Internet Identity Workshop 17

Book of Proceedings

www.internetidentityworkshop.com

Compiled by
KAS NETELER, HEIDI NOBANTU SAUL AND EMMA GROSS

Notes in this book can also be found online at
http://iiw.idcommons.net/IIW_17_Notes

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

October 22-24, 2013
Computer History Museum
Mountain View, CA

Contents

At IIW we love a good t-shirt as much as we love our facilitation team.

About IIW – the Internet Identity Workshop

The Internet Identity Workshop (IIW) was founded in the fall of 2005 by Phil Windley, Doc Searls and Kaliya Hamlin. IIW is a working group of Identity Commons. It has been a leading space of innovation and collaboration amongst the diverse community working on user-centric identity. The event is now in its 9th year and is Co-produced by Kaliya Hamlin, Phil Windley and Heidi Nobantu Saul.

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

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

For additional information about IIW, you can go here: http://www.internetidentityworkshop.com/about/

To read the Values of IIW as articulated by attendees of the 11th event held in November of 2010, you can go here:

http://www.internetidentityworkshop.com/iiw-values/

To read descriptions of 'what IIW is' as articulated by attendees of the 11th event held in November of 2010, you can go here:

http://www.internetidentityworkshop.com/what-is-iiw/

IW #18 will be May 6, 7 and 8, 2014 in Mountain View, California at the Computer History Museum. Registration will open in early February 2014. You can check for it here: http://www.internetidentityworkshop.com/

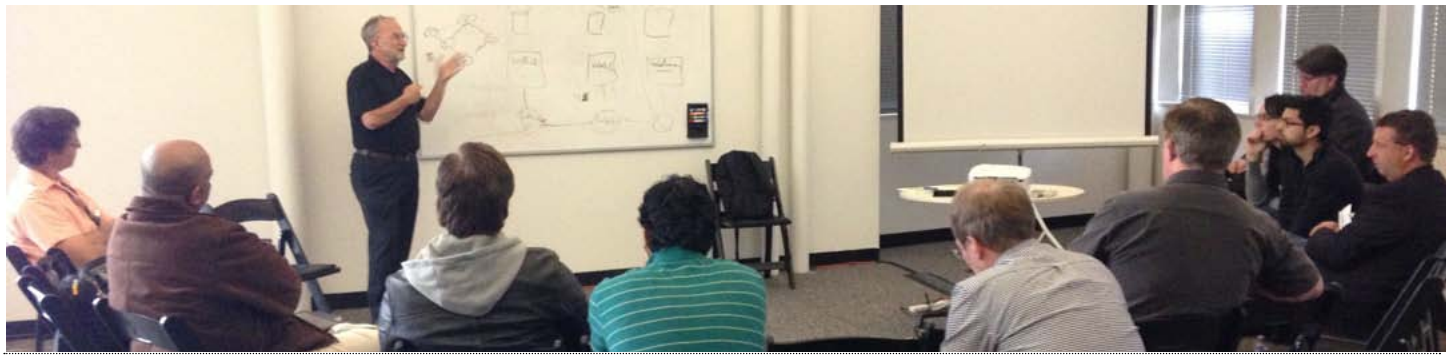
IIW Events would not be possible without the community that gathers or the sponsors that make the gathering feasible. Sponsors of IIW #17 were:

Microsoft, Jan Rain, GIgya, The Trusted Cloud Company, Neustar, miiCard, Google, OASIS IDtrust,White Label Personal Clouds, Apigee, Yubico, NetIQ, Secular Connect

If you are interested in becoming a sponsor or know of anyone who might be please contact Phil Windley at eventbrite@windley.org for event and sponsorship information or reply to this mail with your query.

Upcoming IIW Events in Mountain View California: May 6, 7 and 8, 2014

October 28, 29 and 30, 2014



IIW 17 Session Topics

Tuesday Oct 22, 2013

Session 1

- To Switch or Not Switch… Enabling Smoother Transitions Between Work & Personal – Vicki Milton
- Internet Of Things – Developing a Classification Framework – Jeff Stollman
- Respect Connect "Demo" Safe single sign on for Personal Clouds – Andy Dale/Drummond Reed
- Where Does Your Project/Product Fit in the Personal Cloud Market Matrix – Johannes Ernst
- Identity Revocation The RRVS (required recipient valid since) SMTP header – Bill Mills

Session 2

- How to Make Money Implementing Attribute Exchange: Services, Solutions &Trust Framework – David Coxe
- A Periodic Table of Trust Elements-Building Real TrustFrameworks from the Bottom Up –Ken J K
- NYM ISSUES (pseudo-nym) Why Do We Need "real" name policies? - 'aestetix'
- Defining a Simple Use Taxonmy for Personal Data (think Creative Commons) Sean Maguire
- Find/Create Killer Product (App) & Win In the Market Ali Jelveh
- XDI2 Technical Overview – Markus Sabadello

Session 3

- Federation Conversation / Blood Bath – Tim Bray
- Retiring Protocols – Marius Scurtescu
- VRM 101 – 2.0 - Doc Searls
- Idie Box Freedom Box, 8 Personal Clouds – Markus Sabadello/Johannes Ernst
- A Universal Shopping Cart – Kevin Cox

Session 4

- Respect Connect Deep Dive – Drummond Reed
- OAuth Open ID Connect + FICAM – Allan Foster
- Persistent Compute Objects & The Fabric of Cyberspace & Quantified Everything – Phil Windley/T.Rob
- Household ID and Personal Data @ Rest – Nick Katsivelos
- Putting Informed in Consent – Ken JK

Session 5

- The Business of Personal clouds – Gary Roe
- GreenList Payment Addresses – How to create a new Identity Attribute that benefits everyone on the Planet! – Rick O'Brien
- Secular Connect – Michael Lewis
- Talking Tag – Doc Searls

- Personal Data Ecosystem Architecture – Joe Andrieu
- Skinning the SQRL (Secure QR Login) – T.Rob
- OAuth the good parts intro/review – Dick Hardt/Dam Blum

Wednesday Oct 23, 2013

Session 1

- Respect Connect Deep Deep Dive – Drummond Reed
- User Challenges with Federated Login!! Follow-up From Day 1 – George Fletcher/Vicki Milton
- Vertical $ Opportunities – Connecting the Dots in Real Estate – Monetizing VRM By Delivering Billions In Consumer Savings – Bill Wendell
- ReDelegation in Ouath II – Alan Karp
- NSTIC 101 - Kaliya H

Session 2

- Personas and Privacy – Annabelle Richard
- Security Concerns for RP's I - Session Strength & Reauthentication Proposal from Google –
- Adam Dawes
- Identity Revocation PartDeux – Bill Mills
- Use Case – Mandated Parent Education – Lisa Horwitch
- Personal Cloud Logo Terms – Johannes Ernst
- COZY Cloud MES Info - Benjamin

Session 3

- Customer Commons-Creating a World of Liberated,Powerful & Respected Customers – Doc Searls
- Building Personal Cloud Applications - FUSE - Phil Windley
- FIDO Alliance Update – Sam S
- Personal Data Ecosystem Consortium – Update – Kaliya H
- FCCX Update – Federal Cloud Credential Exchange – Joni Brennan + Jim
- Anonymous Authentication – How Does it Help our Life – Kazue Sako

Session 4

- Health IT Architecture – Debbie Bucci
- Ontology for the Personal Data Ecosystem – Joe Andrieu/Lionel Neuberger
- RP Challenges to Federated Login – Jack Greenberg
- OMIE – customer commons – Doc Searls
- Personal Clouds as Media Indexes for Local Sharing – Phil Windley
- My Identity/Your Identity - Gihan Dias

Session 5

- Google's OIDC'ish Auth Platforms on Android, Chrome, iOS – Breno de Medeiros
- Non-Cloud Providing Enterprise Use + Coordination – Dave Sanford
- Online Data & ID After Death – Akiko Orita
- Intentcasting – Doc Searls
- Descant:Data Systems at the Intersection of Story Telling and Data Reputation – LaVonne Reimer
- After Email… So How Do We Replace It….What Does It Look Like… Kaliya H/William Dyson
- Venture Free StartUp Financing and How Respect Network can Earn Income – Kevin Cox

Thursday Oct 24, 2013

Session 1

- Do Not Disturb Brainstorming – A DNT with TEETH!! – T.Rob
- OAuth 2 Interop Testing – Justin Richter
- Mapping Out Our Digital UnConference – Matt Schutte
- After Email – user experience for all the things we use it for – Kaliya Hamlin
- Can Identity Proofing Eventually Replace Authen? – Rick K (NetIQ)

Session 2

- How do RP's Learn of Big Account Changes at an IDP like Google – Eric Sachs
- Personal Cloud Network - RISK THREAT – Counter Measure Models – Dan Blum
- Email: Are We Asking It To Do Too Much? - Jim Fenton

Session 3

- Exploratory Conversation for Social Good / What Value Does Online Identity Bring to Local Economy - Bill A +
- Privacy – why not? – Morten V Christianson
- CloudOS Programming 101 – Phil Windley/Kynetx
- Trust Frameworks - 101 Definitions / 201 Application - James Varga + Joni Brennan
- Identity by Presence – The Death of Single Sigh On and Federated Identity – Kevin Cox

Session 4

- Rally CRY and Guiding Principles (Part 2) Matt Schutte
- NSTIC (national strategy for trusted identity in cyberspace) Let's Get Real!! – Kaliya Hamlin
- Mapping the Connect Code flow to SAML Artifact Binding to create a server profile – John + Allen

Session 5

- Come to the Movies – UMA (user managed access)
- Cybernetic Augmentation, User Agents & Identity – Michael Lewis

An Overview of One Person's IIW Experience

By: Alan Karp

The opening plenary session had people gather in small groups and individually think of a cross-company or at least cross organization collaboration that succeeded. The first surprise was how hard it was for most people to think of one. Having dredged one up, we were then asked to list five reasons it was successful. The universal answer was shared goals. Another one that came up was an agreed upon governance model. Would final decisions be made by fiat from one person, by majority rule, or something else? We were then asked what we could do in the identity community to make collaborations more likely to succeed.

There was a session on building a taxonomy for the Internet of Things. Was it a human or automaton that initiated an action? To whom does the data belong? For example, data from the Nike Fuseband is for the wearer, but the data from a bathroom scale is for whomever is standing on it. On the other hand, my furnace might "own" the date from my thermostat.

One session discussed Nyms, labels we use for ourselves or apply to other. These need not be pseudonyms. For example, a nickname that is widely understood to refer to a person (Kung Fu Panda for Pablo Sandoval of the SF Giants) is a nym. We discussed how nyms can be used to enhance collaboration. See nymrights.org for more info.

There was a good discussion in the session on OAuth, OpenID and FICAM (Federal Identity, Credential, and Access Management). The goal was to see if the community could come up with profiles that FICAM could accept.

I held a session on Redelegation with OAuth, a topic not covered by the current OAuth spec. The goal is to make it easier for our developers to move the current implementation to a fully OAuth compliant one in a future release if that becomes an important requirement. Unfortunately, the current spec is silent on redelegation, which is using one access token to get another one for the same resource but with reduced rights. The most likely redelegation spec will involve passing something called authorization grants instead of delegated tokens, but that's not much of a change from what our developers are building into Release 1. In particular, the data flow will conform to the spec, but the data passed will be different. That's a good thing, because it's easier to change the data than it is to change the flow. We would have had to pay consultants $10,000 to get this info. Thanks IIW!

An interesting problem arises from a court requirement that divorcing parents take a court-mandated course. These have been done in person, but they are moving to a web model. The problem is knowing that the person sitting in front of the computer is the one who is supposed to be taking the course.

There is a requirement for something called anonymous authentication. Am I over 21? Am I a paid subscriber to this site? We want to answer those questions without the issuer of the credential knowing who used it at the verifier even if the issuer and verifier collude. A cryptographer described the problem and solution without mathematics and asked for and got a number of interesting use cases.

The session on a Healthcare Architecture discussed how the industry is moving from a heavyweight, SOAP-based design to one based on RESTful standards, such as OAuth and OpenID Connect.

A fun session was titled Email Sucks, which started out listing all the reasons we use and like email. We separated email's failings into infrastructure, UI, and how it's used categories.

One guy described an idea for using identity proofing instead of username/password for identification.

It's sort of like your security questions, but it takes into account your geographic location, the machine you're using, past patterns of access, etc.

