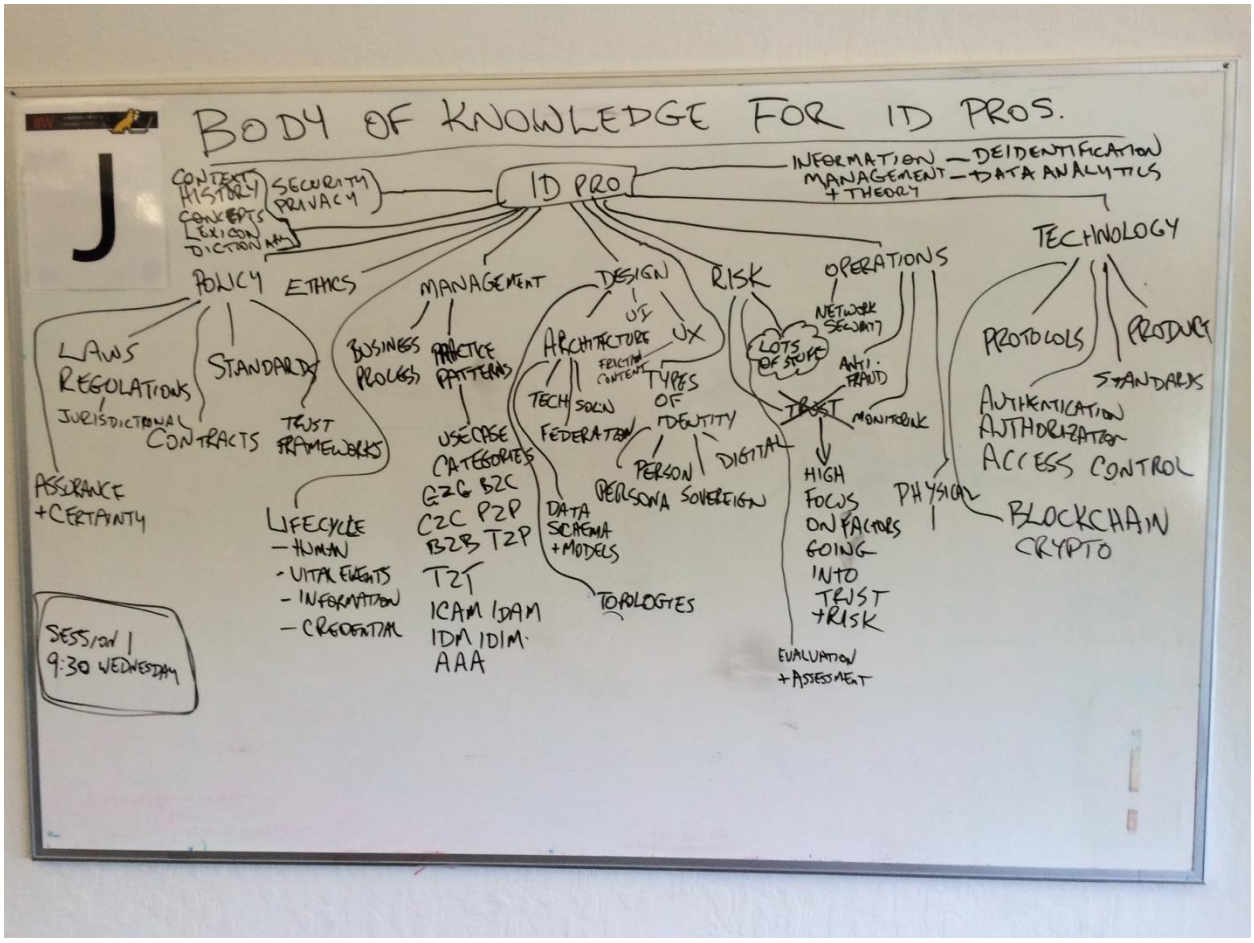


Body of Knowledge for Identity Professionals

Wednesday 1J
Convener: Andrew Hughes
Notes-taker(s): Andrew Hughes

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

The group brainstormed ideas for the body of knowledge that should be expected of an Identity Professional.



Black Box Algorithms

Wednesday 1I
Convener: Kris Alman
Notes-taker(s): Tom Leon

Tags for the session - technology discussed/ideas considered:

How do the algorithms that private companies are creating impact the balance of power and control of personalization vs person-centered applications in Education, Health, and other industries

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

Resources:
Black Box Society – Frank Pasquale (http://www.greenapplebooks.com/book/9780674368279)
Audrey Watters – blog post "Identity, Education and Power" (https://medium.com/identity-education-and-power/identity-power-and-education-s-algorithms-a766527bb6cd#.vugr7k73q)
Initial Statement:
Man made algorithms that are making decisions on people (credit decisions, education decisions, etc.)
Asking questions about what is happening, specifically in education
There is a company called Knewton, who has teamed up with Pearsons, Houghton Mifflin, etc. These are companies that are known for creating curriculum; as more materials go online they need to close the loop on how to do assessments.
In doing personalized learning, they are de-linking the teacher in the equation. Based on how they are doing, they are moving people (children/students) up and down the learning channel.
Education and HealthCare are deeply personal
Education: FERPA and COPPA
DOE governs FERPA, FTC governs COPPA
Affects where we go, what opportunities we have, etc.
If there are black box algorithms that are becoming part of the big data brokers, you don't know what info and decisions are being made.
Patient Privacy Rights: Org that looks at issues of HIPAA
HHS governs HIPAA
How do we have access to our medical records and where do we go from there
? How do we deal with the privatization of these services that are integral to our futures?
? When you are talking about agency, children have little capacity to make their own decisions. How do they gain agency – can they?
? Is the concern that the power is being taken out of the teacher's hands in guiding the student?
What are the means that you as a parent/legal guardian have to address the student's path through their course?
Kris gave and example of an algorithm affecting a pacemaker that is addressing AFib. Should people have information into how these work so that they can understand how
CONCEPT: is this similar to Redlining where a person is deliberately excluded? How do you get out of this How do you know, how do you check? Who is profiling you and how do you change what is being profiled?
Whatever metadata might be created out of a company that is proprietary may include personality traits.
Keystroking pacing
How long does it take to accomplish something
The soft skill of "Grit" – does a student keep at trying to accomplish a goal

Businesses can do with this what they want, and the metadata is not governed by COPPA/FERPA/HIPAA
There is no Private Right of Action
BlueCross/BlueShield example
Customers of BCBS have no right to sue because of these breaches
EXAMPLE: There is health insurance that is regulated and other that is not regulated.
Big Companies used ERISA (Employee Rights law)
They would go to United, Kaiser, Cigna, etc. and purchase directly with these companies as administrators
Because they did this, nobody is minding these plans offered by the big companies
? If companies can gather information about their employees, they can use it against their employees?
THINK Tim Armstrong/AOL calling out the Million Dollar Baby
Do you get put on the list of people who cost too much?
? WHAT should we do about these black box algorithms?
Is it a technological issue?
Is it a policy issue?
Person-Centered vs Personalized
How do you put the student at the center
Need to humanize it – move it back to being Person-Centric and not just personalized
What does it mean to be "Personalized"?
Is this a corporatized way to use language that sounds good on paper but is not really quantifiable?
Education: Is it working? Algorithm says that a student is doing well, but teacher disagrees
Should the box be open? Should people have insight into what is going on inside the box?
Respect and Transparency. They should have some insight into what the algorithms are expressing
Tools
Market Forces should give the power back to the parents/students/patients
There is a tension, an asymmetry
What is the key to Value. What are the problems, and how do they manifest themselves in the market?
These need to be embedded.
There is a cultural aspect.
Who are the stakeholders? Not just shareholders ~ Community
Today this is not necessarily about just making money.
If the stakeholders (Parents/Patients) want to see something more Person-Centered
Need more options.
What if we took a different approach?
If you started to talk about design principals and values that could be embedded in the product culture
What would that look like for these different sectors – Education / Health Etc.
How can these laws of product designs be drafted and adopted by innovators?
How do we have corporations respond to stakeholders
I am not sure about your Personalization; how do we move to Person-Centered
How do startups compete with the monopolies?
The startups will start driving more Person-Centered services that respect the individual, that are transparent and are meeting the individual needs
CHALLENGE: How do we get buy-in from the stakeholder

Monolith to Microservices

Wednesday 2C
Convener: Will Tran
Notes-taker(s): Will Tran

Tags for the session - technology discussed/ideas considered:

OAuth2, #JWT, #Microservices

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

Microservices:
What do they look like?
- HTTP based (mostly)
- Do one thing well
- Bounded context
- well defined APIs
- independently deployable modules
- Dimension of business capability

What do teams look like?
- Pizza box sized teams
- Agile methodology

What do you get?
- Velocity
    - lower team communication overhead (smaller teams and well defined boundaries of responsibility)
    - enables continuous delivery
    - teams focused on a smaller domain can iterate faster

Note: I thought Alan was being sarcastic when he called out some of these things with "that's not obvious" but my sarcasm meter may have been over sensitive so I tried to finish up this section as quickly as possible. Recommended reading if you need more details or convincing:
http://pivotal.io/platform/migrating-to-cloud-native-application-architectures-ebook

How to get there:
Full Rewrite -> not very agile
Take a business capability that is ripe for evolution. Maybe a new capability, or an existing capability that you want add lots of features to. This becomes your first microservice.

What that looks like: Assumptions: AS, Client and Resources are all owned by the same entity, e.g. a mobile banking app. Trust cannot be assumed between the applications or teams that deliver them. All apps trust the AS however.
Step 0:

Mobile App (Client)
get a token (e.g. via authcode grant like
https://developer.pingidentity.com/en/resources/napps-native-app-sso.html)
Should this be opaque or JWT? If the body is sensitive, make it opaque.

Authorization Server (AS/OP)
- determines the token's scopes

monolith (Resource)
- verifies identity through /userinfo
- verifies scope through token introspection

Step 1: Add Offers Resource (e.g. sign up for this credit card)
- Should the Mobile app use the same token for both the monolith and Offers?
    - No. This would violate the principle of least privilege, as the monolith could reuse that token to access offers directly and vice versa.
- Should the Mobile app get a token use the same token for both the monolith and Offers?
    - No. This would tightly couple the mobile app to implementation details.
- Solution: Use an API gateway
    - API Gateway exchanges the opaque token for a JWT (e.g. ID Token with scopes) whose scope and audience is restricted to only the resource to be accessed.

Step 2: Add Analytics Resource (app -> GW -> Offers -> Analytics)
- Does the GW get a token can can be used for Analytics?
    - No, that would violate principle of least privilege. Analytics should only be accessed by Offers
    - Offers exchanges the token it receives for a new one whose scopes and audience are restricted to only allow interaction with Analytics.

How to transform tokens?
Opaque <-> JWT at the gateway
- JWE
- Maintaining a mapping in the AS (e.g. persisting tokens, and using jti as the opaque value)
- Could be cached by the GW until the JWT exp

How to exchange tokens?
JWT -> new JWT with different aud and scopes
- RFC-7523 JWT Profile for OAuth 2.0 Client Authentication and Authorization Grants (https://tools.ietf.org/html/rfc7523)
- (Draft) OAuth 2.0 Token Exchange: An STS for the REST of Us (https://tools.ietf.org/html/draft-ietf-oauth-token-exchange-03)

- Questions/Comments
C: JWT verification is hard / I don't trust my dev's to do it right. Let something external do it instead
A: It's easy in Spring Security OAuth (and other libs). Microservices should be as self sufficient as possible. Also we're assuming these services only trust the AS and don't trust each other.

C: Or you could use self issued JWT instead of client ID/secret to authenticate clients
A: Yes.

Q: Why don't you just use PKI?
A: (from audience) not very microservicey, things become tightly coupled and inflexible with PKI
Rebuttal from asker: Well that depends…

C: (after the talk) You can use infrastructure e.g. network security groups to enforce trust domains instead
A: This could be enough for some. This is about empowering the application itself to make these decisions. Developers may not have the ability to manage infrastructure to that level. And if you want to move fast, best to reduce the dependencies on things you don't control as much as possible.

Q: Any best practices on dealing with coarse grained vs fine grained authorization?
A: As an example, you can think of a coarse grained authorization saying "you have the ability to read 1 or more foo", and fine grained as "you have the ability to read this/these particular foo" both could be expressed as scopes, but this could allow a token's scope values to get out of hand. You could mitigate this on the token side by asking for the exact scopes you need when you request a token. On the AS, you'd need to supply it this knowledge of the foo you have access to somehow. If you can't get the AS to deal with that, you could wrap that knowledge around a custom service exposed via some custom API, where the onus is on the resource server to check it; or incorporate another AS that can exchange a token from the first AS and use that knowledge of foos to generate a token containing the fine grained scopes.

Talking About Power Asymmetry

Wednesday 2D
Convener: Kaliya Young @identitywoman
Notes-taker(s): Kevin Marks

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

Annabelle: continue woman's breakfast thoughts on representation of groups we are supposed to be serving - refugees was a strong point the book Asymmetric Society is worth reading: main actors were people; now businesses

A person to a website relationship is very imbalanced - the problem with infocards is you create an illusion that people have power in the relationships, but the big site has more.

Fairness and justice matter we have an opportunity to level inequality Privacy Power differential in tech

Anonymity can be powerful - an anonymous article was cited in Japanese parliament on daycare issues giving a voice

Bill: how do we reshape structure for more symmetry?

[Kaliya reshapes room into a circle]

Anabelle: there are models of fairness where they don't really exist. The Personal Cloud initiative rely on individuals having an electronic resource that they own and maintain. We rely on individuals having the time and money to take care of that We get data anonymity and power for those with the luxury to afford this

Kaliya: Bob Blakely and I have a paper based on a keynote we did on this. Those with wealth and power have more ability to maintain their identity

Annabelle: if you have the resources you can remove advertising
if everything relies on advertising, do we have to reconsider that way of funding the web

Annabelle: "you can chose to sell your data" - we're still framing it as commerce - selling yourself as a product

David: that happens because of lack of trust - if you could trust the assertions we make, would be paid for by the risk reduction for the RPs

Annabelle: if you're a content provider with revenue from advertising, trust isn't going to affect your need to sell that information

Kevin: if we have verifiable claims we are creating an incentive for redlining to prove you only have high value readers

Lewis: VRM is premised on people having the power to share their own data, and get back power from markets

Annabelle: markets don't work that way in practice: in theory every consumer has the ability to shop anywhere for food or banking; in practice a lot of that ends up based on redlining through store location

Lewis: I don't think VRM will take us to the promised land, but we should look at radical changes

Mike: Any situation between humans and businesses is asymmetric by default, as the trust model we rely on as humans doesn't work. One way to solve this is to incorporate everyone, - and I'm mike, inc and I sue you

Annabelle: you can't copyright facts

David W: I like inverting the corporations are people trope but it doesn't really change the power

If corporations have the capacity to mine us to create IP based on our data - the deepest from of IP is our identity; why can't we copyright our identity.

Kaliya: I want to talk about power asymmetry in the physical world - even how we sit in the circle and

who is choosing to sit how – how much space do you take up expresses power and comfort. We watch that happen and need to help those signaling lower power and bring them in. This kind of observational skill and leadership is essential. If we want to make space designed to get input from different populations. There are also gender race and class asymmetries that happen in this community which we don't always bring up.

