Internet Identity Workshop 15

Book of Proceedings

www.internetidentityworkshop.com

Compiled by
KAS NETELER, HEIDI NOBANTU SAUL AND EMMA GROSS

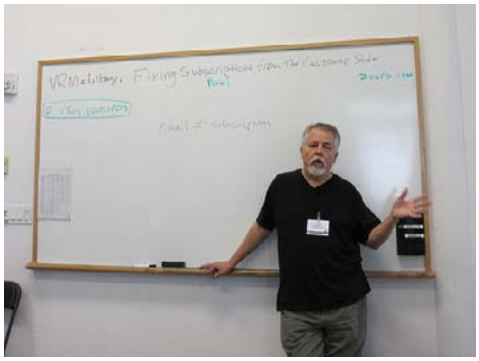
Notes in this book can also be found online at
http://iiw.idcommons.net/IIW_15_Notes

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

October 23-25, 2012
Computer History Museum
Mountain View, CA


Contents



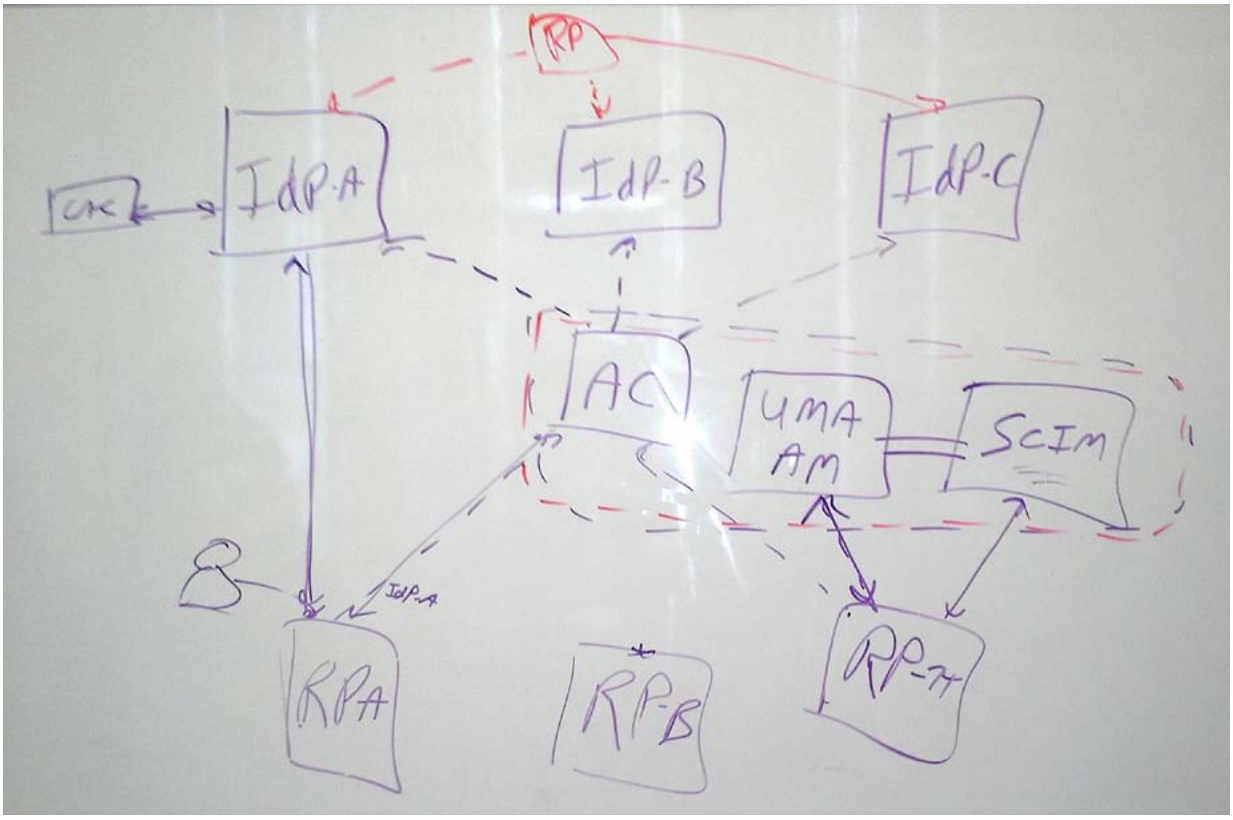


Identity Clearing House

Tuesday 1A

Convener: Justin Richer

Notes-taker(s): Amanda Anganes



Goal: Building a collaboration environment at MITRE.

Ideas:

1) variable levels of control/security tied to different accounts

* Employees using companiy-issued credentials

* Government personnel using CAC

* Invited partners

* Collaborators

* the general public (registered)

Anyone logging in may have multiple accounts with different rights/permissions tied to them. Ex: General with a CAC account as well as Facebook or Google account. May want to log in with either to gain access to different levels of secured information.

2) Identity Clearing House: Account Chooser, allows users to authenticate using a variety of protocols. Entry protocol is translated into OpenID Connect on the wire, with additional attributes indicating which account the user logged in with. If user has multiple accounts, bound together, then if the user tries to access something requiring more security than the account they logged in with, system can

request step-up authentication for the user to authenticate with a higher-security credential.

Users with low-trust accounts (coming from an IDp we don't have a relationship with) could be vouched for by users with higher-trust accounts (gov't employee, MITRE employee).