Personal Clouds are a hot topic at IIW, and there was a session on Risks, Threats, and Countermeasures when personal clouds get networked to each other. We filled in a table and added some additional columns.

A company called SquareTag has created the concept of a PICO (persistent compute object) that has a persistent presence in the cloud. This was demonstrated last year in a session titled "Whiteboards are People, Too" that demonstrated how to give an inanimate object a presence in the cloud. This session showed how to develop apps for PICOs.

One guy has been working on something he calls the Collaborative Internet as a way to accelerate progress. The problem is knowing who to listen to. That was a topic for another day. The purpose of the session was to come up with a simple tag line that he could use as a rallying cry. We came up with trust.worthy.net and "Bringing the trust of the village to the Internet."

The final session I attended was on User Managed Access (UMA), a framework that lets people interact with a service to manage access to their resources. The umanatarians (Yes, that's what they call themselves.) showed a video of a nice demo.

To Switch Or Not To Switch

Tuesday 1A

Convener: Vicki Milton

Notes-taker(s): Ariel Gordon

Tags for the session - technology discussed/ideas considered:

Switching context, Organizational identity vs. personal identity, BYOD, IT compliance

Today's world: rich diversity of devices and ownership models. Information Workers use a mix of organizationally-owned or a personally-owned device to perform their work duties.

Two primary jobs for IT: control access (compliance), and make users more productive.

Progressive organizations: users can use their personally owned device, with a personally-owned identity that IT doesn't control. Still IT needs to allow these users access to organizational resources. This makes enforcing compliance harder. There are solutions to enforce policies on consumer-owned devices via EAS or MDM.

What's the correct user experience? Should users be switching back and forth between personal and organizational context on the device, or is there a way for these identities to coexist in a way that doesn't push the complexity to end users?

Different companies take different approaches. Richard O'Brian: Biometric capture has come of age. Biometrics, such as voice control is a method by which we can achieve seamless authentication. Can it be used to switch context? E.g. user tells the device that it's going to be doing personal stuff. Vicki: many IT are taking a conservative approach to biometrics, for example don't want to store user's bio template.

Vicki: interestingly, investments in strong authentication are starting to outpace the strong auth that exists in the enterprise. Personal identities like Google and Microsoft are using 2MF, while the huge

majority of organizations are still using passwords.

Michael Gile: let's not forget that it's one individual with multiple profiles, represented by different identities associated to their own credentials.

Kirk Brown: in some cases it doesn't matter whihch ID you use. Example: if you're about to pay your bill at Verizon, it may not matter to them who you are when you make the payment (?).

Vicki: issue of Privacy exists independently of work context, especially in Europe.

Very strong cultural influx (Privacy requirements/expectations are different in Europe vs. US).

Additional challenge: explaining to users that they need to agree (opt-in) to corp rules to access org resources from a personal device (waiver).

Michael Gile: Samsung has an interesting approach with Knox: virtually two separate devices; complete isolation of apps/files. On traditional iOS or Android devices, remote wipe erases the whole device; not sure if the same applies to a Samsung Knox device.

Peter Cattaneo, Kirk Brown: happy to use separate applications for different personas (e.g. use Lync and IE with work identity, Skype and Chrome for personal stuff). The selection of an app makes a contextual statement about the identity I'm using. In summary: separate cluster of applications with well-known accounts (strong IdPs). Drive contextual cues as to who you are at that time.

Woman from Amazon: this doesn't scale. Also, may want to use apps with multiple personas (dual-headed apps).

Coupling is a challenge for Relying Parties too. RPs have different trust relationship with IdPs in response to legal imperatives.

Peter: social issue + technical issue: Are protocols smart enough to help with identity disambiguation?

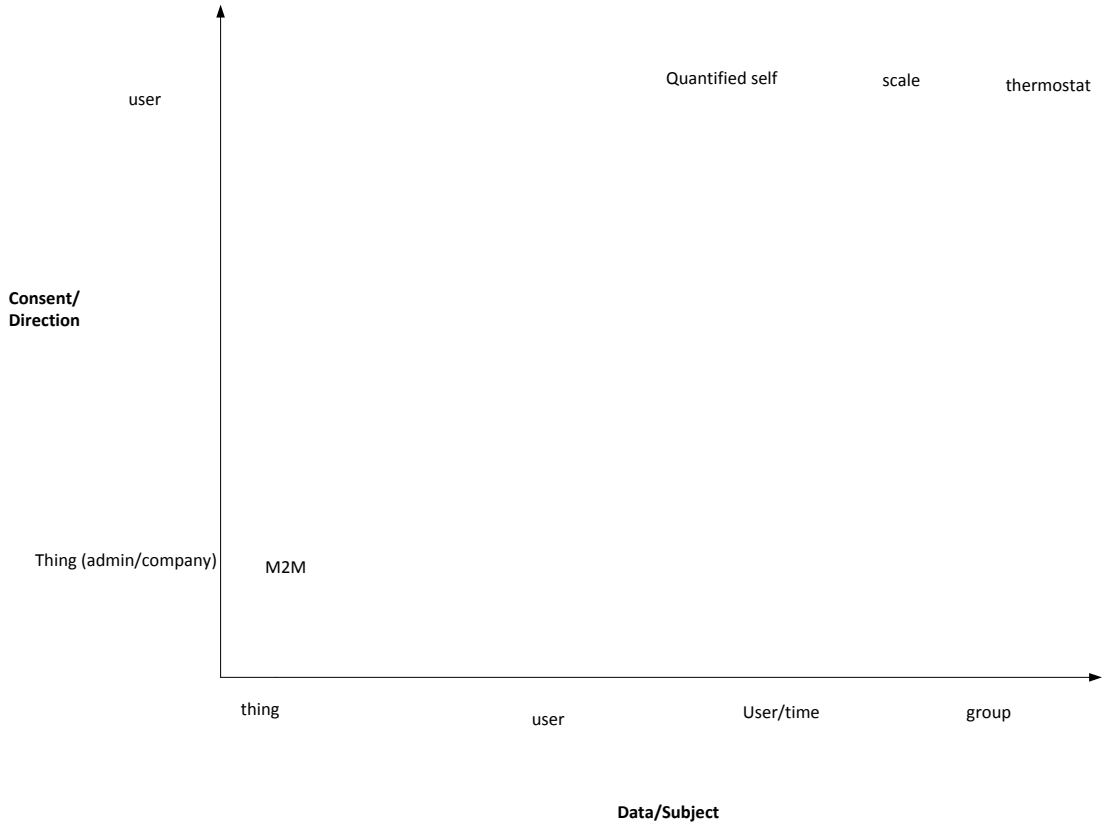
Internet of Things

Tuesday 1E

Convener: Jeff Stollman

Notes-taker(s): Dave Sanford

I came late to session, the group was in the process of creating a framework for devices in the Internet of Things (IoT). On the whiteboard was:



Discussion at that point was about multiple user cases including bathroom scales, cars where user identity comes into play.

Some discussion of constraints against 'self-incrimination', information created in these devices that no amount of 'discovery' can collect – related to search and seizure.

Also discussion of the varying degrees of discoverability required for IoT devices, ranging from passive sensors that are configured and provide data but don't need to be discoverable, through some limited/authenticated domain of discoverability (my house/my cert), to freely discoverable on the Internet – with lots of variations between those points.

Discussion about the distinction between user and administrator. For some devices user might be always able to be both, in other cases the 'household CTO' and others will require some involvement in operations and maintenance by an outside party.

A useful proposed norm for migrating to 'smart devices' was "When you replace a device with a smart device, it should by default act like the dumb device it replaces until it is reconfigured". It was agreed that this will not apply to all types of devices or for that matter business models of device makers.

As part of clarification of the Consent/Direction axis there was discussion of explicit authentication vs. unwitting use which is authorized vs. outside administrator. Some people viewed this axis as about authorization and permission, whereas Jeff indicated that he had proposed it as who consented/directed the device.

More discussion of authentication – included some fairly weak forms of authentication/discovery/joining of personal networks – including stronger (user, device cert) but also allowing weaker (location, network access. We agreed that dumb devices combined with weak authentication could lead to undesirable results (e.g. my fitbit sending data to someone else's account when I'm in their house).

Some devices are input only, some are output only, both and they may vary widely in their amount of processing and discoverability.

Where Does Your Project/Product Fit in the Personal Cloud Market Matrix?

Tuesday 1G

Convener: Johannes Ernst

Notes-taker(s): Johannes Ernst

These aren't exactly meeting notes, but they do summarize the results.

http://lists.pde.cc/lists/arc/personal-clouds/2013-10/msg00059.html

http://lists.pde.cc/lists/arc/personal-clouds/2013-10/msg00063.html

How to Make Money Implementing Services, Solutions and Trust Frameworks with an Attribute Exchanges Trust Framework

Tuesday 2A

Convener: David Coxe

Notes-taker(s): David Coxe

During 2011, IDW and Google designed and developed open-source software to support cloud-based web services based on standards like OAuth, OpenID Connect and SAML to enable the data flows for Identity Providers (IDPs), Relying Parties (RPs), Attribute Providers (APs), and users as key elements of the online identity credential and attribute exchange ecosystem. IDW subsequently implemented an Attribute Exchange Network (AXN) as an online Internet-scale gateway for Relying Parties (RPs) to efficiently and affordably access user-asserted, permissioned, and verified online identity credentials and attributes from third party providers (Attribute Providers (APs) and/or Identity Providers (IdPs)). The AXN business model stimulates market participation through a mechanism for accessing, servicing, and monetizing existing and new online business markets that are currently underserved by the online identity ecosystem. The AXN is built on open industry standards as a neutral transaction, contractual, and claims management hub that can enforce privacy and security precepts driven by industry and in support of the National Strategy for Trusted Identities in Cyberspace (NSTIC) Guiding Principles.

The Periodic Table of Federations

Tuesday 2D

Convener: Ken Klingenstein

Notes-taker(s): William Lowe

Basic overview: this session highlighted the lessons learned by InCommon during their 10 year plus experience operating a federation of autonomous IdP's and SP's. Based on this experience, Ken formulated a periodical table that identified common considerations for those interested in creating and operating their own federation.

Goal: start a conversation that could help create a standard framework for creating and operating a federation of autonomous industry participants.

Goal: determine a framework for the creation of federations that enables 'fire retardant federation operators'. (i.e. make it as simple as possible to create and operate a federation in order to reduce common mistakes)

Terminology: Trust frameworks or marks are bad terminology because they're often misconstrued. But, based on experience, we understand trust elements that can be used, in concert, to create frameworks and marks.

Background: InCommon runs a full mesh federation, as opposed to a hub-and-spoke federation, meaning each federation participant manages it's own Identity Provider (IdP).

InCommon Federation projected to include 20,000 IdP's within the next few years.

Federations consist of tools and rules. Rules can be subject to legal enforcement based on privacy laws within the federations region.

There are federation operators and federation participants. Federation operators need to set the federation schema.

National Information Exchange Model (NIEM) is the largest federation in world. For a list of Shibboleth Federations, scroll to the bottom of: http://en.wikipedia.org/wiki/Shibboleth_(Internet2)

Referring to the periodic table diagram presented:

- Rows of the table reflect layers of scale in the ecosystem

- Rows include federation operators elements, operator to member elements, member to member elements, attribute authority elements, end user elements.

Federation operators need to set rules for: eligibility, termination dispute resolution,

identity vetting.

Other possible considerations for federation operators: audit applications for minimal attribute disclosure, compliance with European privacy laws, etc.

End user privacy still needs work. Added tools for individual control of managing privacy is on the horizon. InCommon hopes that in 2 years all institutions in the federation will provide their users tools for better management of PII.

Why? Because nobody really understands exactly what "downstream" dissemination of user data means. Where does it go? More importantly, what can you do with my data?

Some technical considerations...

Schema needs unique bindings. For example, kids need binding to parent and teachers.

If you asked if somebody is a student, do you assert that the individual is a student because InCommon said so? No. Each institution validates their own people.

What about correlation? Non correlatable identifiers are best option for ensuring anonymity.

Signed assertions. Syntax is normative. Rough semantics for commonality of meaning.

Attributes are provided by the gateway.

How do we set a standard for federation creation regardless of industry?

Biggest change for federations from industry to industry is schema. Single most non generalizable aspect.

Dynamic metadata requires commonality of policy.

Why federations? Federations normalize us for behavior, which is the only way to achieve scale.

Possible next steps:

Step1: Find new elements in the wetware.