Mike: there really is real discrimination on the internet. If the thing on the other end thinks you're a woman or a man, or in certain zipcode you see different prices and ads

My daughter si s sociology major, and helped me think about blacklivesmatter that colour-blindness is not a thing that we can do -
classism in power asymmetry is going to fail everybody

Annabelle: people's identity and the various privileges and systems of oppression impacts their experience online - certain groups have to think more about their identity online have to present themselves. A great example is women in the gaming community over gamergate where women are attacked mercilessly for having an opinion on games while female, and presenting as a women can be a threat.

Kaliya: becasue our culture has a lot of power asymmetry it causes problems inherently

Annabelle: Facebooks policy for 'real names' discriminated against Native people's names because they don't look 'real' to the algorithm,or transgender people who don't use their birth names.

Anil: what can we do in order to not impose the first world perspective. What can we do proactively to ensure that. I went to a workshop with non-profits on the role of identity for people who have been trafficked. If you require them to have an identity it makes them much more targeted, which I hadn't considered. As architects, what can we do to bring in those perspectives?

Maybe we should get rid of gender given what goes wrong,. The way we classify our identity gets encoded in code, it's not black or white. It gets messy

David: if the laws of identity are true, then people can assert different identities.

Annabelle: we can't rely on market forces to protect the rights of minorities - they don't have market power by definition - how do we inject ethics into the system?

Anil: this is not abstract for me - I fill out where the market forces don't make sense - i need to bring an investment convening perspective; I don't know the answers. Although I am not the same complexion for people here, I'm not at the margins of society. Problems of power asymmetry exist - what can we do to provide solutions.

Bill: what are design principle that we can build into this - we need to bring people into the deign process. Native Americans, transgender, people fleeing abuse. Identity and relationship matters.

Kevin: markets can empower too - ebay created ways for people to build businesses, whereas advertising is based on stereotyping and prejudice

Annabelle: the same day delivery article re amazon is a good example of unintended consequences - Prime users in certain neighborhoods gave a racist/classist effect that gave a power imbalance. Evaluate your decisions based on that. That we are in this room is indicative of privilege; we are going

to make mistakes. When we get feedback from a community we need to be receptive to that feedback. no one solution is going to work for every community. The way that social space has evolved not he internet - 10 years ago the forum was the be-all and end all -there were walled garden communities with moderators and known membership. We have evolved into this twitter/tumblr model where everyone is screaming at each other. When you talk to the social justice community there is a struggle to create safe spaces for people. You can't do that without that behavior injecting into that space - a single global community doesn't work. Especially when you have groups with mutually conflicting needs for their safe space. We need to recognize that systems don't work for everybody.

Discrimination lawsuits work for race, gender etc but we don't have that based on class. If we dissect power that is correlated with wealth and privilege. If a child has a collection of power imbalances. Class and poverty being the overwhelming factor.

Kevin: class in a different sense is legally represented by class action lawsuits

Anil: privacy and security become a luxury good, only available to a specific class of people. I know nothing about Bill Gates's kids because he can provide that buffer. It's an example of it being a luxury good. Look at the design of systems.

Kaliya: one of the things we need to think about is how we talk to different populations. I would like to write some kind of document about in person dynamics. I'd like to invite people who haven't ' been aware of that to have some kind of knowledge about it. Those who choose to speak about dynamics we see get pushed back on as victims.

Literacy and awareness of this is key

Mike: telcos, military kinds of things are part fo our models –top down, command and control. Our identity systems place people into roles they have to play. we have created a software tradition that isn't embodiment of our beliefs that this should eb an asymmetric system.
What does a symmetrical system look like.

Bill: how our stances in the room effect our design. Watching IIW try to shift the dynamics. Developing a literacy of power.

Kevin: the language of standards is an authoritarian one, and we are told MUST and SHOULD and MAY, and have all evidence and examples removed

ERASMUS - Feedback

Wednesday 2G
Convener: Mike Schwartz
Notes-taker(s): Mike S

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

ERASMUS = Emergency Responder Authentication System for Mobile Users

Mike was gathering feedback on a technical design for mobile identity he has included in a white paperhttp://www.gluu.co/erasmus-white-paper

This solution is being proposed as a potential CCICADA pilot. For more info see: http://kantarainitiative.org/confluence/display/ccicada/Home

Jim Fenton provided some useful insights into strengthening the security around sharing attributes between the mobile sender and receiver. He suggested that a challenge response mechanisms be defined to protect the encrypted attributes, and prevent replay of the credential.

Practical UMA

Wednesday 2J
Convener: Josh Gubler
Notes-taker(s): Eve Maler & Scott Fehrman

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

The UMA Work Group developed V1.0 and V1.0.1 of, and is further developing, the UMA protocol. See:

- http://tinyurl.com/umawg (where you can find a Join link and information about the IPR policy of the group)

The UMA Developer Resources Work Group is developing open-source client libraries, sample applications, and other resources to "seed the ecosystem". There is already work done on a Java "resource server client" (that is, a resource server as a client of the authorization server). See:

- http://kantarainitiative.org/confluence/display/umadev/Home (where you can find a Join link and information about the IPR policy of the group)
- https://github.com/kantarainitiative/wg-umadev

See the attached slide deck for a quick comparative description of OAuth, OpenID Connect, and UMA. Today, UMA can handle "narrow" and "medium" ecosystems pretty well, where the resource owner and the requesting party are in the same domain or in domains that have pre-established trust. The UMA WG is working on resolving architecture issues with "wide" ecosystems, where there is no pre-established trust between the relevant authorization server and claim issuer(s). The issue is kind of like a certificate authority problem.

See the attached "generic flow" PNG files for high-level and low-level versions of UMA messaging flows. Each request/response arrow has a reference out to the specific specification section. See:

- https://docs.kantarainitiative.org/uma/rec-uma-core-v1_0_1.html
- https://docs.kantarainitiative.org/uma/rec-oauth-resource-reg-v1_0_1.html

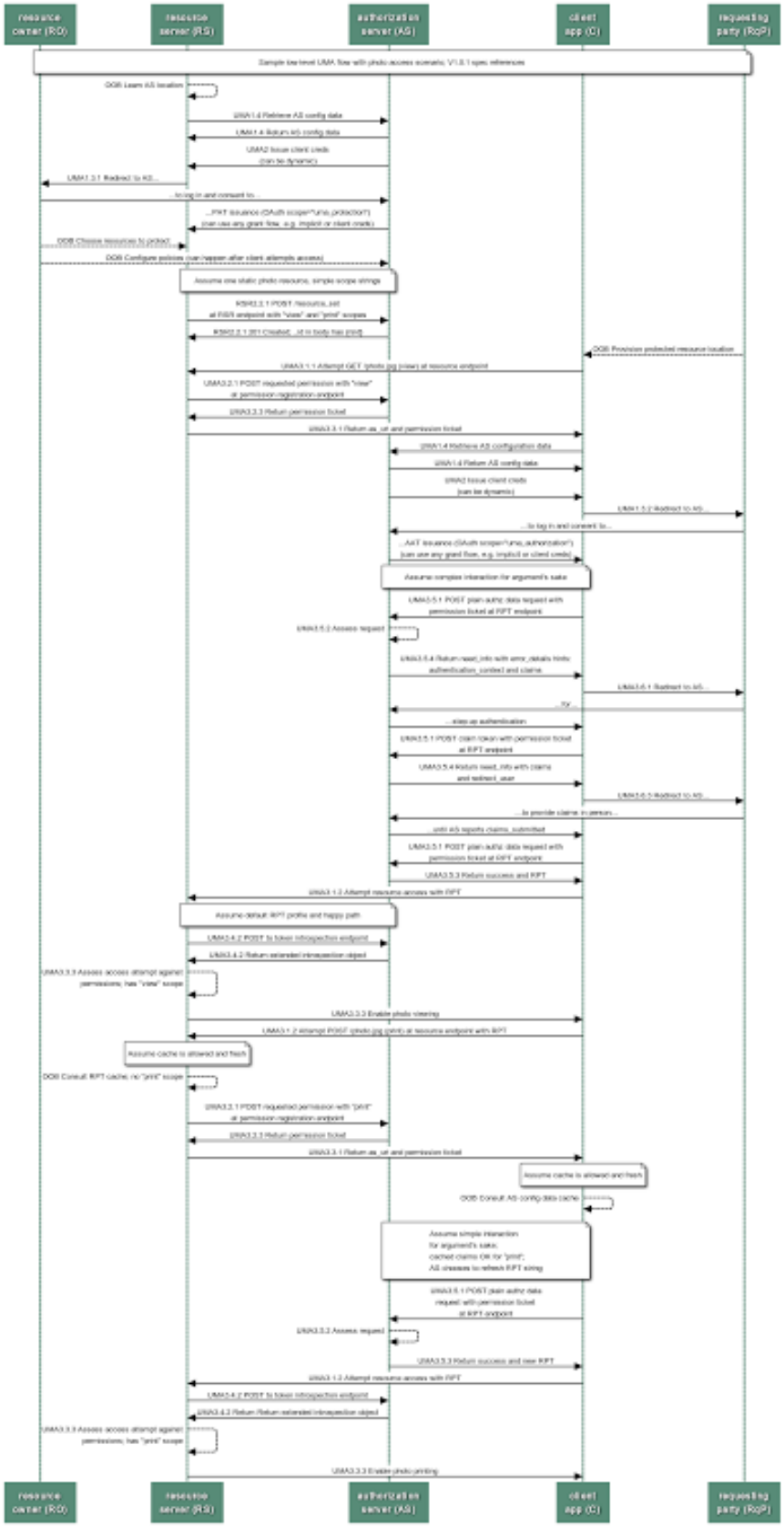
Q: What is OpenUMA? A: OpenUMA is the open-source project underlying Forgerock implementation of UMA in its ForgeRock Identity Platform. OpenUMA is based on the OpenAM and OpenIG projects, comprising the AS and RS components of UMA. See:

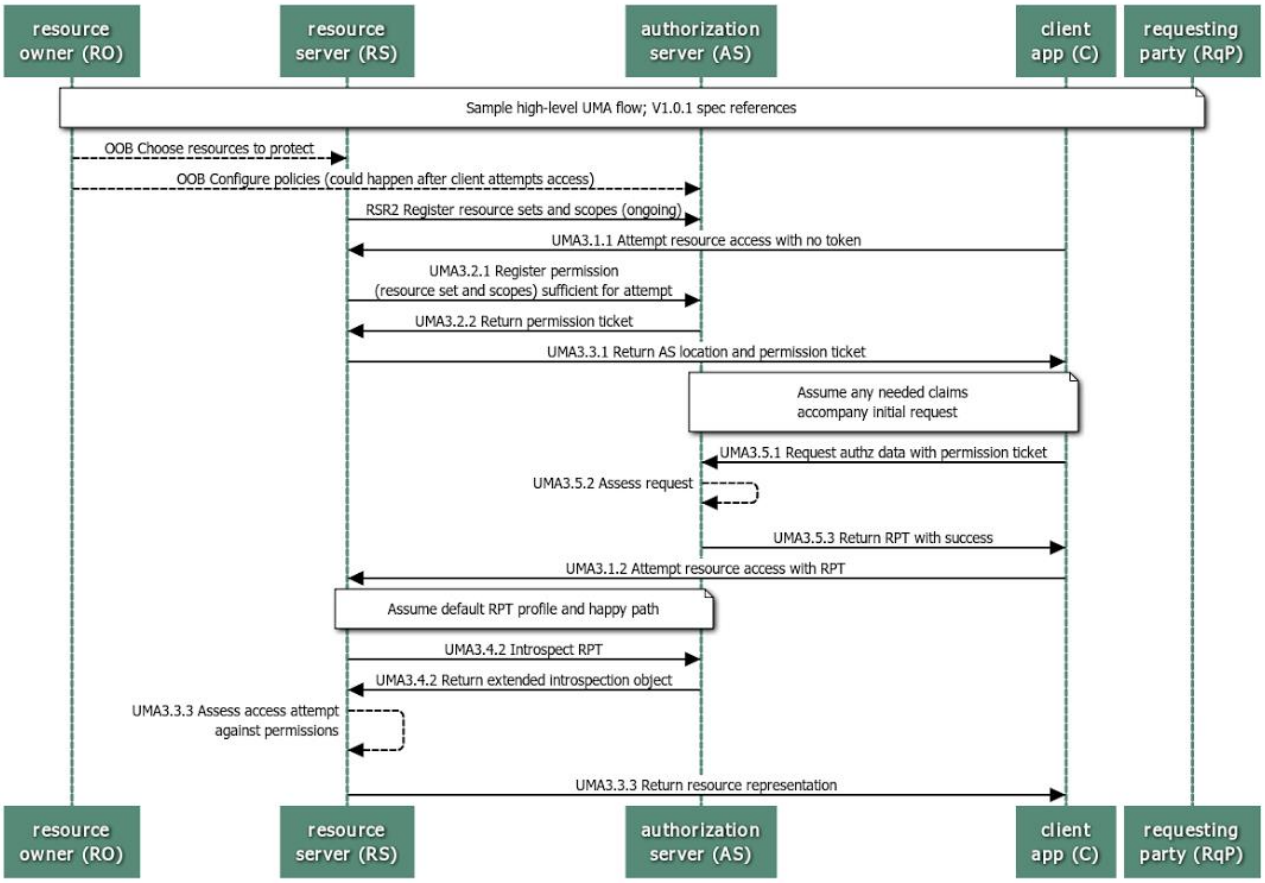
- https://forgerock.org

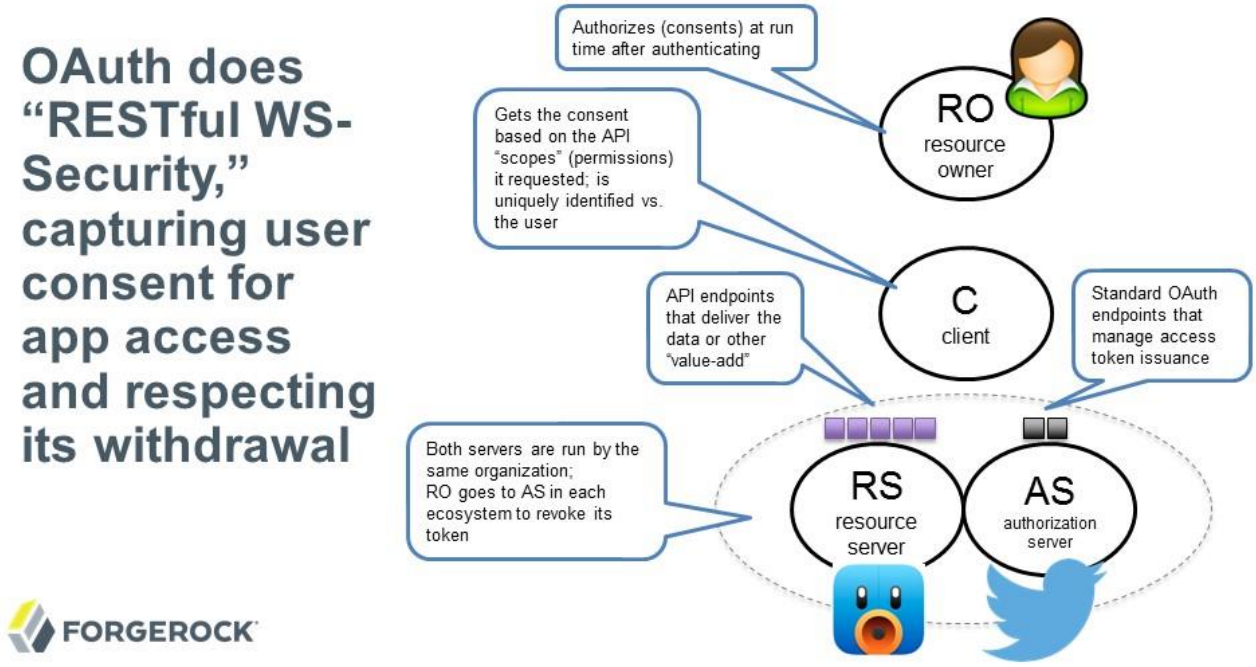
There are several other implementations of UMA, including open source. See:

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

SEE BELOW for CHARTS


resource owner (RO)
resource server (RS)
authorization server (AS)
client app (C)
requesting party (RqP)


resource owner (RO)
resource server (RS)
authorization server (AS)
client app (C)
requesting party (RqP)
Sample high-level UMA flow; V1.0.1 spec references
OOB Choose resources to protect
OOB Configure policies (could happen after client attempts access)
RSR2 Register resource sets and scopes (ongoing)
UMA3.1.1 Attempt resource access with no token
UMA3.2.1 Register permission (resource set and scopes) sufficient for attempt
UMA3.2.2 Return permission ticket
UMA3.3.1 Return AS location and permission ticket
Assume any needed claims accompany initial request
UMA3.5.1 Request authz data with permission ticket
UMA3.5.2 Assess request
UMA3.5.3 Return RPT with success
UMA3.1.2 Attempt resource access with RPT
Assume default RPT profile and happy path
UMA3.4.2 Introspect RPT
UMA3.4.2 Return extended introspection object
UMA3.3.3 Assess access attempt against permissions
UMA3.3.3 Return resource representation

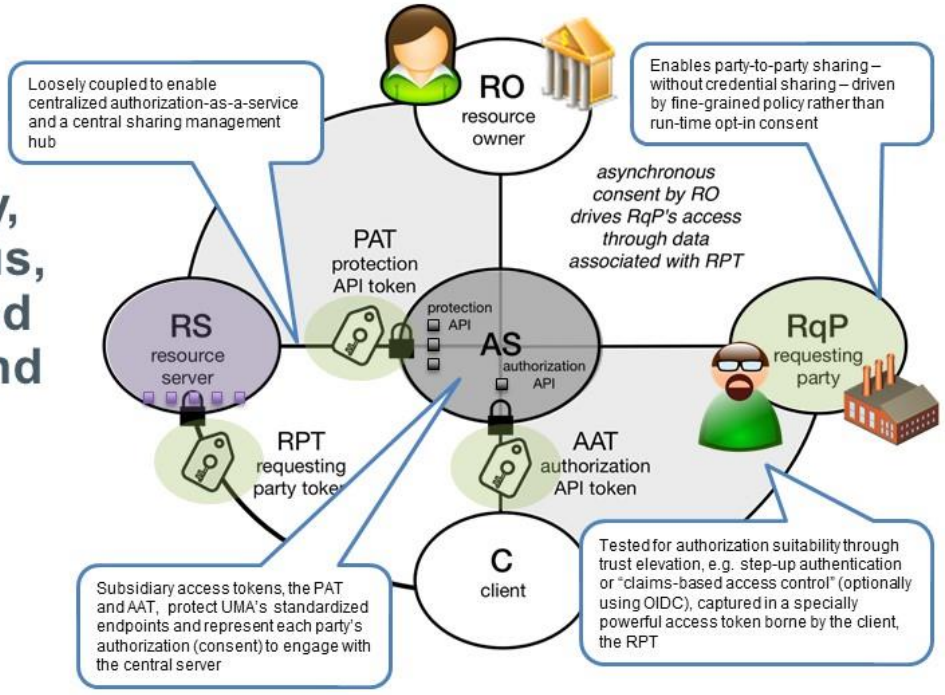

OAuth does "RESTful WS-Security," capturing user consent for app access and respecting its withdrawal
Authorizes (consents) at run time after authenticating
RO resource owner
Gets the consent based on the API "scopes" (permissions) it requested; is uniquely identified vs. the user
C client
API endpoints that deliver the data or other "value-add"
Standard OAuth endpoints that manage access token issuance
Both servers are run by the same organization; RO goes to AS in each ecosystem to revoke its token
RS resource server
AS authorization server
FORGEROCK

OpenID Connect turns single sign-on into an OAuth-protected identity API

SAML 2, OpenID 2	OAuth 2	OpenID Connect
☑ Initiating user's login session	✗ No sessions	☑ Initiating user's login session
✗ Collecting user consent: not responsible	☑ Collecting user consent	☑ Collecting user consent
☑ High-security identity tokens	✗ No identity tokens per se	☑ High-security identity tokens
✗ Distributed/aggregated claims	✗ No claims per se	☑ Distributed/aggregated claims
☑ Dynamic introduction *(OpenID only)*	☑ Dynamic introduction *(new)*	☑ Dynamic introduction
✗ Session timeout	✗ No sessions	☑ Session timeout *(draft)*

FORGEROCK

UMA adds party-to-party, asynchronous, scope-grained delegation and control to OAuth



FORGEROCK

Sovereign Identity Part Two: How it is Enabled by Blockchain Tech

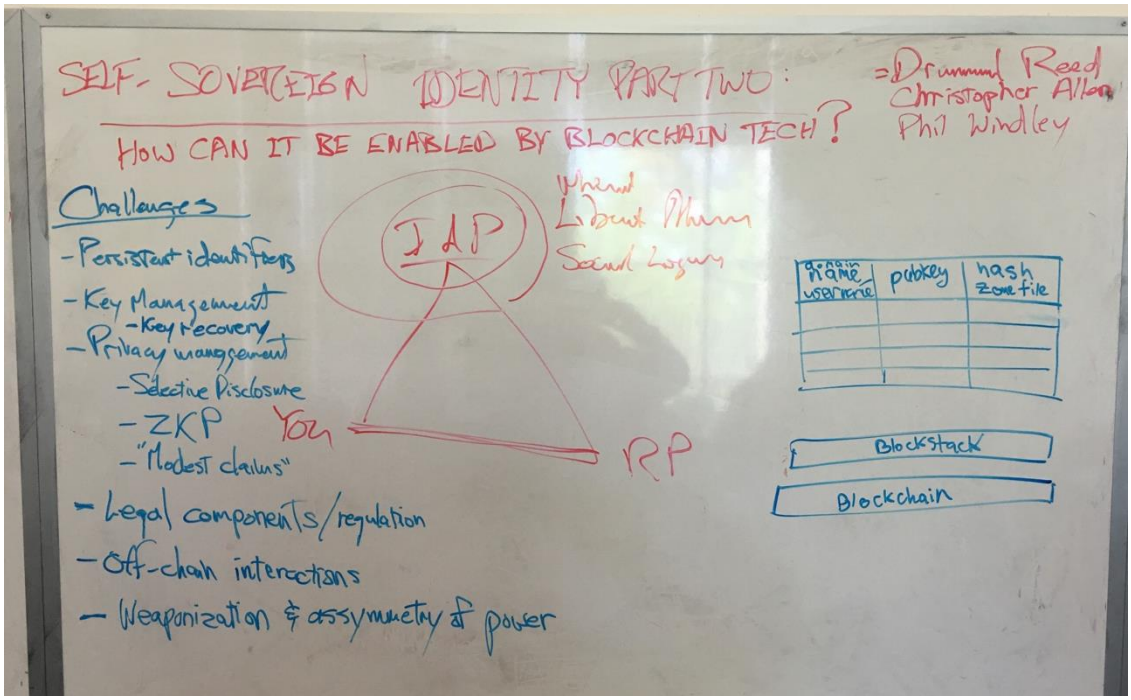
Wednesday 3A
Convener: Drummond Reed
Notes-taker(s): Drummond Reed

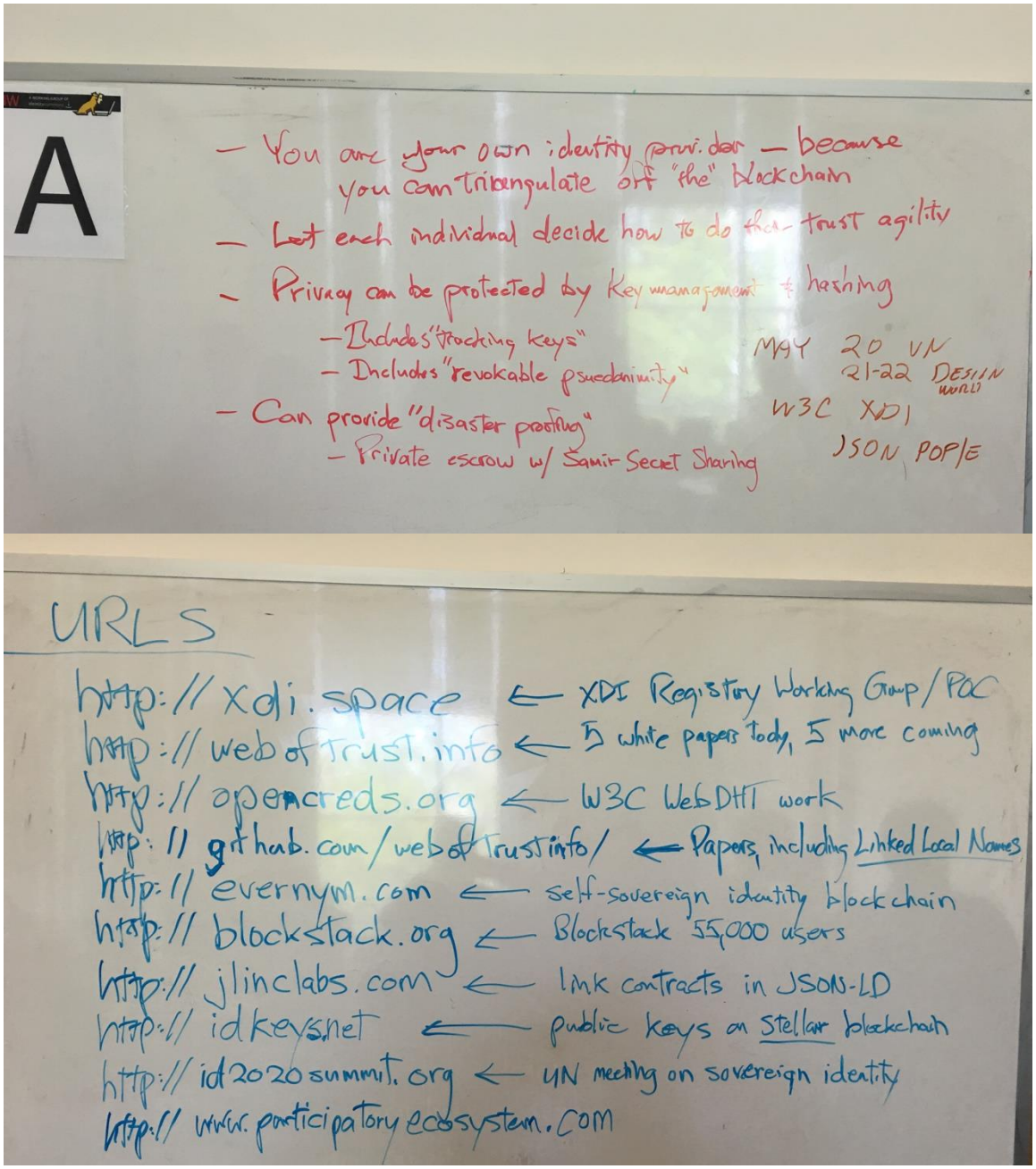
Tags for the session - technology discussed/ideas considered:

sovereign identity, digital identity, blockchain, policy

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

See pictures of 3 whiteboards below. Included 5 minute summaries of how 3 companies are approaching sovereign identity on the blockchain: Blockstack, Evernym, and JLinc Labs.




A
- You are your own identity provider — because you can triangulate off "the" blockchain
- Let each individual decide how to do their trust agility
- Privacy can be protected by key management & hashing
- Includes "tracking keys"
- Includes "revokable pseudonimity"
- Can provide "disaster proofing"
- Private escrow w/ Samir Secret Sharing
MAY 20 UN
21-22 DESIGN
W3C XDI
JSON POPLE
URLS
http://xdi.space ← XDI Registry Working Group / POC
http://webofTrust.info ← 5 white papers today, 5 more coming
http://opencreds.org ← W3C WebDHT work
http://github.com/webofTrustinfo/ ← Papers, including Linked Local Names
http://evernym.com ← self-sovereign identity blockchain
http://blockstack.org ← Blockstack 55,000 users
http://jlinclabs.com ← Ink contracts in JSON-LD
http://idkeys.net ← public keys on Stellar blockchain
http://id2020summit.org ← UN meeting on sovereign identity
http://www.participatoryecosystem.com

$1M: Does Your Project Stack Up?

Wednesday 3C
Convener: Colin Wallis
Notes-taker(s): Colin Wallis

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

R&D Funding for Identity and Privacy projects (a new and much less cumbersome channel than those currently in existence).

file:///C:/Users/colin/Downloads/Kantara-v3 template%20CCICADA%20IIW%20April%202016%20.pdf

Identity & Privacy: It's Canada's Game!

Wednesday 3D
Convener: Joni Brennan
Notes-taker(s): Joni Brennan & Mei Lin Fund

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

Founded 2012 ~ Made for Canada Trust Framework bringing people together to accelerate development of trusted identity serices solutions for use in Canada and globally

Identity critical for ecommerce and payments

DIACC – membership – Federal representatives and industry participants (Innovation Science and Economics), province of BC, Ontario, SME's

Fed, Provincial, private working together

Proof of concept pilots to solve real world challenges via commercially viable services

What problems need to be solved

Eg confirm age prior to alcohol purchase
Fill critical prescription online

Diacc principles

Workgroups and meetings

Pan Canadian Identity Trust Framework

Joni Brennan worked in US and international space

Wanted to stay away from many iterations of trust frameworks, different approaches – wanted 1 scalable model, public or private that allows for lots of innovation

US does not have a trusted attribute authority – US laws prohibit agencies from talking about identity information

Canada does have one and wants to be privacy respecting

There is a layer of trust in Canada – to assert attributes for digital identity

Allows Pan Canadian Trust initiative vs Kantara (US entity) / At gov level there is a clear distinction between Identity and credential in US
In US, there is a credential service provider category – its much more than 1 big idea

What is a trust framework?

A set of rules and tools that a community uses for its digital identity transactions to government – used to govern a particular community – rules for participating in a particular federation

Trust Framework Pillars

Standards and protocols and Business Legal Operational Policies (business, legal and technical processes)

Could be at a federation level, or national level, territorial or private sector

Challenge in the US – every state has its own way of doing caucuses – federation of 50 states with turnover with CIO, under federal umbrella

Canada has 10 provinces and 3 territories – Vision – citizens and businesses enjoy simple convenient and secure access to services in a manner they choose and manage

- Enable a whole of gov approach for seamless e-service delivery
- Improves client experience and user convenience by supporting a “tell us once” approach
- Enables jurisdictions to trust and leverage each other’s identity

Kantara initiative worked closely with GSA – had a trust framework for criteria for assessment – identity services, token manager services – worked hard to meet criteria set by NIST

Made contributions into ISO – so could not put in “check your state drivers license”

By having the trust framework specify how to create a solution – painted innovation into a corner

Found edge cases that didn't meet criteria – it's a big challenge to have flexible frameworks that allow innovation and prescriptive enough that you can verify trust

Do I need to check if 3rd parties have been verified? Eg checking weather is low risk to your reputation – no. If more risk to your reputation, need verification

Need service agreement to know if 3rd party is in breech.

What is right level that verifies trust and does not over burden

Identity cuts across everything – tent keeps expanding
Special snowflakes but at the end of the day, all water

Need to have a CORE and then profile off of that

Example – working for financial institution, PCI compliance, ISP 2700, KYC, outside money laundering….already doing all this – if financial institution has already jumped thru these barriers

How do you recognize trust – if we can trust that you have a valid compliance eg PCI, ISO 27000 – identify same ones specific to identity

These are the challenge spaces

US trust frameworks – enforcement becomes less clear – FTC enforces breeches of trust frameworks

FTC is regulatory, but trust framework (rules and tools) supports the policies.

Violations not clear who enforces

Multi party relationships – agree to same set of rules and tools – in the US – for gov agencies delivering citizen services – instead of one off contracts with each contractor – US recognizes a set of trust frameworks as ok – so provider of service contracts to comply

In Canada – these are eco systems with many parts and components – to have trust, governments have to trust certifying bodies to carry out certifying on behalf of governments

Primary mission of govs is delivery of service assistance – Trust Turtles all the way down – build up that trust so as not to re-invent each time

Anil John – US has transitive trust relationship with entity they certify – assess the assessor – its not true in other jurisdictions

Canada is evolving – does body have mutual governance, are they transparent?

Don't want each gov agency to do the identity proofing every other time
At a higher level of abstraction – started from the top – define objectives, what are the outcomes we are trying to get out of this trust eco system

Personal data is private Secure

Based on Kim Cameron's 7 IDentiy laws and a few more

1. Roles within an identity eco system
2. Objectives – what outcomes which each of the actors must meet

DIACC principles of a digital identity ecosystem for Canada

1. Robust secure scalable
2. Implement, protect and enhance privacy by design
3. Inclusive open and meets broad stakeholder needs
4. Transparent in governance and operation
5. Provide Canadians choice control and convenience
6. Built on open standards-based protocols
7. Interoperable with international standards
8. Cost effective and open to competitive market forces
9. Able to be independently assessed, audited and subject to enforcement
10. Minimize data transfer between authoritative sources and will not create new identity databases

Andrew Hughes – Registration for service

Someone signs up for service, organization and partners decide on the rules of what constitutes evidence of identity – how much they depend on drivers license

That's a profile

Framework says responsibilities are to verify against known sources and store reliably

Anil – US and Canadian difference – Canada said they are the authoritative source of information for their citizens

In the US, going to data brokers to assert identity

In Canada while not issuing credentials – will be vouched for by government –its regulated, vital stats dept, passport, citizenship collect – they don't tell others

Andrew - Canada has a authority – rules for access and modify are not providing access to other Canadian entities (even gov)

Anil – a Canadian citizen trying to get canadian services, it is a Gov entity that approves you. The agency program delivering the service does the proofing.

The Gov agency in the US doing this is using commercial services to do proofing

Andrew – in certain profiles, high assurance requirement – only gov service providers will be allowed to do the work. In more commercial usage, someone will do those services probably private sector

In future state – gov will have some assurances about what they do, because they subscribe to the framework

Getting a trust framework is difficult – herding cats

Canada 2 pillars

1. Modernization of Government Service Delivery (inside gov)
2. Full participation in the digital economy (outside Canadian gov – including global)

Changing government with Trudeau administration – PM writes mandate letters for which Ministers are accountable for

His thing is Open Govt – published all the ministerial letters – they call for central hubs to deliver gov services – leveraging Key Concierge to private sector

DIACC delivers Pan Canadian Trust Framework. Done 2 proofs of concept:

1. Remote opening of bank account
2. Proving provincial residency – user centric model to allow a citizen to leverage other records opt in – privacy by design up front – did you use your ATM card in the province

Looking for 3rd proof of concept

DIACC is doing research and offering commercially viable service that would benefit citizens

DRAFTing Pan Canadian Trust framework – will publish in June and people will adopt and test and get feedback to make sure provide value, meet the needs.

Cross border use cases

BC Gov – taken drivers license and Care Card are now on 1 card – Services Card – to allow it to be leveraged for multiple services. Each walled off in trusted module technology. Already deployed

Jbrennan@DIACC.ca www.www.DIACC.ca @mydiacc

There are rounds of public consultation – to get regular people to share concerns, diverse focus groups, lots of public outreach.

At start, were lots of concerns about privacy – people are supportive.

In British Colombia – CARE card is health insurance card- and they had 9 milliion cards for 4 million people – huge fraud issue.

Until 2012, cards didn't expire. Now will be 5 years.

Canada has strong privacy regulations – all outside businesses must meet Canadian regulations and must comply.

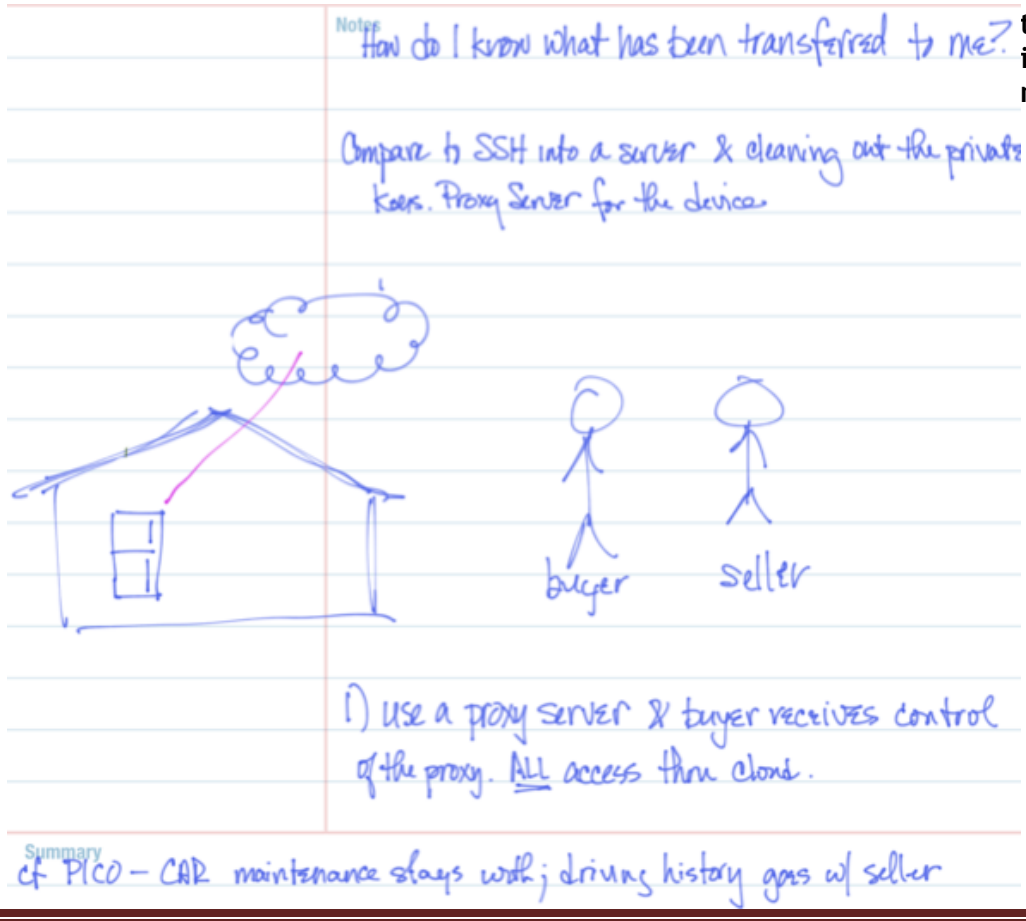
I Just Bought Your Smart House

Wednesday 3G
Convener: Alan Karp
Notes-taker(s): Judith Bush

Tags for the session - technology discussed/ideas considered:

IOT, internet of things, home automation, smart house, authorization transfer, authorization server, ownership transfer, escrow, PICO, concentrating component, wise elder of the network, proxy server, vendor cloud

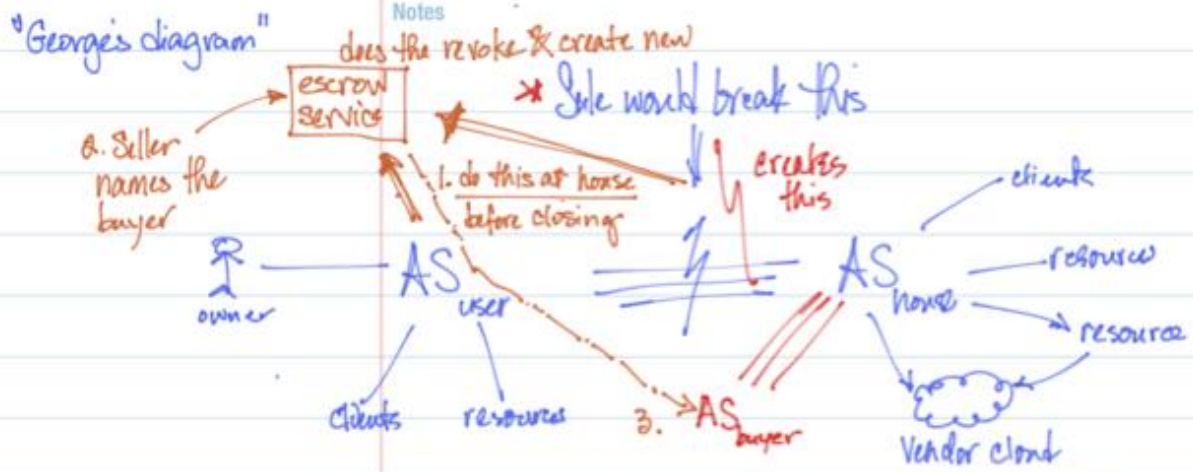
Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this action items and next steps:



Date: - -

Notes

"George's diagram"



STANDARDS

[use data]

- Vendor needs to separate personal data store from the object's [maintenance history]

ATTACK POINT

- Swap credential API No Transfer ownership send notice to AS

revokes previous keys
issues new keys
→ guarantee ixfer

+

- NOTE the sale is not in the house itself · How do

- Method to transfer:

Summary

- Pre exchange a public key, inspector verifies public key, buyer remakes sellers public key Rental car use case

"Concentrating component" the wise elder of the network

Side note: Public key promiscuity – Correlatability

Curriculum for Intro to Identity Management

Wednesday 3J
Convener: Kaliya Young @identitywoman
Notes-taker(s): Ken Meiser

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

Curriculum ideas:

50k view: problem statement and history How did we get here?

Why identify?

Risks that are assumed by the parties Sub communities:

Context and viewpoints from differing perspective

Roles Define Identity and it's various forms

Brands Entities People Organizations Government Groups

Standards Example: Oauth and FIDO

Identity management lifecycle Trust Identity proofing Privacy vs security

Identity types : anonymity, pseudononomy, true name Data rights

Auth vs verification Assurance and trust

Reading list: Phil's book The Live Web published by Course Technology in 2011 and Digital Identity published by O'Reilly Media in 2005.

Identity Events

Wednesday 4A
Convener: Phil Hunt
Notes-taker(s): Phil Hunt

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

Here is a link to Phil's slide deck:
https://github.com/independentid/Identity-Events/blob/master/IIW-IdEvents-Apr2016.pdf

OIDF – Enhanced Authentication Profile (EAP) Use Cases

Wednesday 4D
Convener: Annabelle Bachman & Mike Jones
Notes-taker(s): Paul Madsen

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

Mike Jones described the value proposition

Good things coming out of IETF - Token Binding specifies how applications can bind tokens to particular TLS sessions. Can prevent cookie/token replay - mitigate risk of bearer tokens

Dirk Balfanz @ Google implemented an earlier version of this for Chrome

The first deliverables for EAP is to write a description for how to do token binding for an OIDC id_token, to prevent an id_token from being represented

basic idea is you put a reference to the public key of the TLS into the id_token so that the Client can confirm the token is being presented over the right TLS channel

a second deliverable of the EAP is to allow an

a) the OIDC RP to signal to the OP that it desires 'phishing resistant authentication'
b) the OP to signal that it did indeed do so, and some level of detail

The WG will need to specify how the RP can best direct the OP

Dick asked whether the OP being able to prove that it actually performed a specific authentication was in scope. Mike said 'perhaps'.

Dick told the minute taker to 'fuck off'

Justin drew out the OIDC triangle, asking to which channel the id_token is bound. Brian responded that it is bound to the channel between the UserAgent & the Client - regardless of whether the id_token is presented over that channel (or not)

Justin asked for clarification on the scope of the authentication - is in scope where the OIDC RP might be doing its own strong authn, in addition to accepting the id_token?

Mike responded that his assumption was that the OIDC OP would be doing the strong authn.

Annabelle pointed out that the other mechanisms exist as an alternative to Token Binding with the same security characteristic of mitigating token theft, ie PoP etc. John referred to the HTTP Signing spec, a different Proof of Possession Mechanism. Lots of grumbling about OAuth 1 and MAC spec.

Dick asked whether these two deliverables were independent and whether there could be value in combining them - ie the FIDO keys could be used in the token binding of the id_token.

John said the WG would be looking at that.

Mike explained how the Token Binding worked for federation, specifically that the OP can mint a token that is bound to a TLS channel that the OP doesn't participate in

Dick posed question "what do we mean by 'strong' authentication?" or what do we mean by 'phishing resistant'? etc etc

Consensus seemed to be that we should talk in terms of the resultant security characteristics, rather than LOA or specific mechanisms

People's Digital Identity Life Cycle

Wednesday 4E
Convener: Bill Aal
Notes-taker(s): Tom Leon

Tags for the session - technology discussed/ideas considered:

Identity Needs in a Person's Life Cycle

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

Identity Needs in a Person's Life Cycle
What is the framework for thinking about a person's lifecycle in the digital identity space
Round-table Questions:
The concept of a lifecycle intrigued participant 1. Are their risks.
Participant: How does it link to an offline identity. Do you have one ubiquitous identity
P3: Meatspace – how does a person have complete control over your own lifecycle
P4: A cradle to career database is being created for users. How do health records follow us. Longitudinal
P5: Book. Digital Immortality. There is a longitudinal aspect that transcends death. Identity and Persona and Reputation
EVENT: Door shattered. (not) Fun, but made for Exciting presentation!
P6: All of the events that are asserted throughout a life and makes the identity. Control and different between a record and conclusions that are drawn.
P7: Ability to carve up events into relevant subjects. You don't want to have the same view along the lifecycle. What passes along after death. There isn't a universal answer.
In Healthcare, you can have different diagnosis from different doctors; how does that persist.
P8: Thinks about life. We think a lot about Data, but we need to think about how we handle treat. Governments have perpetual life as sovereign entities. As an individual, we need to be able to reach though space and time – super human – through our data. Life = autocatalytic self perpetuating organisms. Value embodiment is moving to data where our physical being is a vessel. A user lives on in memory AND IRS legislation.
Yiddish has survived because it has been digitized. Languages fail and fade away.
Bill: Difference between identities and identifiers. Identifiers are given by the State, by and Institution, etc. Our lives, however, are not these identifiers.
We need to be able to subdivide our global identity.