Step2: Find complementary trust marks to create comprehensive trust framework

Federation Conversation

Tuesday 3A

Convener: Tim Bray, Google

Notes-taker(s): Vicki Milton

- There are developers that don't care about the underlying technologies
- Tim created a blog that asked "why federate?" – get out of the password business
- Got ugly really fast – flamed everywhere
- Still believes that federation login is a generally good idea
- But was very educated through the pushback he received and it should be taken seriously
- Federated login = sign in with Twitter or Facebook

Arguments

- Users don't understand what is happening
- Confusion as to what is happening in SSO operation
- Trust plays a role
- Users are worried about information flows from IDP to RP
- I don't like being tracked
- Leaves trails
- I don't like you
- Consumers don't like the companies asking for the data or sharing data
- I don't like spooks

- Can be accessed by the government/intelligence professionals
- Metadata creates patterns
- Companies are beholden to government requirements
- I like Mozilla persona
- just use that
- I like password managers

What's the problem

- I forget which provider I'm supposed to use
- Not sure which IDP I used last time I was there
- You're a single point of vulnerability
- You're a single point of blockage
- Too much power to Facebook
- I'm a user not an operator
- Understands why a developer would want to get out of the password business but the user can't see the value to them.

There are objections to Google and there are general objections. Which ones did you see? Tracking discussion included concepts:

- Reacting to brand
- Every IDP is up against the same thing
- Some IDPs may be seeking to be on the login page
- Google and FB are the primary IDPs
- Federation happens in the enterprise space as well, but that is not the direction for this discussion
- IDPs are just identities that users use to represent their persona online. So inherently they see the repeated use of a particular identity as a way to triangulate their behavior.

NASCAR page was a really bad thing – looks like crap

What about oversight by government?

- Small sites might not be as likely to push back on government data requests
- Single provider allows them to better see where the user went as opposed to many sites.
- Federation blocks the movement to a claims based world??
- Oauth was designed to enabled AuthZ without disclosing identity
- Google didn't get into business as an identity provider, but as an application provider. But the aggregation of identities and the data platform created a basis of mistrust.
- Low friction way to facilitate data provider through a user paid revenue model would be very interesting.
- Need to build applications that assume the user has more than one identity.
- Industry isn't about driving to one identity.

- Users don't understand that they are making a trade for information for authN. Need informed consent.
- Microsoft does a pretty good job of providing info on what's going on
- Be interesting to separate the AuthN from the tracking.
- Check out the Mozilla Persona protocol.
- Allows the user to log into an RP through an IDP without letting the IDP know what you're doing.
- Google does track what you're logging into, but they don't generally look at the data before it's purged
- The thing that's missing is the voice of the user
- What's going on is that corps are collecting data on what the users are doing
- There are ways to do federation and only releasing attributes instead of identity.
- Not clear that the user would understand it anyway
- Tim's blog is for developers and doesn't represent the voice of the user and their concerns
- Why aren't there people out there reviewing IDPs? Walt Mossberg doesn't report on this.
- RPs make the choice, not the user
- There's no way for a person to actually know what's going on, no history, no reputation
- Google has a single privacy policy, but there is no way to test that anyone's doing the right thing because it's all new
- MFA will not scale to multiple sites without federated identity. With a single second factor on a federated identity, we can improve the quality
- Google says should enter passwords on any site without 100 staff to deal with identity security.
- Don't want to carry around a token for everyone
- Google authenticator app is in substantial use across platforms and it doesn't use federation
- Is there demand for an identity prosumer market.
- Email account is a single point of failure, and big IDPs as users to enter a backup account to address account compromise.
- There is a large world of users that have identities with IDPs that enable self assertion and they don't necessarily track nor do they have this problem

I don't like tracking. There are some people that are more concerning:

- Bad guys
- Government
- Other government
- People tracking to monetize
- Some identities are "followed" by people and so users are concerned about linkages sending messages to the primary.
- Users make an explicit decision about who they want to be perceived when they sign in.

- Forgetting who they logged on is a big problem
- Users biggest issue is not in identity representation, it's in having to authenticate.
- RPs needed an IDP and often choose one based on data exchange and what is offered. But that is what concerns the user is that RP value exchange.
- Context matters. Work/personal. Login is about establishing your context
- Women have been known to have more personas than men (6-10) compared to men (2-4).
- IDP fatique could lead to the consolidation of personals to 3-4 IDPs which represents a more complete persona of the user
- Privacy impacts due to this.

Universal Shopping Cart

Tuesday 3J

Convener: Kevin Cox

Notes-taker(s): Kevin Cox

Tags for the session - technology discussed/ideas considered:

Behavioral identification, personal shopping carts, CloudOS,

The idea of using the person's device instead of a user code and the idea of using previously remembered behavior instead of a password was discussed. The idea that a person's shopping cart is theirs and not the website was discussed and the implications of how that reduces the need for strong identification at the website selling the goods. Strong identification is needed at the time of the payment but that identification is the responsibility of the payment gateway and not the selling website.

It was pointed out that there is a whole new product needed to manage the history of what goes into the shopping cart.

Persistent Compute Objects & The Fabric of Cyberspace & Quantified Everything

Tuesday 4F

Convener: Phil Windley & T.Rob

Notes-taker(s): T.Rob

Tags for the session - technology discussed/ideas considered:

Internet of Things, IoT, pCloud, pico, sensors, actuators, devices

Phil's Slideshare: http://www.slideshare.net/windley/persistent-compute-objects-picos

Phil started the session with a slide deck explaining the key concepts and their implementation by the folks at Kynetx. He explained that while Kynetx has one implementation, the concepts are generic

and could be implemented in other ways. However, Kynetx has a current working implementation which he was able to draw on for purposes of illustration.

Phil referenced David Gelerntner's book Mirror Worlds as having mapped the territory that we are finally able to build with current technology. The book describes computer models that mirror real-world objects and behaviors in real-time and then record those states and behaviors. The result is the ability to correlate events across previously unrelated systems to improve efficiency, safety and comfort and to generate complex automated behaviors.

T.Rob presented in the second half. Although no slides were presented, the deck from Monday's pCloud & VRM Day is relevant. T.Rob asks the question "what architectures can support a world in which the most mundane objects are instrumented?" We currently have smart forks, basketballs, pens, chairs, shoes, switches, outlets, exercise equipment, medical devices, and more – with much, much more on the way.

The current architecture is that all of these things talk through an SSL tunnel to the vendor and the device owner gets whatever data and integration that the device owner sees fit to provide. This isn't the optimal architecture, it is simply inherited from the world in which computers cost millions of dollars and vendors owned all the data because it could not work any other way. But today it can work a different way because most people have the equivalent of a mainframe form the 1980s in their pocket. There is no reason to cling to the old architecture when vendors kept all the data, nor should we.

An alternative architecture was proposed in which devices report data back to the device owner first, then vendors and other 3rd parties are secondary or tertiary users of that data. Rather than trusting the data because it arrives over an authenticated SSL tunnel, device manufacturers should sign the data so it can be authenticated outside the context of a connection. The vendor's economic model should work without necessarily getting the user's data. Then the user can choose whether and how much of that data to allow out to the vendor. The incentive is then on the vendor to provide some actual value to the device owner in return for access to the data.

This architecture is reflected in the Kynetx implementation of picos. Kynetix provides hosting and initial implementation of code to represent different types of real-world object. But the owners of those objects own the data on which the code is run. Rather than pushing your data to the vendor's cloud where they operate on it (think Google Docs), instead the vendors' software is brought to the data and operates on it there.

Mirror Worlds: or the Day Software Puts the Universe in a Shoebox...How It Will Happen and What It Will Mean
David Gelerntner, Oxford University Press, USA (November 14, 1991)
http://www.amazon.com/exec/obidos/ASIN/B000QTD1HE

Out Of Control: The New Biology Of Machines, Social Systems, And The Economic World
Kevin Kelly, Perseus Books; 1St Edition edition (May 1994)
http://www.amazon.com/exec/obidos/ASIN/0201483408

Let's Get Cirrus About Personal Clouds
http://www.slideshare.net/tdotrob/lets-get-cirrus

http://www.slideshare.net/windley/persistent-compute-objects-picos

Household ID and Personal Data @ Rest

Tuesday 4G

Convener: Nick Katsivelos

Notes-taker(s): Leon Brown

Nick @ Family CTO R/G

Issues: Lots of devices in house, lots of stuff in-home to take care of, looking to make Family CTO into a movement

Family	Enterprise
Personal	SMB

Gap is in family space

Ideas get killed for not understanding personal information: Example was a product to help making a birthday event for a six year old which may involve collection photos. Lawyers poo-poo it.

“API Economy” and people exposing data - lots of data mashup apps and services

Issue: Login + chicklet of social logins

Talking about commoditization of authentication and how developers leverage convenience of using a larger login system

Movie “Terms and Conditions May Apply”

Want: Similar to OAuth methodology, abstract storage from access. Offer developers a simple way to access.

PDE - Personal Data Ecosystem mailing list

“Jan Rain” ??? ▫ Ask Marla Hay

How high in the trust parameters need to go allow access to arbitrary storage?

Where you don’t want to pay PCI compliance? PCI compliance still required if you have data stored on an individuals

Wine example: I shop at three wine sites, they can give me purchase history

Individuals have an API on their personal data ‘wine api’

Ancillary service like TripIt dot come - initially email it in an data aggregates back to my storage.

Mes Info (My Info - in French) - What happens when you give a customer their personal data? Ask Joceyln Searles. Using 300 interested customers who have multiple service usage. Developers get access to provide value.

HouseHold ID - Would help if multiple people could be aggregated on a single lump at times. Like going to the supermarket. Good research problem: Families hack the system all the time - multiple family members using same CVS card. How prevalent?

OAuth the Good Parts Intro

Tuesday 5J

Convener: Dick Hardt/Dan Blum

Notes-taker(s): Dam Blum

Note: this session was combined with the session OAuth 2.0 Assurance by Dan Blum

Summary: Attendees of this session were primarily interested in sharing observations on OAuth best practices. After some discussion, a debate arose about best practices for securing the OAuth interaction with mobile clients. This debate wasn't resolved.

General Notes:

OAuth is a framework, not a protocol

As client, you don't know where the access token came from

Many implementations still use OAuth 1, there was some discussion of this but no strong reason or justification to continue focusing on OAuth 1 was expressed at this meeting

How do you build an API that lets people run apps that register people on the device

what are the best practices? Use access tokens over SSL.

Major social networks (e.g. salesforce) are giving developers samples that are "like" what they are trying to do, often this is driven by historical reasons

Secure OAuth use with mobile devices discussion / debate

Dick Hardt advises

Don't use implicit flow; register device

Separate mobile client app seeking access to OAuth data into two parts:

1) the user agent on the device and

2) server component

Store the app tokens in the client server, store only per-device tokens on the endpoint; this effectively means that every endpoint is registered

A debate arose: what is the value of dynamic registration when you can't authenticate the device to begin with?

User Challenges with Federated Login!! Follow-Up From Day 1

Wednesday 1B

Convener: Vicki Milton/George Fletcher

Notes-taker(s): Vicki Milton

Tags for the session - technology discussed/ideas considered:

IDP, RP, User challenges, Data exchange, User experience

There are benefits and drawbacks to being an IDP or an RP, for example:

RP

+ get out of the password business

+ lowers sign up barriers to entry

- Vulnerable to IDP zigzagging, could go away

- account recovery changes

IDP

+ Ability to follow the user to where they go

+ greater brand loyalty through continued use of identity

- Meeting needs of RP

- potential legal liability

This session will explore the impact to users, the benefits and the challenges. We'll also catalog known unintended consequences from today's implementations (both good & bad)

User benefits

Sign in Ease of user

Better security, less likely to be hacked due to concentrated security investments by big IDPs

No form fill

With long term identity relationship, may get greater access to services for having a quality account

Email as sign in – simplicity and memorability in the username

User challenges

Data exchange

Not understanding what get's shared

Distinguishing which data is needed for functionality vs. what is being asked for during sign-in

Unclear on the potential use of the data

Ability for users to easily assess horsetrade

Opt-in

Agreeing to data access before perceived benefit

Alternative approach of Just-in-time opt-in creates friction

The architectural differences between native app vs. server request. Servers will require upfront requests.