PAPER: Identity and identifiers – how are we recognized as a person. What is the context in which issues come up.
: PreBirth – Prenatal Screening, Birth announcements, doctors visits
: Birth: Naming, National Identity, Christening/Bris, Community Recognition/etc. Health
: Adoption:
: School:
: …
There is both an internal and external views of an individuals.
Perhaps there is a gradient of relationships. Concentrations of relationships. There is a developmental piece.
Internal is dependent upon an individual's memory.
Bill – Moving and threw away his college papers; this was a big part of his personal identity.
In school, you change persona every year. Is there a time where you should have the opportunity to revoke your identity? At age 18, should you be able to expunge your records?
Oregon has a 75 year retention policy about your education records. You could have an avatar of yourself created based on faulty or outdated data.
There are rocks everywhere and can be used to hurt someone, but we don't get rid of rocks; instead we tell people to not hit each other with data. Should we have a similar view of data – that data's existence isn't the problem, but people shouldn't use data for nefarious purposes.
If you design systems around bad actors, you are destined to fail.
? Is the data accurately portraying the REAL user? A person can change.
What are the life events that happen, and how are they used?
Commons and co-management/ownership of data? Is there a MINE for data?
Life events:
Gaming
Sports
Arts
Events/Proms
Driver's License

Is HIPAA violation if someone is recorded at a hospital by someone else? Life in the ER where someone in the background was captured.
Publication of Private Affair is a Tort – do you need HIPAA to adjudicate this?
HIPAA is different than Privacy. There is no gradient in HIPAA. How does this affect defamation?
As there are gradients of intrusion, are there gradients of permissions?
There are trust relationships. Dr/Patient privilege that cannot be compelled to disclose for a court.
There are ethical codes that say a doctor shouldn't disclose otherwise.
There is not a data institutional protection.
There needs to be a service layer.
How do we construct an identity with our life events. How do we use the online world to move through life.
Identity is linked to autonomy and decision making over time. We need tools.
Community identity is important; people have their own world views. There are rights and responsibilities with this from a data perspective as it crafts a person's identity.
What uses to people put their identity to?
Persona is a part of an identity. There is a totality of ME via data, but there are slices that are shared or given.
Concern about what you have shared voluntarily that is then used elsewhere?
There is a social construction of our identity. There is HOW we show up in places online.
How do I show up online and in person with different personas at different points in time.
There is a tension between identity from a personal AND state issued identity.

There is a research framework that is being worked: what would be a good way to connect on an ontological level.
Time/Space are relevant in the matrix. There are vectors of change. Difference between data and information. Data+Meaning=Information
You don't mind for your banking to get some data, but that same data is bad if gotten by a hacker.
Social interaction involved expression and perception. If you can firm this up, you can provide metrics that allow people to have a framework. Measure expectation against performance in a channel.
Information is a novel construct. Is there a measurement of novelty that can be marketed.
Folks who are work for large companies, are there these conversations in the worlds that we inhabit?
Should I only be allowed to have a single identity? How much control should I have over what is released and what is private. At what point is something MINE, versus part of the community?
Add Military Service as a life event. When you are in and out of the military, what do you have access to? Think special Ops military and the information that needs to be extended to their extended family.

CHEDDAR: Implementation

Wednesday 4F
Convener: Doc Searls
Notes-taker(s): Kevin Marks

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

Doc Searls: what is called advertising these days is actually Direct Marketing, which has always been annoying. ~ the whole adtech industry is falling apart. I know one $100M adtech company that says it is a zombie ~ while advertisers are putting ads in front of you that take 300ms to appear, they pay the adtech in 120 days

The reason you see toe fungus ads everywhere is because of tracking you across sites ~ there used to be a few name brand agencies, now there are thousands of adtech companies, and publishers don't control them ~ there's a phrase in the Big Short " wherever you have a mania and fraud, there is a bubble" Adtech has both

Don Marti wrote about the toe fungus ad problem here:
http://blog.aloodo.org/posts/service-journalism/

CHEDDAR is a list of rules for making acceptable ads: http://blog.aloodo.org/posts/new-acronym/

CNAMEs: Ads, and other third-party resources such as analytics scripts, served from a subdomain of the publisher's domain

HTML5: avoid the malvertising risks of vintage plugins by using web standards only.

Encryption: Limit the ability of ISPs and other observers to gather user data that can be used for targeting later.

Data leakage protection: Many users are still unprotected from web tracking - notify them and offer incentives

Do Not Track: use the EFF DNT policy on your site https://www.eff.org/dnt-policy

Accountability: accurate WHOIS info for everything in the adtech chain. No anonymous registrations.

Reciprocity: an offer of signal from the advertiser for attention from the audience.

Phil Windley: how does a site assert that it supports CHEDDAR, and how do you check?
Doc Searls: building an implementation guide is the next goal here

Trust Frameworks Explained

Wednesday 4G
Convener: Andrew Hughes
Notes-taker(s): slide deck Andrew Hughes

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

The deck is "Trust Frameworks Explained in 20 minutes or less"
http://www.slideshare.net/AndrewHughes6/kantara-trust-frameworks-2016-0508

Privacy: Confusion of Identities

Wednesday 4I
Convener: Akika Orita
Notes-taker(s): Akika ORITA & Kazue SAKO

Tags for the session - technology discussed/ideas considered:

privacy, identities, real name, after death

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

- Two topics are introduced. The first one is marriage and surname choice case in Japan as an example of identities and privacy issue. Name change reflects one's personal life regardless of one's intention such as marriage or divorce. The second one is victims' Facebook on TV news as an example of treatment of deceased's social media. Even if there are "public" timelines, it might not be considered really public ones, but communication with their friends.

- Regards to the former topic, we were talking about marriage and surname system in the US and Japan, working name and stage name as an alias of legal name, how to change our legal name in the real life and some example of name changes.

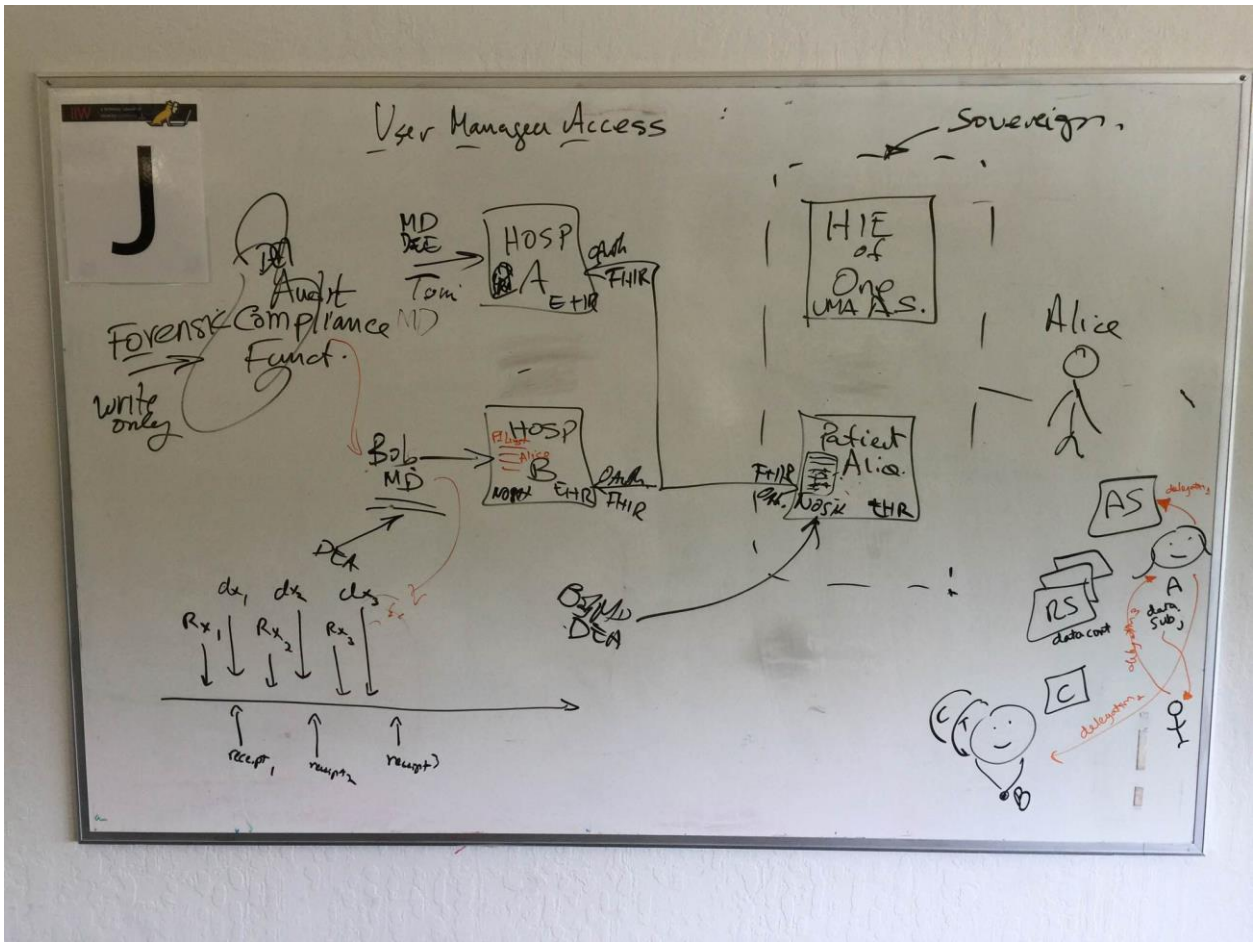
- Regards to the latter topic, we were talking about deceased's account treatment on Twitter and Facebook. Once their social media contents There is also an aspect that to keep one's account alive even after death is archiving.

UMA + JLINC

Wednesday 4J
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:

How the blockchain might add an auditable compliance service to a sovereign personal UMA Authorizatiion server and a personal resource server. The UMA trust elevation protocol may be the right place to integrate this.



Common Ontology for Personal Data Interoperability, Part 2

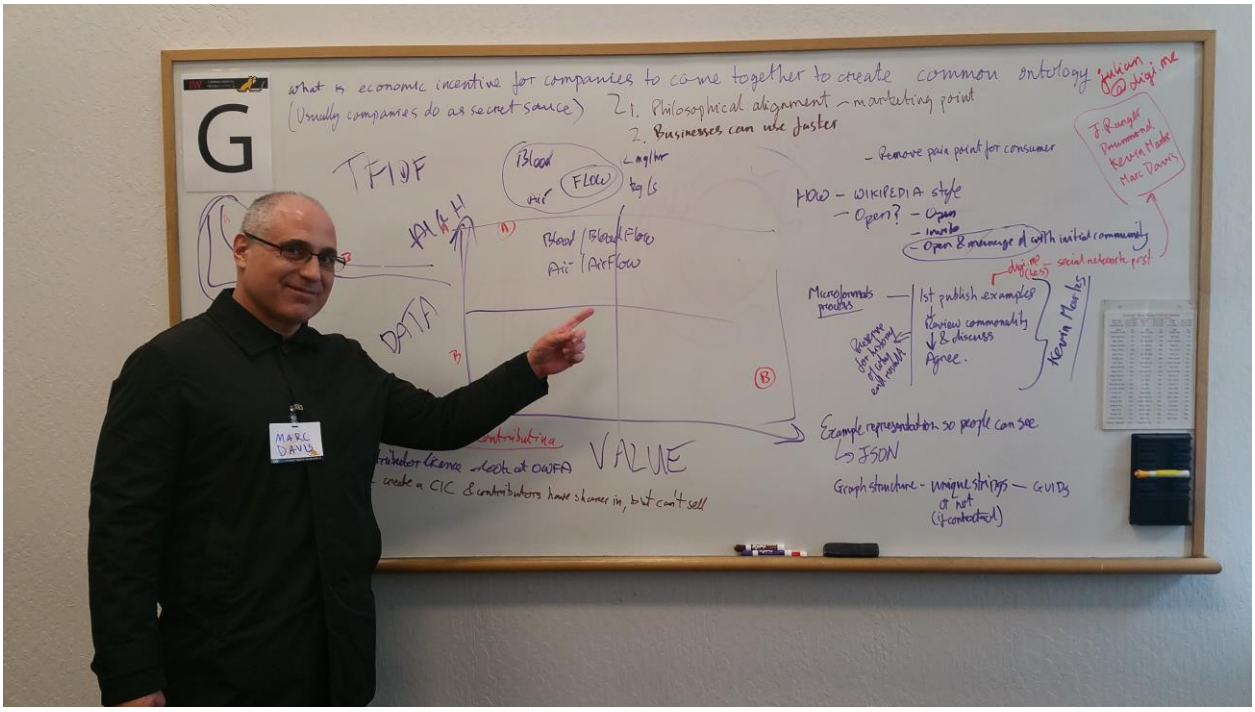
Wednesday 5G
Convener: Julian Ranger
Notes-taker(s): Julian Ranger

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

Day 2

1. In Part 1 of this session the previous day it was agreed should have a further Part 2 session at this IIW to explore what it would take to create a single ontology (or minimum set) - the What & How. Points to note:
    a. Look at use cases and solve for those first
    b. Look at other ontology standardization examples and why they failed or succeeded
    c. Discuss "Data to Value" maps
2. The first question was what is the economic model for companies to come together to create a common ontology? (Usually companies do as secret sauce.) Two answers
    a. Philosophical alignment - marketing point
    b. Businesses use data faster with less work <- the main point
3. Talking about data elements only for the ontology - fields and values.
4. Marc Davis introduced the concept of Data to Value map to work out which areas should be worked on first for a common ontology
    a. Data fields follow a power law, i.e. some fields are used a lot, and most others used very little
    b. If you then map in a classic 2 by 2 matrix with Y axis being data frequency across ontologies to be normalized, and X axis being value of data element to the business on Y axis, you can plot where each data element / element sits. Clearly those in top right quadrant (high data frequency & high value) are the ones to normalize to a common ontology first.
5. Question of what are the first steps on the path of getting to the 'Golden Goal' of a single normalized ontology (or minimum set)?
    a. Create a small manageable group in first instance to start the process of creating an open ontology
    b. Wikipedia style site to manage process
    c. Suggested follow Microformats process
        a. 1st publish examples of normalized data with traceability
        b. Review commonality & discuss
        c. Agree version to go forward
            i. (Note: keep a & b for history of why have end result)
    d. Agreed will include an example representation to show usage - will use JSON
    e. Probable graph structure - unique strings (though discussed option of non unique if contextual) - may map to GUIDs (though discussion on whether necessary at this level)
6. Agreed that following group of 4 would create strawman of 5 above, based on an initial example of a normalized social media post to be provided by digi.me, with others to contribute if interested (contact group via julian@digi.me):
    a. Julian Ranger
    b. Drummond Reed
    c. Kevin Marks
    d. Marc Davis

7. Final discussion on economic model for contribution:
    a. Open, with contributor licence - look at OWFA as an example
    b. Or could create a CIC (can't then sell), but contributors have shares if any value accrues



Identity for the next 1.5 Billion

Wednesday 5I
Convener: Mei Lin Fung
Notes-taker(s): Jason Wong

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

Spirited and positive discussion. A big deal – it's happening. Empowering individuals thru access to the Internet will equalize individuals with knowledge. There are
multiple models – stakeholders, governments, financing organizations – identity will play a role in some and not in others.

Doc Searls

Observation – there are 50 Identity shops here at IIW. The space is evolving. How identity plays with Internet Access is going to be interesting.

Question - How will this last past the current political administration?