Must relinquish data to gain service benefits

User experience

Forgetfulness, how to recall what was used to login the last time, especially when using long term cookies

Still no common ceremony

How to determine when the data can automatically be used, vs. a need to ask the user

If something goes wrong, who are you going to call, the RP or the IDP

Manageability

No user management

Lack of control

Requirement for a secure and controllable experience

Customer relationship

May not know the IDP that is being used

If the user is faced with inability to access a paid service, who reimburses the user?

The most trusted IDP is not an option on the sign in screen

Need to better convey the trust relationship that exists between the RP and the IDP

Unintended consequences

Persona “slamming” – forcing a merge of persona activities due to limited choices of sign ins

Need for a persona manager – account user shows last user login

Device could play a role in helping the user decide what identities are available to use

Increased account security on a core set of IDPs

Lack of flexibility in data exchange approval screens

Need for optional scopes – technology is available is isn’t being used

Increased difficulty in app developer experience

UI design has too many words

Need to separate app data needs from marketing promotion data needs

Value proposition statements are not included

We are habituating consent

If you fail to share data, you fail authentication

Users are creating “trial accounts” to see what data is being used

Leads to abandonment of trial account once trust is established (they move to IDP account)

Site can’t link the identities to see cradle to grave site use

Implementations don’t allow a slow build on the relationship

Reduction of passwords might adversely affect the revenue streams of password management software

Re-delegation in OAuth – AuthorizationServiceUserClient

Wednesday 1I

Convener: Alan Karp

Notes-taker(s): Alan Karp

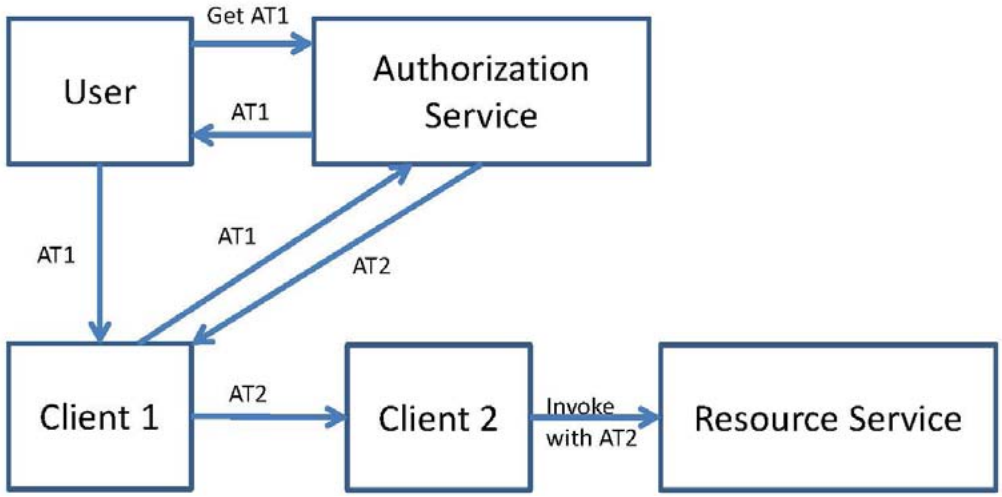
OAuth 2 provides a means for a user to delegate to a client permission to access a protected resource. However, that client frequently needs to re-delegate that permission to another client. The current specifications, http://tools.ietf.org/html/rfc6749 , http://tools.ietf.org/html/rfc6750 , are silent on how that is to be done.

There are two expired drafts to consider, http://tools.ietf.org/html/draft-richer-oauth-chain-00 , and

http://tools.ietf.org/html/draft-vrancken-oauth-redelegation-00 , which are similar but not identical.

I am working with a group in HP building an infrastructure component that is currently OAuth-like (because our developers are on a tight schedule and don’t have time to learn OAuth). I would like to make it fully OAuth going forward, but we need re-delegation with sub-scoping now. The point of this session is to find out what the re-delegation spec is likely to look like, so we can make our implementation easy to change when the re-delegation spec gets published.

The pattern we’re currently using is shown in the figure. It is not OAuth because the User gives Client 1 an access token rather than a grant. The transfer to Client 2 also is an access token. The current draft proposal says we should be passing grants instead. Fortunately, in a later release we could simply change to using grants with minimal disruption. Also, in our current implementation we have combined the Authorization Service with the Resource Service, but that is allowed by the spec.



NSTIC 101

Wednesday 1J

Convener: Kaliya

Notes-taker(s): Michael Lewis

Tags for the session - technology discussed/ideas considered:

NSTIC, NPO, IDESG

Kaliya started off with a question: Why are you here at this session? What do you want to get out of it? Answers varied, but general theme was "What is NSTIC and what is the status?"

What's going on

Security industry- smart cards and access control cards.

Concerned with FICAM and NSTIC, lack of physical security aspect.

Not involved in steering groups.

Digital rights ppl think he knows about NSTIC, so he wants to

Thought NSTIC was a flawed strategy, want to see

NSTIC after Snowden

Involved with NSTIC, frustrated wants to discuss to make it better

Don't know anything about NSTIC

How does NSTIC make decisions

Security Standards Committee- things not moving too fast, have functional models, want to try to push it forward (new session proposal?)

Need update

NSTIC office- want to know what ppl think, help correct misperceptions

Did ppl get grants and is that process working?

Have proof of concept code

Grant awardee- here to get best practices

New Session Plan: Not enough critical mass to have the "let's get real" conversation, so Kaliya is going to talk about history, state and what is NSTIC, and how to get involved.

FICAM - federal program, goal is how to support citizens login into agencies.

After 9/11 mandate that all government employees and contractors need to be ID'd with interop systems.

12M IDs issued. Now how to do it for citizens?

NSTIC

At start of first term, Obama admin did a study. National cyber-security review.

Found that password reuse is a problem to be solved. Catalyst for engaging with industry sector.

Andy Osmit and Mike Garcia wrote a draft in July 2010.

First draft published in April 2011

What is NSTIC about?

passwords suck, how do we address it?

reduce number of credentials

use more single/federated sign on

Kaliya wrote a response to the backlash about “global id” problems that could be addressed:

normative rules and practices for everyday life

lawful intercept

Creepy NSA stuff

NSTIC addresses only #1

Govn’t motivation for NSTIC

Each government agency can’t issue its own secure ID/smartcard

too expensive

everyone would have chain of dongles

... but also a national ID isn’t going to fly: Americans don’t like it

NSTIC is a way to create free-market solution that can be leveraged by government agencies

Bonus: how to use the 12M government issued credentials in private sector

issues: legal liability, what is the bar for proof, how to be pseudonymous, etc.

Jim: Important to know that this is not a government initiative.

It is a government funded a project that is led by private sector.

Now a 501(c) nonprofit

[Perhaps for tomorrow: What do people _think_ NSTIC document says? Lot of different perceptions.]

Early NSTIC History:

National Program Office (NPO) launched. NPO to facilitate.

Jim:

see NSTIC.gov: there are three parts

1 Federal Cloud Credential Exchange

2 Pilot project awards: e.g.

2a service awarded to SecureKey. Allows citizens to use provider of their choice (google, etc.) to access govm’t services

2b Recent award to Michgan to do this at the state level

3 IDESG - Identity ecosystem steering group <--- this is what we’re concerned with here.

A NOI for governance was issued

David T came up with charter & bylaws proposal to bootstrap it

RFP was issued for a Secretariat:

Trusted Federal chosen as Secretariat and awarded $2.5M to manage bootstrap process

14 stakeholder categories were created.

e.g. business & entrepreneurs, regulated industries, ID providers, unaffiliated, etc.

Anyone can join Plenary for free, and self-assert which category they want to join.

Plenary elects:

management council (including, Don, Kalyia, etc.)

chair of Plenary (currently Bob Blakely)

Governance meeting was 270 people.

Bit of a rush... so the stakeholder groups were solidified before there were even rules adopted by plenary, before management council was elected.

Goal output is: “Identity Ecosystem Framework”. What is this?

Stakeholder groups don’t really do much except elect people.

current state of IDESG (a.k.a. NSTIC/although its not really technical accurate):

no overall plenary mailing list.

lots of individual mailing lists.

seems like mostly government contractors who have time to go to meetings

week diversity of participation:

e.g. disabled community, minority communities, immigrant communities, sexual minority, religious communities (important for schools that implement IDs that object)

Trusted Federal ran out of grant money in Oct (was supposed to last until next Aug)

q: What does Trusted Federal do?

a: schedule/run meetings and plenaries, basic website, mailing lists.

Mgmt Council has no visibility into Secretariat’s ops, budget, etc.

NPO will put out competitive bid for fund to support the framework stuff.

Hopefully the 501(c) will win it... government _has to_ issue only competitive bids.

Undecided: how to fund this 501(c), re: corp membership fees, personal fees, grants, etc.

Jim:

What is your recommendation for moving forward and improving situation?

Kaliya:

Look at Ken Klingenstine is doing good stuff. (Also a NSTIC pilot recipient).

Look at Andrew Hughs & Tom S: also doing work in similar area.

Both working on interop of Trust Frameworks.

Get the vocabulary / taxonomy figured out.

Define what is a functional model.

Engage with citizens: e.g. youtube videos to get real world use cases

Q: Anyone on Mgmt council know how to do

Jim: resources

1 NSTIC Notes site, including a functional model

2 idecosystem.org

3 @NSTICNPO twitter handle

4 NSTIC.gov

Q: where do we get more diversity?

A: e.g. Go to Laraza and find a techie and get them to commit staff to showing up

Kaliya's magic-wand wish list:

1 Regional f2f meetings

2 use professional community building and synth practices

Personas & Privacy

Wednesday 2A

Convener: Annabelle Richard

Notes-taker(s): Dave Sanford

Because of the need for common attributes shared across personas - attribute firewalls between personas were discussed along with the need for firewalls to "allow poking holes" between those firewalls as needed.

There was some push back against the initial discussions assuming these personas were used in a federated space.

Distinction was made between personas, attributes and context. One definition of privacy that was put forth as privacy = 'contextual integrity'.

Also discussion of separating the discussion of:

user behavior required to maintain separation of personas (hard to maintain consistency)

conceptual frameworks to allow definition and implementation of personas

tools that actually allow users to have and manage multiple personas

There was discussion of big data business models hovering up data and able to break separation. For most people this ability to de-anonymize them doesn't matter, for a few it is a matter of life and death.

There was discussion of not tying personas to account ids. One thought was the idea of mapping personas to times of day/calendar attributes. Various exceptions to this were identified in normal human behavior (personal interrupts during work, etc.).

The claim was made that if a common payment method or credential (bank acct, credit card) across personas, that transactions would be mapped in the cloud.

There was a continuing discussion of whether we want to assume good actors (Relying Parties, Identity Providers) in the cloud – or protect against these as bad actors (big data aggregators not honoring boundaries). Consensus is that we need to support and assume both to some extent – but that these are different problems.

Some discussion of the UMA authorization manager and its ability to support multiple personas.

There was discussion of two different ways in which context is created, either context is inferred from transactions or persona owner declares context.

Not all personas are created equal. Some need to be strongly authenticated, others not so much.

It was pointed out that it only takes one mistake from the users to allow the big data mash-up parties to break persona separation – once that is broken it will be impossible to fix without discarding personas and creating new ones.

We want to encourage as many good actor business decisions (e.g. Amazon will not send email recommendations for LGBT products even if your history suggests that you want that, because who knows who will read that email).

Our main job is to facilitate building of tools, given the assumption that there are some external bad actors. The question was asked – where was the ethics review at Target that allowed the pregnancy prediction to be made and acted upon. Providers need to recognize the ethics.

Still an open issue as to whether we will only or best be able to separate context by ID. If we want to limit or question the linkage between context and IDs, we would start with what we want for personas – identify how to call out contextual awareness and then figure out how and when to link this to identifiers and authentication.

Personas can be thought of as sets of 'public' attributes.

There was some discussion of the old pre-Internet models:

pay cash in the physical world (anonymous)

buy drink, show driver's license – the transaction information never goes back to DMV

There was the claim that targeted advertisement is being found to be not that effective – however at the moment more money is going into it.

Security Concerns for RP's I Session Strength & Re-authorization Proposal from Google

Wednesday 2B

Convener: Adam Dawes

Notes-taker(s): Adam Dawes

Link to Presentation:

https://docs.google.com/a/google.com/presentation/d/1G_T_dE5KNSa71P47h_u7x7fDwMYn68Ux5pjyx-H8okE/edit#slide=id.g10f4027ee_01

Use Case to Solve

Wednesday 2G

Convener: Lisa Horwitch

Notes-taker(s): Lisa Horwitch

Tags for the session - technology discussed/ideas considered:

Personal identification & authentication processes.