MLF: IEEE-World Bank have committed to 10 meetings over the next five years on the sidelines of the IMF/World Bank Spring and Fall Meetings, to track getting 1.5 Billion on line so that an investment in the Internet is an investment in People. Civil servants are working with us to assure continuity through election period. I got to know most of them through 2009-2013 when I worked on the Federal Health Futures initiative under the US DoD UnderSecretary (Health Affairs)

Doc - Mei Lin is working on this with serious players like Vint Cerf, looks like it has an actual chance of succeeding.

Participants (these signed in)

Jason Wong	jdwongmd@gmail.com
Bryan Pon, Caribou Digital	bryan@cariboudigital.net
Timothy Ruff, Evernym	timothy@evernym.com
Maria Vachino, JHU/APL	Maria.Vachino@jhuapl.edu
Bill Jesswein	bjesswein@me.com
George Sammau, Meeco.me	George.sammau@gmail.com
Joyce and Doc Searls	joyce@searls.com doc@searls.com
Kailya	kaliya@mac.com
Peter Simpson IRespond.org	peter@irespond.org
Gary Zimmerman Respect Network	garyz@respect.network
Scott Shelton	Scottshelton314@gmail.com
Jason Law (not present, wants notes)	Jason@evernym.com
Jeffrey Schwartz (not present, wants notes)	flack@flackhacker.com
Drummond Reed(not present, wants notes)	drummond@respect.network

MLF shared People Centered Internet Principles – developed in October at Stanford with the World Bank co-author of the World Bank Develpoment Report (WDR 2016) on Digital Dividends with participation by representatives from Kenya, South Africa, Brazil, Colombia, Singapore, India, Costa Rica and local SV community. Principles were taken by Vint Cerf and Manu Bhardwaj of the State Dept to the Internet Governance Forum and these spurred more ideas, published by IGF.

At meetings organized by State Dept under the www.share.america.gov/globalconnect initiative, an agreement was announced to follow through on connecting the next 1.5 Billion by having 10 meetings convened by the IEEE and the World Bank. The first was held April 13 and attracted an over flow crowd of 160 +. IEEE has 425,000 members in 160 countries, their mission is Advancing Humanity and they have a volunteer organization IEEE Sight and members who can be involved in bringing the Internet to the next 1.5 Billion.

The People Centered Internet has been tapped by the State Dept and the White House Office of Science and Technology Policy to work with IEEE and the World Bank to move the initiative forward. There is broad support for the principles of PCI – and in this session, we did a rough poll of the people in the session to see what they were supportive of – in order to get a sense of where the audience was in terms of interest. (poll done early before rest of participants joined)

1. Complete universal Internet coverage that enables functionality that is otherwise unreachable or ineffective	5 votes
2. The Internet is affordable, open, available and accessible to all	3.5 votes
3. Fosters digital literacy, local content in local language to achieve widespread usage and increased value to people, families, communities and countries	4 votes

4. The system achieves a level of trust that meets the users' expectations of affordability, privacy, safety	5 votes
5. The quantity and quality of educational and information services is increasingly available to families and communities	4 votes
6. Anyone can contribute to improvement of the utility of the global Internet.	3 votes
7. Personal information in the digital environment is protected by law and controlled by the individual	6 votes

Ideas proposed by Mei Lin – Use the IMF/World Bank Forum and with the technical expertise of the World Bank and others, to drive new people centered measures to assure desired outcomes are achieved. The Principles above used to determine which projects People Centered Internet will get involved with and drive to get funded. ie People Centered internet acts as a broker to connect "good for people" projects to funding that is supposed to be "good for people". This works alongside complementing and diverting existing funding (aid and investment) streams, with the support and encouragement: US government Roadmap and engagement of global players. Global Players commitments to immediately direct up to $20billion for this initiative, the US agencies who will be involved in directing lending and aid

Use the global initiative which will involve $450 billion in spending from now to 2020, to require capital investment in the Internet to use the Internet as a measurement instrument to demonstrate that lives are being improved.

People Centered Internet

Approach 1: Evidence based, data driven feedback and act to improve human lives
Approach 2: Project human outcomes (at population level and individual): Track to see if achieved, adjust and Iterate

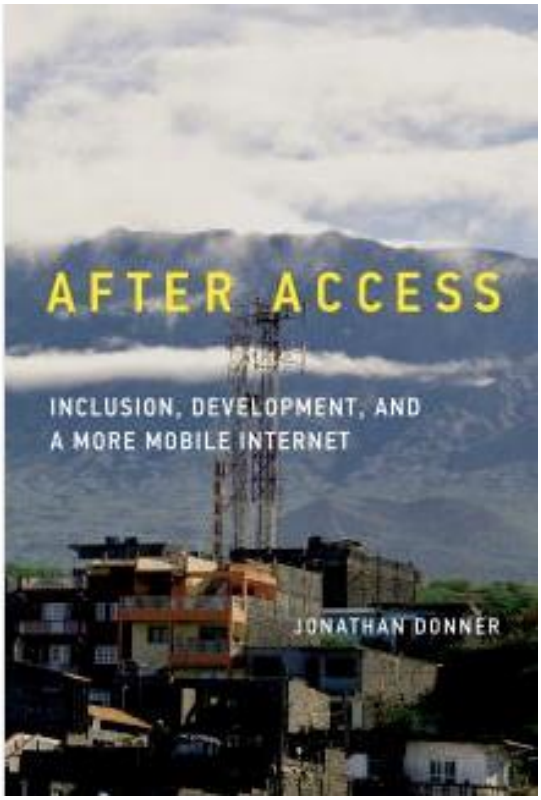
Issues raised

A. We are doubling down on technology –problems already – need socio/anthro arts and sciences not just tech
    a. Nigeria has 12 identity schemes, none of which have more than 25% coverage- Bryan Pon Caribou Digital
    b. India digital ID has 1 billion identities but not connected to legal credentials - Kaliya
    c. China – Social Credit Score by 2020 – Mei Lin
B. You can have Identity without the Internet – Timothy Ruff – Evernym
    a. Smart Card
    b. SMS
    c. MPesa
C. UN Sustainable Development Goals 16.9 require identity – too Constrained – George Sammau
    a. drown by bureaucratic rules – aim for pre set objectives – no room for course correction – eg World Bank and UN
    b. Global Connect is an end-run around existing development organizations, matching countries directly with funders (Multilateral banks and private financing) = real competition for World Bank, IMF, WHO to show results in improving people lives

Types of Identity that we discussed

- Legal
- Not Legal
- Squishy – evolving and changing, and different depending on who you are or when you ask them
- Bio metric ID – iRespond.org has a biometric default identity being used by global public health to track health records for immigrants in border situations – photo of eyes and you are identified.
- Province of British Colombia has a great system, combining drivers license with health care cards.
- Wifi Squares in Cuba are providing crowd access

Recommended Reading "After Access" by Jonathan Donner - MIT Press

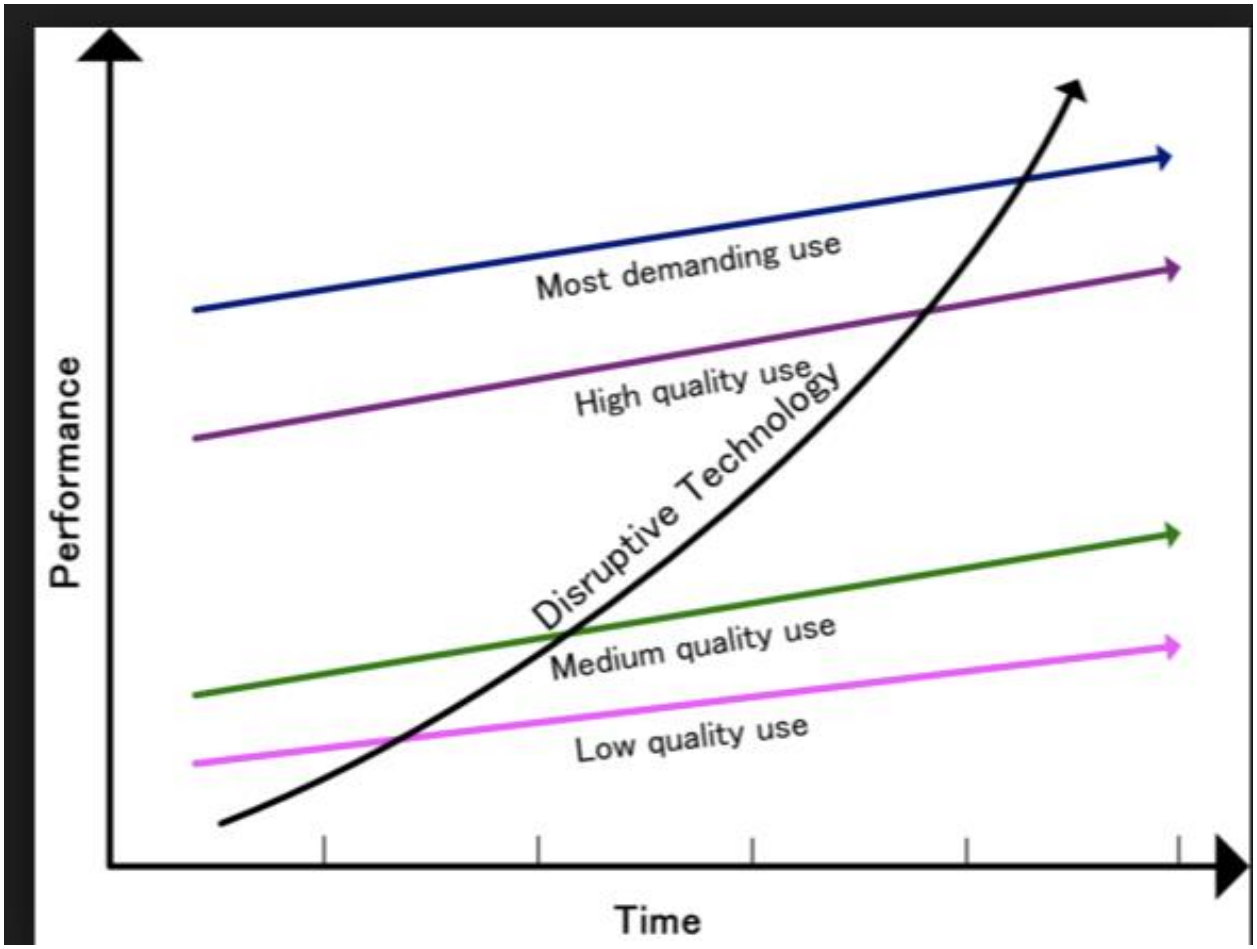


Almost anyone with a $40 mobile phone and a nearby cell tower can get online with an ease unimaginable just twenty years ago. An optimistic narrative has proclaimed the mobile phone as the device that will finally close the digital divide. Yet access and effective use are not the same thing, and the digital world does not run on mobile handsets alone. In After Access, Jonathan Donner examines the implications of the shift to a more mobile, more available Internet for the global South, particularly as it relates to efforts to promote socioeconomic development and broad-based inclusion in the global information society.

Drawing on his own research in South Africa and India, as well as the burgeoning literature from the ICT4D (Internet and Communication Technologies for Development) and mobile communication communities, Donner introduces the "After Access Lens," a conceptual framework for understanding effective use of the Internet by those whose "digital repertoires" contain exclusively mobile devices. Donner argues that both the potentialities and constraints of the shift to a more mobile Internet are important considerations for scholars and practitioners interested in Internet use in the global South.

Bottom Line:

We have an opportunity to Disrupt Identity by working with the "pre-enfranchised" the 3 out of 5 people who are not yet connected to the Internet



Credit - https://en.wikipedia.org/wiki/Disruptive_innovation

Contact Mei Lin Fung mlf@alum.mit.edu if you have a project in a country whose finance minister is willing to propose it. Currently many countries are up to their debt limits set by the IMF – it is possible that Internet projects under Global Connect could warrant special consideration.

Final note – Action Taken!

Pete of iRespond and Mei Lin will work on a project in Myanmar and go after funding under Global Connect for health access and treatment for border immigrants.

UMA Legal

Wednesday 5K
Convener: Eve Maler
Notes-taker(s): Eve Maler

Tags for the session - technology discussed/ideas considered:

UMA, law, contract, agreement, trust framework, DIACC, consent

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

In the session, we discussed the "BLT sandwich" of UMA (business - legal - technical) and how the technical elements may be relatively simple but the other elements may be complex. The UMA Work Group at the Kantara Initiative has a Legal subgroup that is currently working on developing "model text" -- boilerplate term definitions and legal clauses -- to support the creation of contracts, agreements, "access federation" trust frameworks, and consent receipts related to the deployment of UMA-enabled services.
One area where the technical world of UMA might be simple and the legal world might be more complex is in the area of people (individuals or legal persons) acting on behalf of others. For example, a mother might act as the guardian for very young son in granting access to his health records; she is not the subject of the records, but she is the UMA "resource owner" nonetheless. See the attached slides for a view onto these use cases and solution design patterns.

See these links for more information:

- http://tinyurl.com/umawg (where you can find a Join link and information about the IPR policy of the group)
- http://tinyurl.com/umalegal

Thursday April 28

Sovereign Identity Part 3: What are the Challenges?

Thursday 1F
Convener: Drummond Reed
Notes-taker(s): Drummond Reed

Tags for the session - technology discussed/ideas considered:

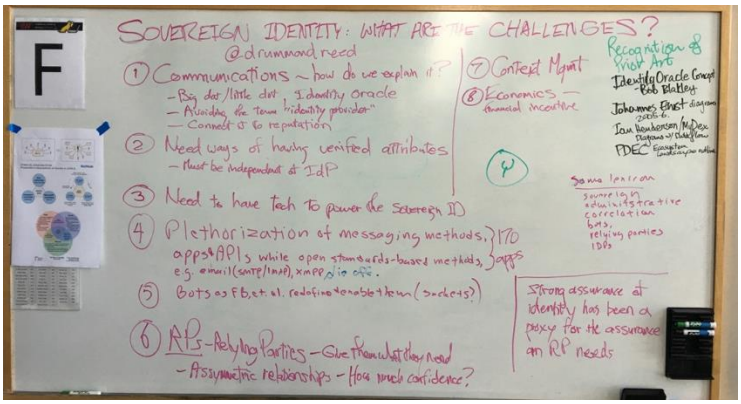
sovereign identity, digital identity, user-centric identity, blockchain, policy, challenges, adoption

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

The session was part 3 to the "What is Sovereign Identity?" session from Tuesday and "Sovereign Identity Part 2: How is it Enabled by Blockchain Technologies?"
The first part of the session focused on the history of user-centric identity as discussed and developed at IIW over the past 12 years and how many of them are every bit as relevant to "sovereign identity" as they have been to user-centric identity.
We then began discussing the challenges to sovereign identity, listing them on the whiteboard shown below. A summary version:

1. How do we communicate about sovereign identity, i.e., educate the audience of individuals and relying parties?
2. How do individuals obtain verified attributes for sovereign identities?
3. How do individuals obtain the technology they need to assert and control a sovereign identity?
4. How do individuals and relying parties deal with the plethora of messaging technologies today (170+ OTT (Over The Top) messaging apps)?
5. How should sovereign identities interact with bots?
6. How do we recruit relying parties (RPs)?

The final point about relying parties received the most discussion. The key point was that relying parties need to be able to get the data or credentials they require at the level of assurance they require—and that this will not be easy. What's necessary is to have enough incentive for all parties.
At the end, Drummond polled the group to ask, "How many believe that the emergence of blockchain technology is a breakthrough for sovereign identity?" Over 90% of the room agreed. Only 2 attendees were skeptical of that conclusion.



Identity in Ten Hundred Words

Thursday 2C
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:

We tried to explain identity concepts using only the thousand most common words. Here are some of the definitions we came up with:

Identity - A set of facts about a thing that make it what it is

Trust - A reason to think that a person or a computer will keep promises and tell the truth

Authorization - allowing a person or a thing to do something

Identity proofing - Making sure that a person's on-line facts match their real-life facts

Authentication - Making sure that a person is the same person you saw last time (which is different from them being who they say they are!)

Password - Something known only by the the person who is supposed to know it that can be used to show that they are who they say they are.

Attributes - facts about a thing or a person

Assertion - a fact that is said by a thing you trust

Single Sign-On - sign into one place and get into other places I'm allowed to go to

Roles - names for things that a person does

Credentialing - giving people a name and a key for a situation

System of record - if two facts don't agree, this computer is right

Assurance - how much I believe something that was said to be a fact

Privacy - being able to say who can know what about me

Standard - an agreed-upon way of doing something

Reputation - what other people are saying about me

Things we want to define in the future:

- security
- security theater
- federation
- breach
- identity theft
- risk

Sovereign Identity on Your Cell Phone With Yoti

Thursday 2F
Conveners: Bruce Nash, David Goate, Simon West
Note-taker: Simon West

Tags for the session - technology discussed/ideas considered:

Bruce Nash, David Goate and Simon West ran a demo of Yoti and called a Q&A for feedback from the IIW community on how it feels about the solution being offered, and what Yoti may be able to do going forward. **URL:** www.yoti.com

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

Features demonstrated:

- Registering for a Yoti using a cell phone.
- Using Yoti for facial biometric Single Sign On into a website.
- Peer to peer sharing of age range, but choosing to conceal your real age.

Calls for consideration:

- Could Yoti explore using other forms of API protocol in addition to the SDKs provided? e.g. OpenID Connect.
- Being able to make an assertion about yourself that isn't necessarily verified by a trust anchor. e.g. from an email address to a complete persona.
- Can you attest to where profile information was verified from (e.g. Passports, Drivers Licenses), and how could that level of confidence be communicated to a relying party? Is there a challenge around discrimination over this? e.g. a relying party questioning the strength of a verified attribute if it originated from/ was verified by a particular government issued ID.
- One of the principles of a self-sovereign identity is your ability to move that identity between providers freely. How could Yoti allow that?
- While each individual's data/identity is centralised and concealed from Yoti's view (Yoti cannot use the data held; the private key for the data is stored on the individual's device), could someone transfer their identity to another without making a call to Yoti; i.e. offline or directly, peer-to-peer.
- Would like to know more about how to allow further devices to use your Yoti, and how to revoke one or more of those devices.
- Could individuals store information on an optional mechanism such as a blockchain, rather than forcing them to trust Yoti to store the data?

Observations:

- It's like a "replacement for captcha!"
- Yoti doesn't appear to be truly: zero-knowledge, verifiable by others, open-standard and open-source. It's essentially a closed authority. How might that change in the future? At the moment the Yoti Guardian council is responsible for holding Yoti to account for being responsible to its users, and transparent.

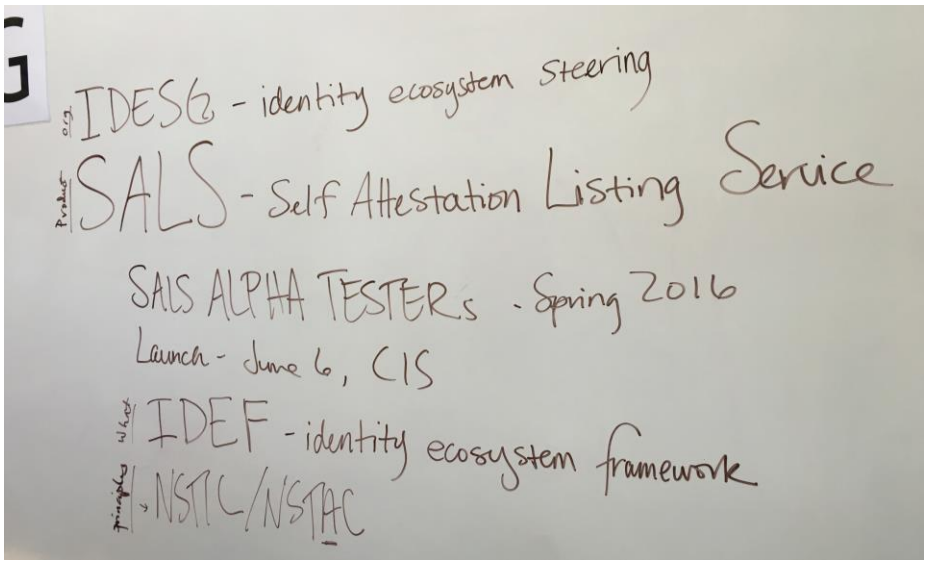
- Being able to share minimal information with someone to get a job done, like only sharing the fact that you have been verified to be over legal age (but not your age itself), is really valuable. It's a great example of being able to exert some control over your relationship with a vendor (see VRM), while meeting the relying party's legal obligations.
- "Yoti isn't really a Sovereign Identity provider because it forces people to verify their identity against a government-issued ID." While this isn't strictly true (you can just register with a selfie), Yoti is a system that people could potentially choose to use as a Sovereign Identity system, although there may be times when they're unable to do so (e.g. when required to present information partly attested for by a government recognised ID - as laws dictate).

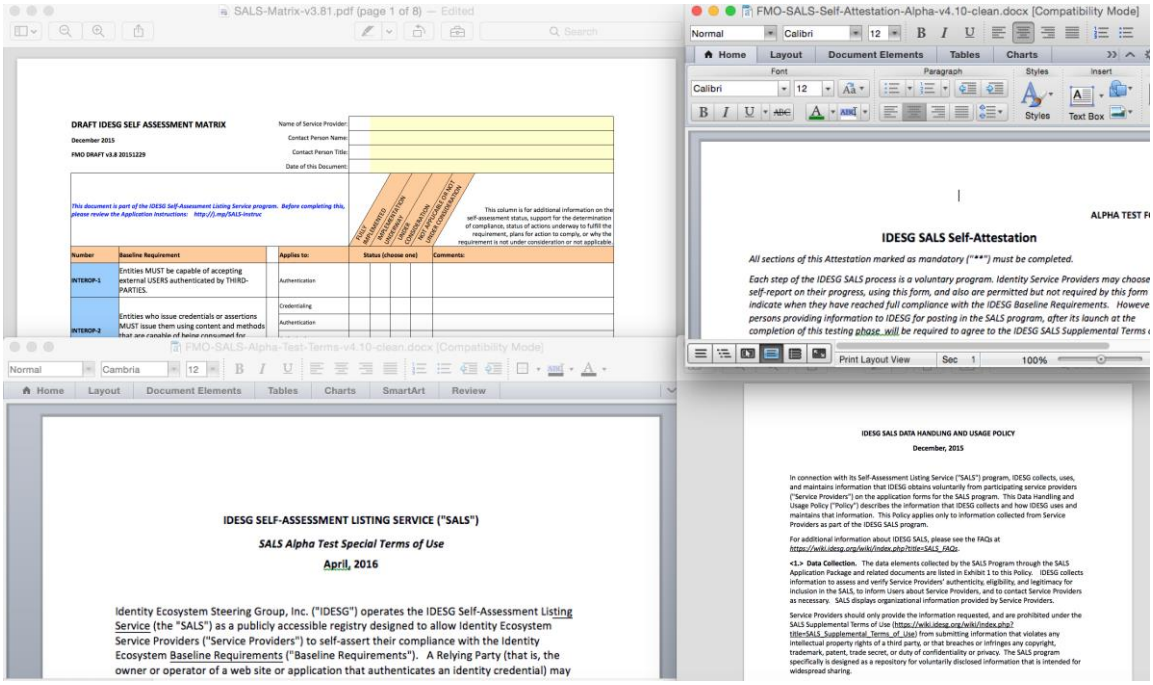
SALS - Self Attestation Listening Service / Launching Soon

Thursday 2G
Convener: Mary Hodder
Notes-taker(s): Mary Hodder

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

We have two screen shots. It was a general discussion with about 20 people, half in IDESG, half interested in the SALS: Self Assessment Listing Service launching June 6.





VRM – Fixing Marketing and Service with Intent-Casting and Personal APIs

Thursday 3A
Convener: Doc Searls, Scott Shelton
Notes-taker(s): Scott Shelton

Tags for the session - technology discussed/ideas considered:

VRM, CRM, Marketing, Intention Economy, Intent-casting, Personal APIs

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

Demonstrated a POC of how a sample VRM conversation might flow between marketers, consumers, and businesses.
Can we give marketers a new channel for communicating and engaging with customers that solves problems they can't solve now and yet respects the customer's privacy, security, and data?
How is a crowdsourced Intention Engine different from Google?

- It can solve problems that Google can't, such as connecting supply and demand for service or product needs.
- There is "money left on the table" (MLOTT) whenever a person can't get what they want or has a problem. Whether a first, second, or third party can fulfill that need, we are missing a channel for everyone to recognize the missed opportunities and a vehicle for solving them.
- Google, Siri, Cortana, Alexa, and others can automate a lot of answers by parsing natural language, but they cannot typically answer questions about supply and demand or give them an easy channel for communicating and interacting.

Understanding intent properly is dependent in part from discerning what words you know and what they mean to you in a given context. This is critical for understanding intent and authorization. While Google, Apple, et al know a LOT about us, the only person who can truly express your intent best is YOU.
Perhaps another difference is that the Search box goes on a website's *Home* page, whereas an Intention box might go on their "*Contact Us*" page. You are expressing an intent to engage.
Discussed which type of ontology or storage system might "win" if this takes off and becomes popular. Suggestions include JSON Linked Data (JSONLD), Microsoft Azure, Blockstack. Also, who controls my personal data store—someone like Personal.com? Perhaps we don't need a winner if we can develop an "identity interface" or sockets that people can talk to and let the intention engine just be a broker for communication.

Protocols for Sovereign Technology

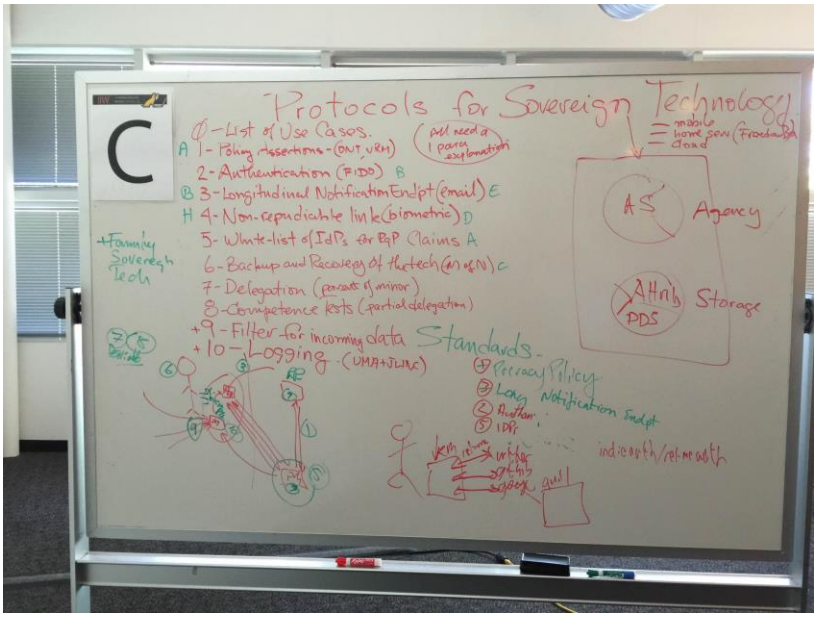
Thursday 3C
Convener: Adrian Gropper
Notes-taker(s): Adrian Gropper

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

Added 9 - Filter for incoming data and 10 - Logging to the 8 components we already listed. Did not take any away.

Ordered the list in terms of importance to two different projects (Green capitals left and right of each item on the attached photo).

Agreed that every vendor claiming to supply sovereign technology needs to say which of the 10 components they support and how.



Biometrics: Revocable & Weaponized

Thursday 3F
Convener: Francisco Corella, Karen Lewison, Jason Law
Notes-taker(s): Francisco Corella

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

The purpose of the session was to provide information about revocable biometrics.

In traditional biometrics a biometric code is obtained by extracting features from a biometric sample, and is matched against a biometric template. But an adversary who captures the template can construct a sample that will match the template, and use the sample to authenticate the user. The user cannot recover from such a compromise, because a traditional biometric credential is not revocable. By contrast, in revocable biometrics, authentication is accomplished using a randomized biometric key derived from a biometric code and helper data. The key is revocable because it is randomized, and the helper data reveals no useful biometric information.

Revocable biometrics have been studied in academia for many years, but are not widely known or used for a variety of reasons, which were discussed during the session. More details can be found here: https://pomcor.com/documents/RevocableBiometrics.pdf

Open Trust Taxonomy Operators

Thursday 4F
Convener: Mike Schwartz
Notes-taker(s): Paul Hethmon

Tags for the session - technology discussed/ideas considered:

technology discussed/ideas considered: oauth token federation

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

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

https://github.com/token-7/token7-specs/blob/master/draft-token7-oauth-token-based-federation-01.txt

Review of "draft-token7-oauth-token-based-federation-01.txt"

Some possible issues with binding a token to the TLS session (and reusing elsewhere)

Feedback given to draft author:

one concern is that this proposed draft is trying to overload the access token, i.e. pass the authorization grant to RS2.
One of the advantages of the grant is that you have authenticated the client. And in your diagram, RS2 is not authenticated
if you were binding the token (AT1) to a TLS session, AS1 would not accept the token from RS1

In general shipping around the bearer token is problematic. Maybe the policy should simply give access to RS1 to call the API of RS2.

We discussed:
https://github.com/token-7/token7-specs/blob/master/draft-token7-oauth-token-based-federation-01.txt

Here was the feedback we sent back to Igor:

1) One concern is that this proposed draft is trying to overload the access token, i.e. pass the authorization grant to RS2.

2) One of the advantages of the grant is that you have authenticated the client. And in your diagram, RS2 is not authenticated.

3) If you were binding the token (AT1) to a TLS session, AS1 would not be accept the token from RS1.

In general, shipping around the bearer token is problematic.

Maybe the policy should just simply give access to RS1 to call the API of RS2.

Igor's response, why not use:
https://tools.ietf.org/html/draft-richer-oauth-chain-00
https://tools.ietf.org/html/draft-hunt-oauth-chain-01

"Yes, I've read both of these drafts. They presume that your resource server is registered/authenticated at your own AS and at all federated ASs. From a purely practical point of view, this is improper for token-based dynamic/automatic federation. I tried to avoid cross domain resource server and client registration/authentication."