USE CASE TO SOLVE: Court mandated parent education for divorcing/separating parents. Currently use a face-to-face class. Now offering online. CHALLENGE: Judges mandating the parent education course need to know that the person taking the online course is, in fact, the person mandated to take the class (and not a "significant other" or the like). Parameters for solution: needs to be minimal to no cost; easy to use; enrollment; serves 2 different clientele populations (paying and no pay – indigent); ability to secure multiple log-ins. COME & PITCH ON THE SOLUTION(S). (Moderated by Kaliya)

Summary:

This session provided an opportunity to hear various solutions to the challenge posted – in a court mandated parent education online course – how can the court (Judges) be assured that the person "ordered" to take the online program is actually the person who signs up, logs in, and takes the class? In addition, how does the online company assure that the person taking the class, continues to be the actual person who is supposed to take the course (ongoing monitoring during class sessions or multiple log-ins)?

Background: The online class is structured in a way where the client purchases a 30-day account. During that 30-day period the client/parent has the opportunity to log in and out as often as he/she wishes. The client/parent is not required to take the course in 1 sitting. The class takes between 3-5 hours to complete. At the end of the class each participant receives a certificate of completion which is then provided to the court as compliance with the court order.

Needs for authentication include:

Minimal to no cost

Not complicated

Easy to use (for parents/clients)

Serves 2 different clients groups (paying & non-paying)

Enrollment – 1 x; then how to monitor ongoing

Summary of items touched upon during session discussion:

KBA processes for each log in different set of questions

Webcams; some type of web proofing at the start (purchase page or onboarding process);

Potential for using picture of the client; how to maintain contact throughout the time the parent is taking the course (facial recognition, voice, etc)

Use of some type of Biometrics (voice, thumb print, eye, signature, etc) – do at start.

Throughout the class find natural junctures within to use monitoring process.

Utilizing existing services (companies, auditing services, etc)

QR, Smart phones, etc.

US Postal Service (hub for ID authentication in future)

Any additional thoughts that one might want to share, please send your ideas to Lisa at Educator425@gmail.com.

Personal Cloud Logo Terms

Wednesday 2H

Convener: Johannes Ernst

Notes-taker(s): Johannes Ernst

Long discussion about how to make progress faster. General agreement with Phil's general proposal to "get it out and fix it later if it needs fixing". So we came up with a few things to do immediately, and things to do "later" if and when we have time and resources.

We decided that we could solve the various use cases for the logo with the following, much simpler approach:

1. We modify the logo to make the phrase "My data, my way" part of the graphics
2. We require that wherever possible, the use of the logo links back to a page onpersonal-clouds.org that we maintain
3. We require that any use of the logo has a footnote that says "The Personal Cloud logo is a trademark of the Personal Data Ecosystem Consortium, a working group of Identity Commons Inc."
4. We do not put any up-front restrictions on the use of the logo. Any use of the logo is interpreted as an endorsement of our principles.
5. If we feel that somebody uses the logo in a way that is incompatible with our principles, we will ask them to take it down.

In other words:
* starting immediately, anybody can put the logo on any T-shirt, corporate home page, or product (following the above rules)
* if somebody puts it on a product that is antithetical to our principles, we ask them to take it down.

Things to do now:
* Put TM on the logo

* Add phrase “My data, my way” to the logo
* Put principles on new page on personal-clouds.org

Things to do later:
* talk to a trademark lawyer about whether it should be changed to a SM or certification mark, or be filed for an (R)
* encourage other companies to use the logo

Suggestions for doing better going forward:
* E-mail reminder for upcoming meetings 1 day ahead
* More in-person meetings

Cozy Cloud Mes Info

Wednesday 2J

Convener: Benjamin, Cozy Cloud

Notes-taker(s): Leon Brown

MES INFO

“If we have data about you, you have them too… To do with them whatever makes sense for you”

Idea to brainstorm with companies that have lots of personal data, see what we can do with it.

Concept: Try to implement concepts discovered in brainstorming year.

http://fing.org/mesinfos

Companies

Independent, all voluntary.

Need prezo or go to site for company list

Google is also participating, but mainly money, not data at this time.

Identify some values for customers

Gestion: Management

Controle: Control - who access

Connaisance De soi - safe knowledge

Conscience: Discovering what you are

Decision et action - can act

Contribute: be able to contribute

Lots of opportunities and risks noted - need slides

Companies are dot one, non-digital companies. Currently most participants disintermediated from the web/clients. There is mediation between the companies and the individual - this may have driven their participation.

We say - don’t try to imitate MINT or others, find your own way.

Give back the data to your users. You enter in to trusted relationship with your customer. Then ask customer to host a service on their (the customers) cloud.

This ‘app’ will provide a service that MINT cannot provide - all the data from the users, within their privacy sphere. Impossible for MINT to access all your data (like invoices, receipts), but by deploying your app on a customers personal cloud you have something that MINT can’t.

Who is financing Mes Info? The companies participating in the experiment + public contribution.

What does Mes Info feel like or mean to a French citizen? MY INFORMATION

From the start of the project, they wanted all sorts of data: mail, photos, history of vacation. This allows services that not possible in a MINT model

One insurance company is providing risk score to individuals

Jumping to COZY CLOUD

Why Cozy Cloud was selected?

Start: December 2012 to explain project. Project decided Jan 2013. Kick off End of October 2013.

Pitch

Cloud is great, but….

...data is new oil - it is the true asset.

Kept currently in web silos currently

Data access is an issue, and frustrating - A Personal Data Disorder as your data is across so many silos you cannot extract value.

Philosophy is that customers/users want to

Single Sign On, Search across all your data, Integration between walled gardens, Mash-ups of my personal data, and have privacy (post Snowden Era), a fundamental right

Answer

Have your data on your server. All your data held yourself you can allow sign-on, search across it, etc.

Difficulty

Data is complicated - much complexity

Cozy - Your Personal Cloud

Your Data, Your Apps, Your Server

Can deploy on your own server, in AWS, in any place

Demo

You sign-in to your cloud, has human readable name, maybe

Reach Your Home which shows the Apps on your server.

Can add ‘apps’ from the marketplace - an app marketplace

Deploy an app on your server

Deploy a photo app - asks permissions for authorization

Server then runs the service on your server. Apps do not access the service - it works at home on your server

All apps are competing for RAM and CPU on my local server. Cozy provides app management to

slowdown/shut down unused apps

Note Taking App Demo

At install asked for rights to access my contacts

Different from other apps, this Note app can add a reference to an actual contact.

You can add a reminder

Cozy provides a set of inter-app communication protocols so a developer could build a To Do list that calls and/or updates information from the Task list (webOS -like in inter-app communication)

Commentary: Overall the magic is in the Mes INFOS project is getting all the companies on-board to give data back to the consumer.

Others parrot this concern/interest

Why? Banks, insurance, post office are interested in (1) any laws of giving data back to the consumer and (2) seeing what developers might do with this data.

Commentary: Interesting is that the framework pushes running the apps on a local server. The architecture requires running an app within the Cozy Cloud server.

Workflow

Email invitation

Kicks off link to start up

Opens a Server in OVH - a kind of rackspace, a host company

Machine opens up in OVH - not fixed size. Elastic.

Includes Disk/storage of 50MB

If user Opens Contacts,

In customers virtual machine: Linux, Cozy, the Notes app/service on top.

Notes data goes into storage area. Storage area is in the VM image.

In OVH today, but could go in users home

Could mail a Box with service

What about static IP? Using ‘Gandi’ a dynamic DNS registrar to provide unique IP

Cozy Cloud is a Personal Cloud Provider

Data - is in Cloud (OVH storage)

What format is all stored in? Is it readable?

Question: Why but your IP in to connecting data/usage between apps?

Architecture - add picture

Each app can have access to data via simple REST requests.

‘data system’ in Architecture diagram reminds me of LunaBus in webOS. Allows app to x-talk and share data.

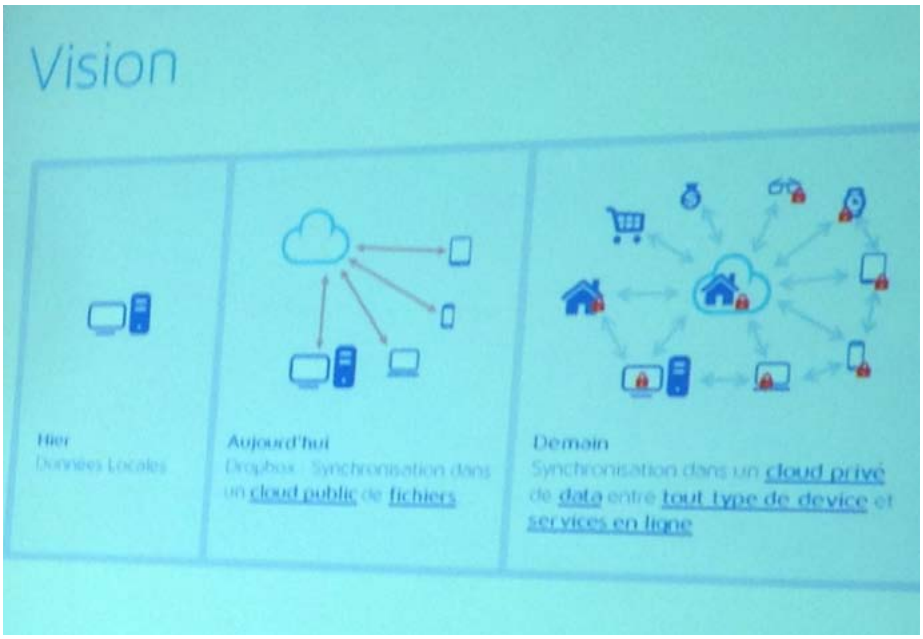
Indexer is Whoosh

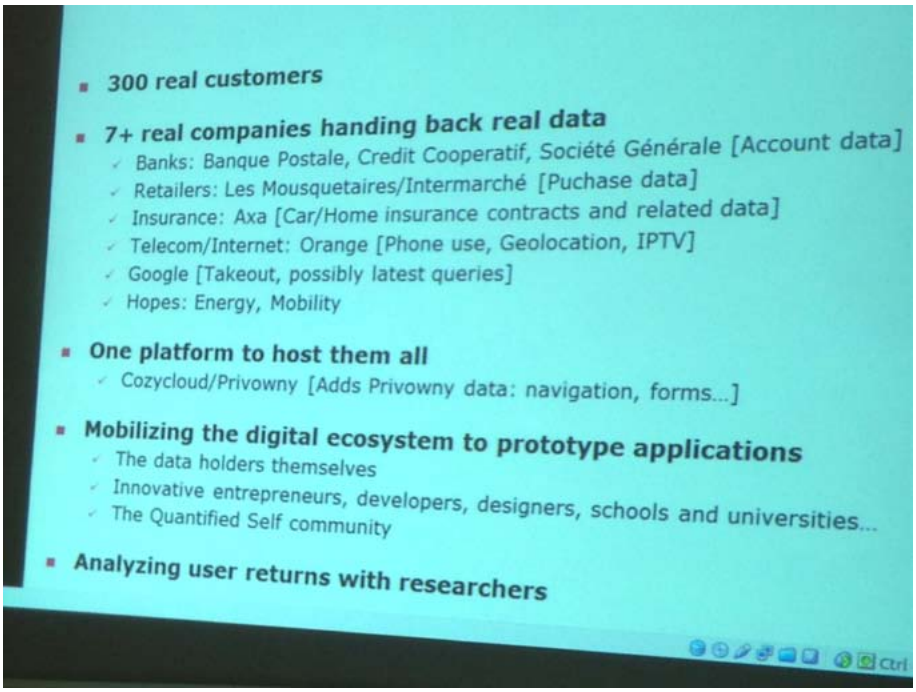
Privacy is today simple: One user, one server. Not multi-tenant at this time.