So You Want to Run A Standards Group

Thursday 5A
Convener: Justin Richer
Notes-taker(s): Justin Richer

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

So you want to run a standards group? / Justin Richer's Presentation at CIS 2016
We like standards
Standards make things possible
Where do standards come from?
How people think it works
Clear problems
Smart people
Reasonable debate
Best ideas win
How it actually works
Pet problems
All kinds of people
Arguing
Sometimes something wins #angrynerds

The Cast of Characters

The Bikeshedder
Pet problems are the best problems
"We can't move forward until this is solved!"
The Lone Wolf
Comes with a problem and a solution
Nobody asked for either

The Ideas Person
Throws solutions around hoping they stick to problems eventually
Can't actually implement anything
"Wouldn't it be great if…"
The Nazgul
Sows confusion and deceit
Sucks all the life out of forward progress
"We need more time to think about this"

The Pragmatist
Focuses on an immediately-relevant subset
Often loses track of larger picture
Looks for rubber-stamps
"We have this in production already"

The Politician
Gathers a bunch of people to say "yes" or "no" along with them to look like consensus
Constantly running back channel conversations

The Idealist
Only wants to save the world
Implementation details will get worked out
The standard is good only if it solves all of the problems simultaneously

The Puppy
Gets excited by a new shiny thing every week
The shiny thing is The Solution to everything

The Yak Shaver
Loves to write formal use case documents
Believes we have to solve all preconditions first

The Scorpion
They're trying to help, but stinging is in their nature

The Doctor
Has many years experience doing something else entirely unrelated
Believes that this deep expertise automatically carries over into the new space
"Well I was a doctor in private practice for 30 years and…"

The Debater
Every hill is one to die on
No issue is too small to be argued

The Contrarian
Likes to say "no", no matter the question
Believes no consensus should ever be perfect

The Wizard
Stops in periodically to impart wisdom
Doesn't pay much attention to ongoing conversations

The Special Snowflake
Their use case is so special that it will require exceptional handling
Usually has a specific solution already in mind

The Arbitrator
Translates between sides of a debate
Helps move beyond "he said / she said" loops of cross-talk

The Developer
Goes and builds new ideas as they're brought up
"I just built this in five minutes and it's simpler this way…"

The Cross-Pollinator
Brings experience and input from another field or group
"We have a similar problem…"

The Articulator
Restates everything more clearly
Good at capturing forward momentum
"So what we're actually saying is…"

The Rock Star
Used to everyone agreeing with them

Dictator
What they say goes
Debate is a sign of weakness

Loyal Opposition
Lightning rod for the unvoiced
The Lorax

St. Bernard
Loyal, hard working
Willing to climb mountains to save people

The Missionary
Just wants to spread the good news of their ideas
You'll convert because they're right

The Proselytizer
Want to spread the good news of their ideas, by force if necessary
You'll convert, or die a heretic

The Kardashian
Only in it for the fame
"This hot new area will make me rich and famous!"

Process Lawyer
The process matters more than the results

Project Manager
Applies the process to get good results
Smart Questions
Doesn't purport to have all the answers but provides questions in the right directions

The Lurker
Could be brilliant, but we'd never know

The Horse Trader
Will trade you their chips for your carrot sticks and ranch dip
"If you do this for me, I'll support your idea"
Working Together
Agreement models
Rough consensus (IETF)
Member voting (OASIS, ITU, IEEE)
Working group resolution to member voting (OIDF, Kantara)

Agreement models IRL
Politics!
Intrigue!
Backstabbing!

The hard truth
Interpersonal relationships drive standards nearly as much as technological merit
Advice for Making a Standard
Keep it focused
Know what problem you're solving
Learn to say "You Ain't Gonna Need It" (YAGNI)
Don't repeat the past mistakes
Build something
Implement something in code
Deploy it into a reasonable test environment
Watch it run
Document all of your sticky points, assumptions, and shortcuts

Dig into actual needs
Someone coming with a solution is trying to solve a problem, figure out what that problem is
Multiple proposed solutions might be incompatible, but their underlying problems likely aren't
Be Patient
It's going to to slower than you want it to
Everyone else's ideas won't seem to have the same trouble as yours do

Choose your fights
Realize that not everything you say matters
Keep Records
Track issues publicly
Listen constructively
Make sure all needs get heard
Even if they're not acted upon
Short round trip times and beer
You don't run out of time or money, you run out of *patience*

Home Environmental Data, SPIMES and Engineered Privacy

Thursday 5F
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:
Blog Post – A Pico Based Platform for Esproto Sensors
http://www.windley.com/archives/2016/05/a_pico-based_platform_for_esproto_sensors.shtml

Demo for ESProto

- Spimes
  - tracking things through space and time
  - Bruce Sterling
- Using picos for collections of things
  - persistent compute object
  - online, event-based,
- Advantages
  - things don't need smarts, or as much
  - things can be low power (not always on)
  - loosely coupled
  - Each device and each collection get own identity
    - persistent data
    - custom programming
    - API
- Wovyn sensors
  - Wifi
  - ESP8266
  - multiple configurations
  - this is a MSA (temperature, pressure, humidity)
  - POSTs to a customizable URL
- Wovyn and picos are a great combination
  - Picos provide an always on, online persona for the device
  - Picos can be used for collections of devices
  - Each pico can have a unique URL for the sensor to POST to
- Building a spime platform
  - Not just for Wovyn, generalizable to any devices
  - Based on ideas from Fuse Connected Car platform
  - pico prototypes
- Device rules
  - router - changes transducer data POST to meaningful events
    - new_temperature_reading, new_pressure_reading, etc.
  - check_battery
    - battery_level_low
  - device - check thresholds for violations
  - device - manage thresholds
  - device - route violations to all collections
- Collection rules
  - log violations
- Advantages
  - Scales – Easy to set up – Collections can have custom behavivior

SimpleSAML php Workshop

Thursday 1,2,3,4 & 5 H
Convener: Dedra Chamberlin & Jaime Perez
Notes-taker(s): Dedra Chamberlin & Jaime Perez

Tags for the session - technology discussed/ideas considered:

We had a lovely workshop attended by folks from: Amazon Web Services
Pivotal ~ Cirrus Identity ~ University of California, Office of the President
Lehigh University

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

First Jaime reviewed some slides on the current state of the project: You can see them here:
https://drive.google.com/open?id=0B5KWOTS_6A31ZWQyRFFtRmdlQTQ

Then folks from Amazon asked lots of questions about SSP and federation in general. The folks from Pivotal talked about how much they like SSP because they can spin up SAML IdPs easily and cheaply for testing as they do their own development.

We took a short break and then the folks from University of California Office of the President, Cirrus Identity and Jaime from SSP brainstormed some desired roadmap items. The things people were most interested in are listed below:

SSP

- Helping responding to mailing list inquiries
- People contributing issues and quality pull requests
- Good bug reports
- Help writing documentation for the service and reviewing documentation that the SSP maintainers write

UCOP:

- Improved discovery service options
- Entity category options

Cirrus Identity

- Tools for unit testing
- OpenID Connect integration (on the IdP side)
- New modules for Amazon and WeChat
- ECP

After the lunch break, we had a technical session focused on how the project could use Docker containers to pre-build SP and IdP containers to make it easier for new people to use the project.

Mark of UCOP offered to help with documentation writing and review in the future. Cirrus Identity offered to continue making code contributions.

Thank You to All the Fabulous Notes-takers!

There were 85 distinct sessions called and held. We received notes and/or white board shots for 67 of these sessions. Thanks to those of you who submitted notes and information!

Demo Hour

IIW XXII #22 Community Sharing / DEMO LIST
Wednesday April 27, 2015

Thank you to all our Demonstrators!

1. **Yubico: Securing online identities with open standards PIV,OATH, OpenPGP, FIDO U2F**
   Stina Ehrensvard, CEO and Founder & Chris Streeks, Solutions Engineer
   URL: https://www.yubico.com/products/yubikey-hardware
   We'll demo the versatile YubiKey, which supports open standards such as PIV, OATH, OpenPGP and FIDO U2F. Use U2F strong authentication to log into gmail and Dropbox among others. See PIV capabilities that combine with Windows RDP login, and check out one-time password capabilities for LastPass, Salesforce and others. Use the same Yubikey to sign GitHub commits with your GPG keys.

2. **Cirrus Identity Gateway Service: Dedra Chamberlin**
   URL: http://www.cirrusidentity.com/gateway
   In enterprise identity, it's a pain to create and manage accounts for external users. The Cirrus Identity Gateway Service gets rid of "guest" accounts, saving your IT staff time and money, and sparing your external users the frustration of creating a new account.

3. **Universal Compiler:** Scott Shelton
   URL: http://www.scottshelton.com/video/UCTrailerSmall.mov
   The Universal Compiler is an open, crowd-sourced way to translate any natural language human instruction into any computer instruction for any platform or device in any language. It connects people, businesses, and devices with intention, information, and supply and demand.

4. **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 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.

5. **Nymi Band:** Shawn Chance
   URL: www.Nymi.com
   The Nymi Band is a biometrically enabled, wearable authenticator that enables persistent identity. The demo will review the Nymi Band hardware, how to authenticate to the device and how the device can unlock a Windows PC running the Nymi Lock Control application (credential provider).

6. **Blockstack Labs:** Muneeb Ali
   URL: http://blockstack.org
   I will demo a command-line interface for Blockstack, the global Internet database. I will show how the CLI connects to a local or remote server, how you can lookup information in the .id namespace, and how you can register new users without trusting any third party. I'll also demo how the CLI wallet works and how you can backup the privatekeys that own the names you register.

7. **Blockstack Labs / Blockstack Desktop App for Self-Sovereign Identity Management:** Ryan Shea URL: https://blockstack.org
   The Blockstack app let's users create and manage self-sovereign identities on the Blockstack peer-to-peer identity network. Today users can update personal information and look up other profiles, and soon they'll be able to sign documents and authenticate with other apps

8. **Blockstack Labs / Confidential authenticated storage in Blockstack:** Jude Nelson
   URL: https://blockstack.org/blockstack.pdf
   I will show how to share data with Blockstack, the global Internet database. It removes a long-standing UI/UX problem in cryptography by offering *transparent* end-to-end data confidentiality and authenticity with no SPOF, as well as secure and automatic public key management.

9. **Yoti / Yoti the identity app :**David Goate, Bruce Nash, Simon West
   URL: www.yoti.com
   Yoti is your ID, on your phone. It helps you prove who you are to companies and people, online and in person. It takes 90 seconds to create your digital identity, which you can use to log into websites using your face, instantly know who you're talking to online and prove your age.

10. **Clef:** Jessica Riley and Darrell Jones III
    URL: http://getclef.com
    We have built a replacement for usernames and passwords and the most secure user-friendly two-factor authentication available. We power logins for over 125,000 sites and the New York Times describes Clef as "magical."

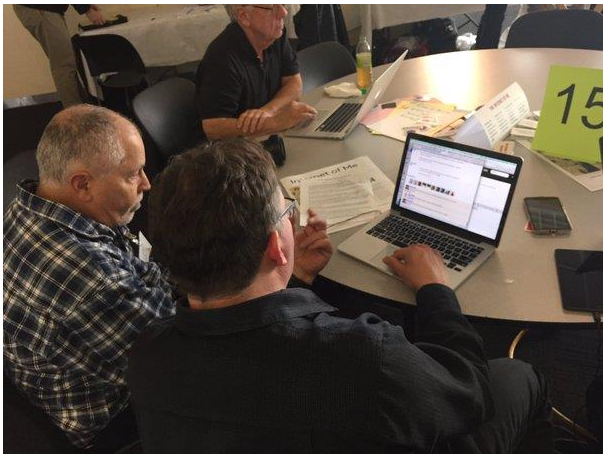
11. **Best Innovation Group / FIBOT – Home Financial and Identity Appliance:** John Best
    URL: https://www.dropbox.com/s/pnqyea0m6zxxquw/FIBOT.pptx?dl=0
    The FIBOT is a stand alone personal blockchain cloud appliance that can integrate with Sovereign identity , it will provide a secure mechanism to shard the private keys to your identity . It will also provide the ability to access your financial information and make secure payments.

12. **IDKeys:** Victor Grey and Jim Fournier
    URL: http://idkeys.org
    ID Keys is a distributed global identity system. It registers cryptographic public keys on the Stellar blockchain to provide fast, secure, resolution without wasted energy.

13. **Spimes and ESProto Sensors:** Phil Windley
    URL: http://www.windley.com
    We use the concept of spimes (Bruce Sterling's neologism for for objects that contain meta data) to organize collections of sensors based on the ESP8266 processor. Using knowledge gleaned from the Fuse Connected Car platform, we are developing a platform that organizes connected things into personal collections while preserving important Internet properties such as decentralization and substitutability.

14. **Cloud Foundry UAA Demo**: Sree Tummidi
    In this demo we will showcase the identity federation capabilities of Cloud Foundry UAA (User Account and Authentication Service). It implements standards like OAuth, SAML & OpenID Connect and is responsible for securing the Cloud Foundry and the Apps and API's running on the platform.

15. And last minute Demo on the **IndieWeb** w/ @KevinMarks

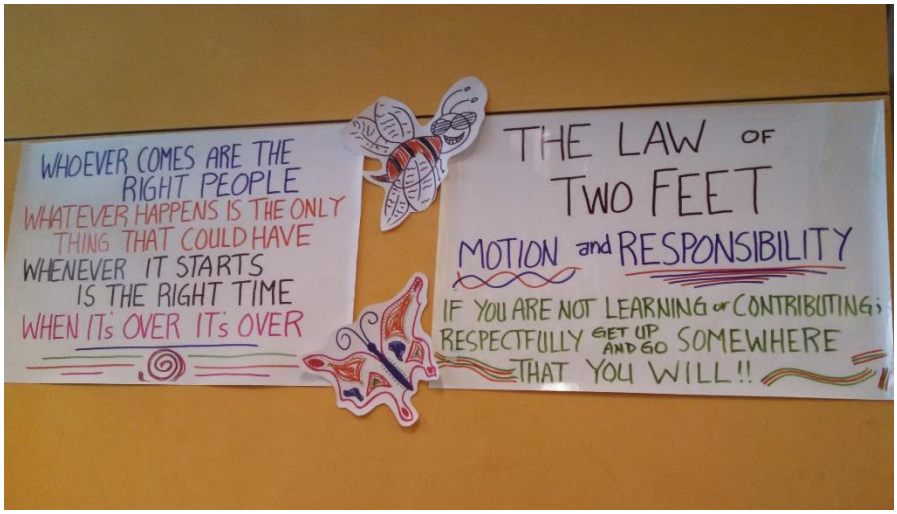


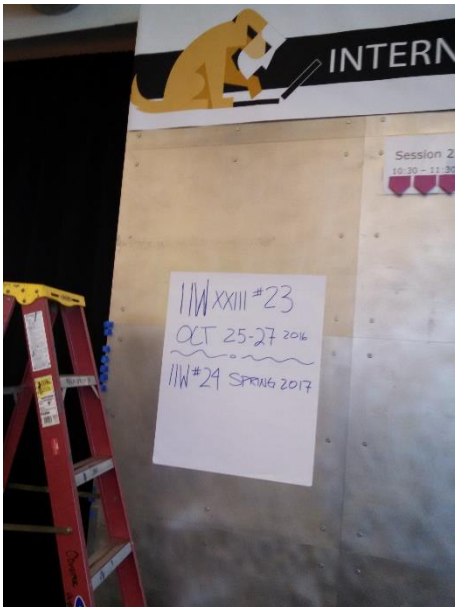
The IIWXXII Demo List can also be found here
http://iiw.idcommons.net/IIW_22_Demo%27s

Becoming Artifacts: Medieval Seals, Passports and the Future of Digital Identity

Dr. Mawaki Chango dissertation, as follows:
http://surface.syr.edu/do/search/?q=Chango&start=0&context=1470928

THE END





See you October 25, 26, 27 2016

for

IIWXXIII

The 23rd Internet Identity Workshop

www.InternetIdentityWorkshop.com