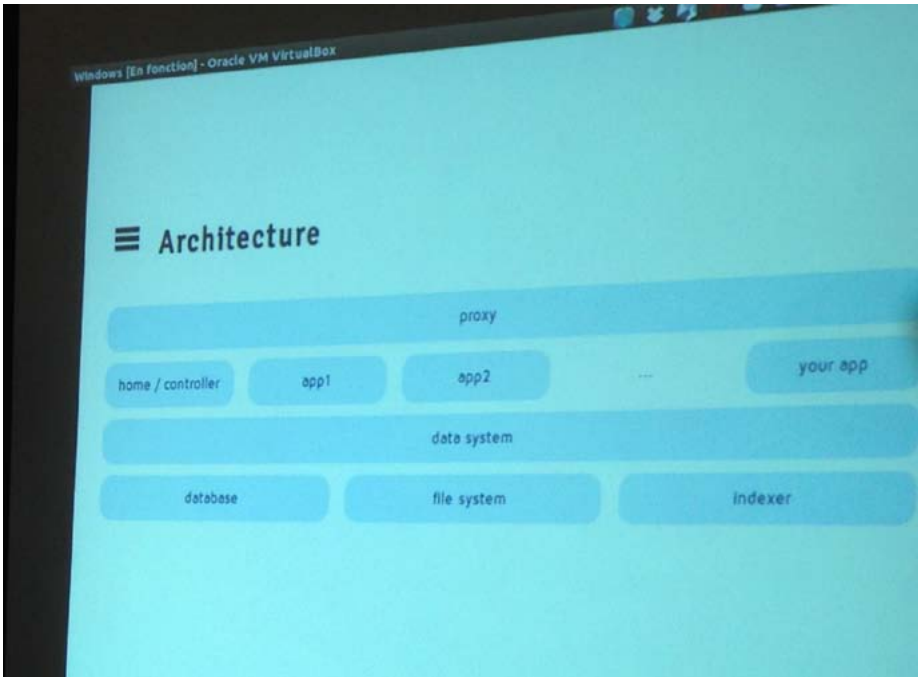
The 300 people in Mes Infos

Is there any administration? If there a user issue or could they blow away their own data.

Some screen captures







Building Personal Cloud Applications Fuse

Wednesday 3B

Convener: Phil Windley

Notes-taker(s): Phil Windley

Here's a slideshare of presentation available here:

http://www.slideshare.net/windley/fuse-technical

FCXX Update – Federal Cloud Credential Exchange

Wednesday 3G

Convener: Joni Brennan /James Shiere

Notes-taker(s): Joni Brennan

Overview of FCCX History, Vision, and Structure:
James Shiere provided an overview of the Federal Cloud Credential Exchange structure and high level goals. The structure was put in place to enable easier on boarding of US Federal Agencies (RPs) to connect with Approved Credential Service Providers aka CSPs (IdPs). The project is an activity that is driven by NSTIC NPO, ICAM and USPS. USPS is the contract manager who put out the RFP and awarded contract to SecureKey to implement the FCCX.

Assurance Program to Join FCCX:
Joni Brennan provided an overview of the Assurance Approval that CSPs who would wish to prove eligibility to FCCX. Once a CSP has been approved by a TFP (Kantara Initiative for example) that CSP is eligible to be consider for addition to GSA procurement list. GSA ICAM has final authority to make judgment regarding the approriateness of an IdP to connect to FCCX. One Example of this type of situation: an off-shore gambling site may be able to meet the criteria and requirements as laid out by ICAM and organizations like Kantara Initiative. However that type of organization may be deemed inappropriate for connection to FCCX based on context of their services.

Current Progress:
FCCX is on track to launch in January of 2014. Previously TFP approved CSPs are very likely the first candidates who will be considered for connection. Kantara Initiative has approved 3 high assurance providers and one low assurance provider. The list grows.

Comments:
“It would be great if the health care industry could make use of something like FCCX.” While it is possible that FCCX may extend or that new iterations of FCCX like services may be created there is currently no clear answer regarding possibility to extend FCCX for health care industry scenarios. It’s something to consider and discuss further.

Joni Brennan may be contacted for further information and interest - joni@ieee-isto.org

Anonymous Authentication

Wednesday 3H

Convener: Kazue Sako

Notes-taker(s): Tom Brown

Presentation slides are available from the convener at k-sako@ab.jp.nec.com

Issuer, claimant, verifier

Verifier checks claimant has claimed attribute without learning identifier of the claimant.

Issuer vouches that attribute belongs to claimant but won't know that claimant is buying beer.

Even if the verifier and issuer collude, they cannot identify claimant

blind signatures

group signatures

ring signatures

zero knowledge proofs

ISO IEC 20009-3

ISO IEC 29191

ISO IEC 20009-2

2 Types of verifications

Level 2: Verify that this claimant belongs to the group

Level 1: Who in the group performed the transaction (privileged operation)

Merchant can validate credit card information without learning credit card number

The issuer can also be anonymous to the verifier

Ontology for the Personal Data Ecosystem

Wednesday 4B

Convener: Joe Andrieu

Notes-taker(s): Lionel Wolberger

The need for a well defined lexicon was presented, and progress was made towards specifying that lexicon.

THE NEED:
A “Build Or Buy” report is being drafted by PDEC. The report enables PDE solutions providers to both discover providers of needed functionality, and announce their value proposition so others can find them. The solutions will be stored in a database. The database stores RDF triples. An RDF triple is a statement about a particular solution with a subject, predicate and object. For example, we looked at personal.com and generated the following RDF statements:

```
:personal p:name “Personal” ;
      a p:company ;
      p:legalName “Personal, Inc.” ;
      p:url <http://www.personal.com> ;
      p:offer :personalService ;
      p:offer :fileThis ;
      p:tagline “All life’s details in one secure place” .

:personalService a p:personalDataStore ;
      a p:softwareAsAService ;
      p:has p:accessPoint ;
      p:has p:accessRules .
      p:has p:authorizationManager ;
      p:has p:consentManager ;
      p:has p:personalAssetStore ;
      p:has p:translator ;
      p:name “Personal Service” ;
```

MAKING PROGRESS:
It was decided that in order to generate the well-defined terminology, we need to express the goal of the exercize. Participants generated goal statements, that were then inspected and a collective goal was formulated.

GOAL:
Generate agreement on a common model and vocabulary of the personal data ecosystem to enable adoption, collaboration and competition

NEXT STEPS:

To recruit a small group of people ready to work on the ontology, generate and close the lexicon that will be used in the report and database.

RP Challenges to Federated Login

Wednesday 4D

Convener: Jack Greenberg

Notes-taker(s): Jack Breenberg

This session centered on issues that Relying Parties face when they begin to implement several "Sign in with ___" options on their sites to increase security and ease of use. For new sites, there may be a concern about UX.

How does the site look to a new user?

Is it clear how to login or is it stressful for the user to understand what is required?

Can users with email addresses from non-IdentityProviders (many ISPs) still create passwords?

There could also be issues on re-visit. If the user clicks a different button than they did the first time, even if it is for the same email address, does he/she now have two accounts or does the site link them in a smart way to verify the user has control of both IDPs? For existing sites, the migration story of moving users off of passwords and over to Identity Providers can be cumbersome.

The group discussed how sites handle these issues, and I offered suggestions based on lessons learned at Google with our Identity Toolkit project, where we develop tools to make tackling these problems as easy as possible. Discovering a user's possible IDPs came up as well and we talked about how the OpenID Foundation's AccountChooser.com project might help in this respect.

Finally, we had a great conversation toward the end about how smaller IDPs can become visible and mentioned that compliance with OpenID Connect's upcoming standard will likely be helpful when "selling" your IDP to RPs because there will likely be libraries for many platforms that make implementing OIDC-compliant IDPs trivial.

RP Challenges to Federated Login

Wednesday 4D

Convener: Jack Greenberg

Notes-taker(s): Jack Breenberg

This session centered on issues that Relying Parties face when they begin to implement several "Sign in with ___" options on their sites to increase security and ease of use. For new sites, there may be a concern about UX.

How does the site look to a new user?

Is it clear how to login or is it stressful for the user to understand what is required?

Can users with email addresses from non-IdentityProviders (many ISPs) still create passwords?

There could also be issues on re-visit. If the user clicks a different button than they did the first time, even if it is for the same email address, does he/she now have two accounts or does the site link them in a smart way to verify the user has control of both IDPs? For existing sites, the migration story of moving users off of passwords and over to Identity Providers can be cumbersome.

The group discussed how sites handle these issues, and I offered suggestions based on lessons learned at Google with our Identity Toolkit project, where we develop tools to make tackling these problems

as easy as possible. Discovering a user's possible IDPs came up as well and we talked about how the OpenID Foundation's AccountChooser.com project might help in this respect.

Finally, we had a great conversation toward the end about how smaller IDPs can become visible and mentioned that compliance with OpenID Connect's upcoming standard will likely be helpful when "selling" your IDP to RPs because there will likely be libraries for many platforms that make implementing OIDC-compliant IDPs trivial.

Omie Update (Version 2.0)

Wednesday 4F

Convener: Doc Searls

Notes-taker(s): Bill Wendel

bit.ly—OmieUpdate

What is Omie?

Pull quotes from Omie home page

What defines an Omie?

At this stage we don't propose to have a tight definition as the project could evolve in many directions; so our high level definition is that an Omie is 'any physical device that Customer Commons licenses to use the name, and which therefore conforms to the 'customer side' requirements of Customer Commons.

Version 1.0 will be a 'Customer Commons Omie' branded white label Android tablet with specific modifications to the OS, an onboard Personal Cloud with related sync options, and a series of VRM/ Customer-related apps that leverage that Personal Cloud.

All components, wherever possible, will be open source and either built on open specs/ standards, or have created new ones. Our intention is not that Customer Commons becomes a hardware manufacturer and retailer; we see our role as being to catalyse a market in devices that enable people in their role of 'customer', and generate the win-wins that we believe this will produce. Anyone can then build an Omie, to the open specs and trust mechanisms.

What kind of apps can this first version run?

We see version 1 having 8 to 10 in-built apps that tackle different aspects of being a customer. The defining feature of all of these apps is that they all use the same Personal Cloud to underpin their data requirements rather than create their own internal database.

Beyond those initial apps, we have a long list of apps whose primary characteristic is that they could only run on a device over which the owner had full and transparent control.

Use Case: Omie as "Home into a box"

Consumer benefit: OMie = Creates "Peace of Mind" to new homeowners

Omie: Different models / versions based on Household profile

Home ownership

Smart Home
Transition to Smart Home
Landlord Property management
Rent collection
New tenant “packages”
Disintermediation Box
Focus on reaching those homeowners, particularly 1st time homeowners, who intent to sell
Give neighbors an Omie Box?
For every home on the market, there are two in the Intention Inventory
Downsizing Box
85M baby boomers
Facilitate digital downsizing

Market potential
110 Million Households
Goal: Help homeowners manage homes, increase value
Ongoing, PICO-enable property manager / home inspector

Market segmentation / penetration strategy
Existing home sales: 5 million per year
Give away device as “closing gift”
Partner with insurance companies, inspectors, mortgage brokers, & real estate agents
Moves: 40 million per year

Potential Home Sellers (for sale by owner) = Intention Inventory
Make available to homeowners who may be considering selling their homes
Zillow: For every home on the market, there are two watching

BASICs: Preloaded on Omie
Issues
Who preloads
Cost to pre-load?

Static items

Digital record of real estate transaction
Contracts
Market brochures, fliers
MLS listing
User manuals of house
Room by room details
eg. Paint colors (PMS code)

Plans
Digitized layout
Digitized site plan
Electronic layout: Breaker Box
Public records: Solaris
Data in Solaris system (used in some states)
Rite of way

Legal documents
Deed
Condo docs

House history
Utility history
Repair history

Home Vault
Links to existing Personal Cloud vendor

Home Inventory

INTENTCASTING Functions / House related use cases
Transition relationship from old owner to new owner
Directory of past service providers from previous homeowner
Service requests
Pre-bundled special offers?

Test sales market

Make Me Move

Linked to Zillow

Geo-Fence bundled into Omie (BW idea)

PICOs

Prompt homeowner to issue IntentCasts based on Life Expectancy of building system, appliance, etc.

Relocation app / Should we move?

Relocation scenario builder

TLC = True Living Costs

Issue buyer-slded IntentCasting

Pre-bundled Apps

Option: Give away Omie

Pre-bundled with apps who pay for preferred placement (free trials)

Different pre-bundle for different market segments

1st time home sellers

More than 70% of 1st time homeowners consider selling “for sale by owner”

App Store

Upgrade path

VRM communities

Functionality

App Store

Remote Property Management

Intergenerational User Interface

Home Warranty Repairs

IoT: Internet of Things

Pre-bundled

Give away Omie

Pay for Placement

1st time home sellers

Check home versus public records

Data Streams: My Home (Consumer Benefits)

Utilities
Ability to monitor monthly / seasonal utility costs
Make recommendations to reduce ownership costs
Mortgage
Monthly updates to home value
Monthly updates to home equity
Auto-payment
Equity Acceleration
Option to make extra mortgage payments
PICO Home Inventory
Shelving / Inventory
Shopping alerts
Home maintenance alerts
Declutter #TossTags

Data Stream: My community / neighborhood / street / neighbors (Community Benefits)
School related data streams
Crime stats
Social capital: donate to Customer Commons
Public incentives / subsidy alerts
Incentive systems offered by local governments
Home improvements
Energy improvements

Benefits
Customer control
Privacy & security

NEXT STEPS:
11/6-11/12: Attend National Association of Realtors Convention
11/6: Real Estate unconference
11/8-11: NAR Exhibitor Hall (shop for partners)

My Identity Your Identity

Wednesday 4I

Convener: Gihan Dias

Notes-taker(s): Animesh Chowdhury

An exploration of peer to peer identity for humans

Two main modes of how one's identity is created and perceived -

1. Human beings get their identity from interaction with other human beings and organizations/groups that they belong to each person makes a set of claims which could be true or false

- these could be verified by

... govt

... employer

... friends

2. other people build profiles of a person

- Some of these claims could be verified by third parties and the subject as well

... both these profiles need to have selective visibility options as well as reviewable

Asserting claims and the capability to verify some or all of the self-made or third-party-made claims can be seen as a variation of a social reputation system

However reputation systems normally have a specific purpose - ebay sellers reputation, Yelp/Zagat reputation score for restaurants , LinkedIn endorsements etc. Can there be a more heneric social reputation system which can be applied in broader use cases ?

Also how to build this reputation score/s semi automatically?

A suggestion is to tie the score against a public identifier , like phone number, Email address, mailing address, a social login id etc. - builds up value/reputation over time

Exploring what attributes should there be for a social reputation scheme

- violence ... safe to be around

- financial

-appearance

- trustworthiness

Data and ID after Death

Wednesday 5D

Convener: Akiko Orita

Notes-taker(s): Akiko Orita

Tags for the session - technology discussed/ideas considered:

deceased, data, privacy, archive

This session started to review several cases of treatment of deceased users. Facebook has two options: “Memorializing” or “Removing” the account, only the former options are allowed to be requested by non-family. Google’s “Inactive Account Manager” released in April 2013, which enable users to reflect their will what happen to their account after their death. A user can set an alert notification followed by 3-12 months inactivity periods followed by two options; to be removed completely or to be notified to “trusted contacts” to share their data with.

We considered not only personal or public space but also “third” place where we have social activity there.

Our discussion expanded this issue to “Authorship” and “Archiving” of data. For example, my data after death may be personal data then , however, after a century, it will be historical data. Individual data is more important than aggregated data because it’s a story of a person. Archival data is valuable to family and society as well. Thus, it is necessary to consider how to treat non-physical, digital stuff after death.

Google’s OIDC Auth platform on Android, Chrome, iOS

Wednesday 5A

Convener: Breno de Medeiros

Notes-taker(s): Tim W Bray

Slides: https://docs.google.com/presentation/d/1RAa7fnVixnwjzxymbkMvgNR5srZyA17lr-bEsCR5li4/pub?start=false&loop=false&delayms=3000

OIDC is interested in mobile

Background (see slides)

Discussion of how they got this to work for Google apps on iOS. 1st G app on iOS has to get the credential via browser or native UI. Then it stores the credential in the keychain and subsequent G apps can use that without having to go to a browser or display any other visual artifacts.

Deep-diving on details of side-scoping & down-scoping

Points out that the technology Google used on iOS has nothing custom or privileged from Apple, so anyone else could in principle build something similar.

Discussion of the usefulness of ID Tokens in the cross-client auth scenario.

Google hasn’t published all the internal APIs on this yet, but think some of them will be useful.

OIDC thinking of adding a secret to a couple of OAuth flows to stifle some corner-case security threats: OAuth symmetric proof of possession for code extension.

Data and ID after Death

Wednesday 5D

Convener: Akiko Orita

Notes-taker(s): Akiko Orita

Tags for the session - technology discussed/ideas considered:

deceased, data, privacy, archive

This session started to review several cases of treatment of deceased users. Facebook has two options: “Memorializing” or “Removing” the account, only the former options are allowed to be requested by non-family. Google’s “Inactive Account Manager” released in April 2013, which enable users to reflect their will what happen to their account after their death. A user can set an alert notification followed by 3-12 months inactivity periods followed by two options; to be removed completely or to be notified to “trusted contacts” to share their data with.
We considered not only personal or public space but also “third” place where we have social activity there.

Our discussion expanded this issue to “Authorship” and “Archiving” of data. For example, my data after death may be personal data then , however, after a century, it will be historical data. Individual data is more important than aggregated data because it’s a story of a person. Archival data is valuable to family and society as well. Thus, it is necessary to consider how to treat non-physical, digital stuff after death.

Venture Free Start-Up Financing

Wednesday 5J

Convener: Kevin Cox

Notes-taker(s): Kevin Cox

Tags for the session - technology discussed/ideas considered:

Startup Funding, prepayments, non compounding finance, credits for payments

To handle small payments efficiently a vendor can ask for customers to prepay and to buy Vendor Credits. This is like a prepaid phone card - but with some differences. The credits never expire and if they are not spent then the customers receive Reward Credits. Reward Credits do NOT earn more Reward Credits. A vendor will offer Rewards commensurate with the risk of the business not being able to supply the services. Typically this will be around 20% per annum. Credits and Rewards Credits will increase with inflation. Increases in credits will be made each day the Credits are unused.

Credits and Rewards Credits are transferrable and can be sold in a market place established by the vendor.

If a customer has too Credits they cannot use then up to 50% of new Credits sold by the Vendor can be sold by the Credit holder.

Rewards are not taxable if used for services because they are legally the same as a discount.

In most jurisdictions if Reward Credits are sold the income from the Rewards will be treated as a Capital Gain.

Credits are secured against future production and in the event of the Company being wound up the Credits have the same status as loans.

Credits can be used to purchase services from suppliers - such as the Respect Network. Credits can be used by other vendors to sell goods on the Internet provided there is an agreement by the vendor.

Credits can be used by investors. They offer the equivalent of a 20% fixed interest on investment where the capital is increased with inflation.

Because Credits are used as the payments mechanism means that the operation and treatment is simplified.

It was suggested that the Respect Network could sell identity audit and security audit services and be paid in Credits from future income. In the case of pre-revenue companies the Credits will not be realised until sales are made but while waiting they are earning a good income.

The Respect Network could also earn income by monitoring and watching the Vendor Credits and could act in a similar way to ratings agencies such as S&P. These services could be paid by the Vendors in Credits.

OAuth 2 Interop Testing

Thursday 1F

Convener: Justin Richer

Notes-taker(s): William Lowe

Interop mailing list: Oauth-interop@elists.isoc.org

Oauth = framework for building protocols
Lots of protocols you can build using oauth
Focal point of OAuth: Reusability. Interoperability of concept, not necessarily technology.
Of all the components, what are you trying to interop?

Goal: bring your code, bring a test server, hammer against other servers. Testing will provide input for the test suite. Just about impedance mismatching. Error code testing. What errors are being returned in certain circumstances, and how are they formatted? Error returns. Are there silent drops or ignoring of errors?

Goal: Explicitly define what we're not testing. Not compliance testing. Not assurance testing. Detach implementation from compliance.

Goal: Test functionality with hints of security, but not testing security of code base in the grander scale.

4 points:
1. clients to authorization server front channel. Is it going through user agent? How does client talk to the server directly. 4 core flows using front and back channels.

2. Client to authorization server back channel.

Client when talking to authorization server has a number of ways it can authenticate. Secrets,

assertions, etc. To specify what you're interop-ing... Answer: What flow are you following? How are you authenticating?

3. Client to resource server: different kinds of tokens, while using same mechanism to get token, creates variability. In reality we've only seen bearer tokens. Although various types of bearer tokens.

4. Resource server to authorization server. Token validity.

Where things should fail, do they fail?
Errors:
bad redirect uri
Repeated code
Bad code
Expiring code
Scopes

Can we use user info endpoint test from openid connect test? Possibly if there is a defined test user API with specific test purpose. Needs more discussion to agree upon appropriate test suite.

Honing the Digital Unconference Structure

Thursday 1G

Convener: Matthew Schutte

Notes-taker(s): Matthew Schutte

We have a video of the session here:

http://www.youtube.com/watch?v=07GrbgcNal4

Summary:
Matthew Schutte has been working on a Digital Unconference Structure for the last few months at:

http://collaborativeinter.net

He is interested in building out this structure and making it available as a medium to foster collaboration between the members of the IIW community between Workshops, possibly on a monthly basis.

DIGITAL UNCONFERENCE

The basic components are:

A publicly shared Google Spreadsheet (Coordination Doc) for

proposing sessions

scheduling sessions

sharing links to the components for each new session

google doc or spreadsheet for text notes

google hangout link

hangouts on air / youtube video link

A google Hangout on Air

In the Coordination Doc we share:

the link for participating in the hangout +

the link for watching the live stream / video

For each new session, the host for that session needs to

create a new google doc or google spreadsheet

share that google doc publicly (and sets permissions to “anyone can edit”) - this step can be skipped if you “make a copy” of the current google doc and select “share it with the same people.”

share the link to the doc back in the MAIN Coordination Doc

create a Google Hangout on Air

share the link to participate in that Hangout back in the MAIN Coordination Doc (url can be copied from the location bar)

share the link to the live stream / youtube video in the MAIN Coordination Doc.

This structure enables:

multiple sessions to run simultaneously

10 people to participate at any one time in each session

an unlimited number of people to watch a session live (with about a one minute delay)

recording and publishing of videos from each session -- hosted on youtube

auto-caption of the audio content (this requires an extra step by the host after the conclusion of the event -- unfortunately, google’s servers typically need some time to process the video file before the author can use the “auto-caption” function)

Once auto-captioned, viewers can search the transcript of the video for specific words (using ctrl-F or Command-F) and can click those words to jump to any specific place in the video (to one second of resolution).

After a video has been published, users can edit any segment that they want and can share a link to that “highlight”. Two ways to accomplish this:

in youtube, you can pause the video at any point and use the share function to share a link that starts at that point.

with tubechop.com, you can set both a start point and an end point and share a link to that segment. However, sometimes tubechop fails to start at the desired “start point.”

Areas that need work:

Instructions

Instructions need to be made clearer for new participants -- including instructions for joining google plus, for those that are not yet members.

Larger Sessions

Larger sessions: management of larger sessions can be accomplished with a “fishbowl” configuration -- two spots (in the hangout) are left available at any time. Any audience member can jump into the hangout. When they do, an existing participant is expected to jump off and follow along on the live stream

HOWEVER, the live stream has a latency issue that can make this “jumping into and out of the live hangout” a bit awkward. The live stream tends to run about 60 seconds behind the actual hangout.

Highlight promotion

we’d like to see some basic functionality for allowing the crowd to indicate which highlights are the best

beyond that, we’d love to see some graph attribute based functionality that allows that “crowd filtering” to be based on custom criteria.

Can Identity Proofing Eventually Replace Authentication?

Thursday 1I

Convener: Rick Killpack - NetIQ

Notes-taker(s): Kirk Brown

Tags for the session - technology discussed/ideas considered:

Identity, Proofing, personas, contextual

Identity Proofing Definition – The “Who” of Identity. Pubblic or semi-public context-based attributes. Proofing means – compare the risk of who? To the risk to the resource in determining the appropriate authentication levels, forms/process. As well as the appropriate access (continuous, just once).

The value is – ease of use to the end user and reduces risk. Less need for layers of Authn.

Who you say you are? – prove it!

And prove it within a particular context based on risk levels of access.

Two step Authentication:

1st Step – Who are you? Or who do you say I am?

2nd Step – Prove it by ….

Why would I ask a user to prove something?

The user tells you who they are. Then you proof it (step 1). Then determine the strength needed of the proofing (2nd Step).

Would you treat an existing user differently? No, always assume it is a new user unless the user asks you to remember them.

Authentication vs ID Proofing

These are all Authentication (adaptive, risk-based, step up).

At HP the user says “Here I am” and the provider responds “Are you allowed to be here?

But there are some providers who don’t care. Like Loyalty Card (Safeway, CVS, etc.)

They don't check your driver's license (Step 2). In reality, nobody cares.

Identity Proofing is more about "Who you are not".

Identity Proofing types:

Knowledge based – focused about the person. What's your mother's maiden name, etc.

Attribute mashup – determines who I am. Like my AD group, personal data, context at that moment, etc.

Out-of-band – using data that is not normal. Such as banks use for fraud detection. You are asked to call back when activity breaks policy.

Most of these attributes the user has no control over. What if the user could choose their own proofing?

Example:

Make it easier to allow a student to pay tuition. Sally's grandmother wants to pay her tuition. Typical systms would force the grandmother to register and be associated with Sally.

Why should grandma need to prove herself to give someone money? Who cares?

Sally defined the contextual context and defined the security policy.

Grandma used her facebook ID. OAuth was used to define the attributes of the token.

Should Sally have control and define her own Authn policies?

Historic Process – Register + Sign In + Authn

Vs

Identity Proofing – User defines authn policy, attributes and ID Proofing type.

Analogy – Amazon Shopping

A new user can show as a "guest" on amazon. Add products to their shopping cart. They can leave the site and come back days later and their context and shopping cart are as they left it. Amazon remembers. Only when the user decides to "checkout" and make the purchase does Identity Proofing occur.

Implementation Ideas

Current method needs to be more circular. Possibly a policy engine that can issue a token based on user created policy. UMA tries to solve some of this.

Problems & Challenges

Persona mapping is difficult via a policy engine

Identity Proofing Value

Replace authentication with Identity Proofing.

How Do RPs learn of big account changes at an IDP like Google?

Thursday 2A

Convener: Eric Sachs

Notes-taker(s): Eric Sacs

Link to slide share: http://goo.gl/MpTVyG

Personal Cloud Network - Risk/Threat - Counter Measure Models

Thursday 2G

Convener: Dan Blum

Notes-taker(s): John Fontana/Dan Blum

The session started out constructing the following matrix. At the end of the session it was partially constructed. As such it is a useful starting point for developers of personal clouds and personal cloud networks, but must be tailored for each individual type of service, as they have considerable variations. Multiple tables are also required as implied under the risk column.

Discussion

An attendee asked - What aspects of this exercise are the same as for any personal storage or collaboration service, and what are unique to personal clouds?

This led to a discussion of personal cloud assumptions and variations that might affect the risk assessment.

Assumptions

privacy (users at center)

cloud portability if hosted - access from anywhere if not hosted

lifetime accessibility

user controls policy and sharing / security option

Personal cloud + network = centralization

Variations

self-hosted

cloud service

de / centralized registry.

common carrier

user or shared control

Threats	Attacks	Risks (or consequences)	Counter-measures
Insiders Users Family Friends Developers Malfunctioning apps CSP admins and priv users … **Outsiders** Intel agencies Cybercrime Regulatory change	Malware DDOS …	**Categorize under "to whom" (user, CSP, business?)** **Categorize under Loss Of** Availability Confidentiality Accountability Use control Reputation **And** Liability	• Good practice: cover many kinds of attacks • Encryption at rest and in transit • Back-up, geo-located • privacy by default • "idiot proof" UI (make the secure way the easy way); promote oblivious compliance Reputation service • audits and assessment (counter risks of integrity and confidentiality)

Privacy – Why Not

Thursday 3C

Convener: Morten V. Christiansen

Notes-taker(s): Tom Brown

There doesn't seem to be a business case for privacy. This is partly a consequence of history and infrastructure.

Can IDPs turn into anonymity protectors?

Privacy is grossly undervalued. We don't think of harms because they don't happen frequently enough. ("Black swan" events). We have short memories.

U.K (and also Denmark): citizens generally trust government and they are also most surveilled

U.S: citizens historically generally do not trust government.

Ponemon (Larry) Institute - privacy research

NY Times sells profiles of readers

disconnect.me gets hate mail even from small bloggers

disconnect.me is pay as you want

mobile apps - often you can pay for an ad-free version although it is a small minority that do

Silk Road & Tor

Pew Results: People's 1st concern is Facebook and Google. Last is government.

Insurance, advertising companies creating profiles from online data

It is social problems that need to be addressed more than technical problems

CloudOS Programming 101

Thursday 3G

Convener: Phil Windley

Notes-taker(s): Phil Windley

Link to presentation: http://developer.kynetx.com/display/docs/Quickstart

Trust Frameworks: Definition and Application

Thursday 3H

Convener: Joni Brennan

Notes-taker(s): Joe Andrieu

101 Definition

201 Application

(evolved from conversation)

A set of commonly agreed Legal, Business, and Technical rules for managing risk in the exchange of information, and the processes and systems that realize those rules.

Contextual

-- Legal

Contracts

Policy/Regulatory

-- Business

Trusting Partners

Entry barriers

Early Ante

-- Tech

Interop

Specifications

Verification

Enforcement

Services (action / operations)

vs

Paper (Vision / specification)

lifecycle?

Example Trust Frameworks:

FBCA (Federal Bridge Certificate Authority)

National Certificate Authorities

Respect Trust Network

AMVA American Association of Motor Vehicle Agency

Kantara IAF+IOP

InCommon

OIX (* lists trust frameworks)

ICAM

SSL/Certificates

PCI

Commonalities:

- A notion of Identity. both of the group and of participants in the group
- Roles
- Obligations
- Rights (maybe)
- Governance (change management)
- Risk management

Not a silver bullet

Starting best approach

OMB's LoAs (1-4)

NIST 800-63 Authentication Controls required by NIST

Trust is earned precisely to the extent that risk is identified, assessed, and managed. That is, the purpose of the Trust Framework is to manage or reduce risk.

Identity by Presence

Thursday 3J

Convener: Kevin Cox

Notes-taker(s): Kevin Cox

Tags for the session - technology discussed/ideas considered:

Single Signon, Federated Identity, Identity by behaviour,

This talk was a preceded in Session 1 Room I on day 3 titled "Can Identity Proofing Replace Authentication" which spoke of the need to build systems that made sense to the user. This means permissions and the underlying structure of the authentication system was apparent to the user.

This lead naturally to Welcomer which is one way such a system might be built. Also Welcomer is a method to build the backend to FIDO (IIW7 Day 2) and integrate the strong authentication of the person to the device. It is believed that FIDO deployment will be accelerated with a Welcomer (or similar) backend system as it solves the problem identified in the session of an easy way for a device

to be the tool for multiple personas.

The Welcomer product enables the history of a user's interactions with websites to be built up incrementally and "automatically" classified and remembered as the user interacts with different websites. This happens because each Welcomer enabled website has its own memory of user interactions. This occurs through by creating a CloudOS pico for each user/device/website interactions. User inputs at each website is put into this CloudOS pico.

In the Cloud each of these pico's are connected through the user. That is, the links between picos is the user rather than the device and the website. This creates a network of picos for the user. It is this network of picos with pieces of memory that is the identity of the person. This approach is in contrast to the normal approach with personal clouds where most of the information is aggregated in the user's own personal data store.

While it was not described in the talk the website can establish links between each pico on its website and with other websites it controls.

The advantages of this approach are the simplicity of implementation because there is no need to move large amounts of data around the network, to set up complicated authorization and permissioning, because everything that can be shared is stored in the pico and the user and the website have joint control over how that information is shared and each has to give permissions for transfer to occur.

The discussions were mainly around the practicalities of this approach and the difficulties of the user understanding what was happening plus the reasons on why a website would implement such a system on their website. In particular these were around different personas on the same device. However, this particular problem will be removed by the integration of FIDO with Welcomer. This was not emphasized in the talk.

In writing up these notes I realize that it is the memories of interactions with the website stored in the picos and the links between the picos that is important - not the mechanism for interaction. That is the system works if the system uses Single Signon, Respect Connect, or Federated Identity. What was being illustrated is that these other mechanisms are not needed to move data between websites under the control of the user.

In practice a website will offer the different methods for a person to announce who they are. However, it is believed that most websites will move towards FIDO plus Welcomer style backend because it is simpler for the end user and the underlying structure maps directly to the user's experience.

The user will interact with a website and have available the previous memories of visiting the website. The permissions granted will only refer to the memories available to the person and can be fine grained. There will be no permissions granted that are not obvious to the person.

The important lessons for the presenter and was to concentrate on the "automatic" permissioning by the behavior of the person. That is, as a person moves from website to website they allow information stored on previously recently visited websites to follow them around and hence automatically grant permissions. By keeping this principle in mind the systems will be easier to understand and hence easier to use.

A blog post that expands on this issue can be found here.

Rallying Cry and Guiding Principles

Thursday 4F

Convener: Matthew Schutte

Notes-taker(s): Matthew Schutte

Mechanisms that have traditionally functioned well to balance privacy and transparency have begun to break down in the face of technological advances. One way that we could phrase this is:

digital developments have perverted the structures that we live within.

The people at IIW tend to be focused on finding was to shape emerging digital structures to help restore, and possibly improve upon, these balancing mechanisms.

Some of the concepts that seem central to the IIW community:

agency

persistence and revocability

anonymity and pseudonymity

trustworthiness

privacy

reputation

trust networks

context

authentication

gossip

identity as a tool to enable community

rather than “trust” or “trustworthiness,” Alan Karp encourages us to use a different term, something like “vulnerability management.”

A rally cry and guiding principles should help provide clarity to those working within the community and foster cooperation. In addition, it should resonate on an emotional level beyond the community so that we can better communicate with the rest of the world about what we are working on and why it is important.

A good rally cry will not be all-encompassing and will not be accurate. However, it should hit at the heart of what drives this community.

Obviously, there is a diversity of views within this community. However, there is significant overlap concerning our overarching goals.

Some stabs at a Rally Cry:

make trustworthiness on the internet function more like a village than a city

Trust. Worthy. Internet.

villageffy the web

identity as a tool to enable community

Come to the Movies! User Managed Access (UMA) Demo Video Viewing and Discussion

Thursday 5A

Convener: Andrew Hughes, Will Lowe

Tags for the session - technology discussed/ideas considered:

UMA, OAuth, Protocol, Privacy by Design

Eve Maler, Thomas Hardjono, Domenic Catalan and Mike Schwartz joined the session by Skype Video – we used a second projector to see them.

We reviewed the "UMA 101" slide deck that introduces UMA, Some of the powerful reasons to use it (versus straight OAuth).

We viewed the UMA Demo Video 2.0 and discussed viewer's impressions and suggestions for improvement.

UMA 101 Slide deck is at: tinyurl.com/umawg

The Beta v2 of the UMA Video is at: http://www.youtube.com/watch?v=1-iLjajOGJs

Cybernetics, Augmentation & Identity

Thursday 5C

Convener: Michael Lewis

Notes-taker(s): Michael Lewis

Tags for the session - technology discussed/ideas considered:

cybernetics, augment, identity

Cybernetics & Identity

no attendees, so I'm posting these notes as the ideas that caused me to suggest the topic.

Motivation

Can users be taught the necessary concepts in ID to become informed users?

Some already consider humans to have enhanced memory by virtue of their smartphones, etc.

Q1. Is 'augmentation' necessary for a strong user-centric ID ecosystem?

Q2. How do we treat peripherals that enhance human memory or cognition, in a strong user-centric ID ecosystem?

Necessity

(Most?) People have a natural facility for taking on different personas, but when it comes to formalizing this process very few yet comprehend all the issues. E.g. taking on a psuedonym:

why we do it

when it is appropriate (social norms, legal issues)

when it works

how to defeat anonymity

Since formalizing this process is a goal of (e.g.) NSTIC, people will either have to become educated about these issues, or be comfortable with someone else making policy decisions for them (be it friends/recommendations, a competitive markeplace, user-agents, well-meaning corporations).

Q3. Can we educate all people enough that they can make meaningful decisions about identity?

Q4. If we can't get everyone, what do we do for those who can't?

Q5. Do I need a User Agent to manage my PII?

Q6. Is that agent monolothic thing, or is it upgradable with e.g. a new protocol for understanding bank statements?

[Bonus Q. Is identity a universal concept? If not an internal decision, then can (must) it be imposed from the outside? E.g. anyone claiming that they don't have an identity is disavowing all responsibility for their actions, and can't be treated the same way we treat 'normal people' (i.e. people who agree to the usually-implicit social contract).]