Use SCIM to store attributes about the user.

User UMA authorization manager for 1) user control and 2) admin/enterprise controls

Another group in MITRE is building an authorization decision engine, which the UMA AM would refer to for decisions.

Goal of overall architecture is to make every piece optional - new apps looking to get on the network could opt-in to using any of the services. Ex, could manage local user accounts if they really wanted to, but option to use ID clearing house authentication would be available (and hopefully easier and with better support).

This is a work-in-progress architecture, looking for comments.

Question: how would we tie multiple accounts to the same person (FB, CAC, MITRE)? Thinking of using SCIM for an attribute store

---

Within the system, the ID Clearing House would allow RPs to not worry about the user. Authentication is delegated, authorization & access controls are all delegated and accessible for retrieving info about the user.

Suggestion: Binding multiple accounts to the same user sounds really complicated, why not just let the RPs do it individually?

Answer: goal is that RPs would not have to be that smart. ID Clearing House would take care of acct binding, etc so that RP can just ask the system what the logged-in user should be allowed to access/do.

Clarification: access/auth decisions are not centralized. Decision services are centralized, but it is still up to the RP to decide whether the returned decision is acceptable, or if they should take another action, etc.

Discovery is very important in this kind of situation

Question: What about BrowserId?

Question: Are people at MITRE likely to trust these systems and be happy to use them? Yes, we think so - already have OpenID 2.0 server, partially blessed by InfoSec, lots of folks are using it already and InfoSec actually likes it.

Also - everything will be open source. Want to play along? Get in touch with us!

Rhetoric, Stories, Explanation, Persuasion Language

Tuesday 1D

Convener: Phil Wolff

Notes-taker(s): Scott Mace

Phil Wolff: When we try to explain identity, people's eyes glaze over. Like weird sports with weird rules.

In England, the MyData meta initiative, a whole bunch of people are committed to helping the public access data like their health records. They're having problems with how do we talk to the public about this. These can be people who found browser back buttons frustrating.

We have a rich vocabulary of ideas. Startups share this problem. Personal data store startups are trying to describe things. A chunk of data can be called a gem but it sounds like a trademark.

Leon Brown, HP: We're trying to talk about the activities you would do. I have an easier time talking about wouldn't it be good if your records were something you had control of. Your medical records. All your supermarket shopping at the list item. Today you have loyalty programs, but it might be interesting to see combined views of family lists. Stories communicate better than the vocabulary. Do you really want to give out your credit card info to five Mint-like visualization companies? Better to manage your own info.

Joe Andrew, Information Sharing Workgroup: Working on an app to see what Web sites do with your information. Fear is a pretty good starting point for people who don't understand the technology. Do you know that Google keeps all your searches forever, and Facebook shared information with web sites without asking you? You agreed to this. They say "I hate XYZ" and we use that to continue the conversation.

Leon: Or you hear, great, I trust Google. Where's the bad part about Google.

Joe: We did some in the field research. There was a lot of cognitive dissonance. I've got things locked down but my friends are foolish. Or people who say they don't share anything on Facebook but I open their settings up and hear the opposite. People have blinders.

Eno [no last name given]: I told people I was coming to this conference on privacy and identity. People still are not thinking of it in terms of you have to prove who you are.

Leon: Is "on the Internet" critical to what you're describing?

Eno: People are more concerned with the online stuff. People are concerned about their personal info being used, a scandal earlier this year, people using fake SSNs to file their tax returns. When the people actually filed their tax returns, they hear "you already filed them." They found out who was doing it. It's a fear trigger.

Leon: It's an encumbrance to remember all these passwords. Is it finding a new way to express my persona?

Phil: The site remembers me. It's the counterexample to being challenged.

Kevin Marks: Sites in the European Union has to explain to users what cookies are.

Scott Mace: There's been extensive criticism of the cookie explanation, that it deteriorates quickly into legalise and gobbledygook.

Phil: Maybe there should be a category in next Webbies, best cookies explanation?

Jay Unger: I've been to Web sites where they try to explain all the difference techniques used to track users. Nobody reads it. We need language about the intent of the Web site or the relying party.

Joe: Who is a huge part of it.

Jay: My mother, all she really needs to understand is what is the intent? What are they trying to do for her or to her? I consult for clients. The first thing I do is put up a slide that says this is the terms of service. What do you think it means?

Kevin: Terms of service TLDR, the Web site that judges terms of service.

Leon: The vocabulary should be visual.

Phil: I wanted vocabulary when you were talking to an investor or a reporter about personal data. Or using words to talk to someone who is more orally oriented than visually oriented. I'm agreeing visual stuff is really important.

Jay: Even weak trust marks like TrustE didn't work either. To know what that trust mark means, you've got to read a six page document.

Joe: it doesn't give you any data behind it.

Jay: It's all descriptions of the accreditation process and the tech underneath it as opposed to intent. People want to know what you as a RP or a web site, what is your intent, what are you guaranteeing, not how you do it. Honestly, you're going to change the tech over time anyway.

Minoti Amin: It's all going to be tied back to what you get out of it.

Sara Smullett: How do we give people the language and knowledge about the space so they understand the value, and why is the exchange there? Most people don't see it as their problem. I can't get past the apathy.

Jay: Pew did a study about 10 months ago, looking at how people react to three types of privacy notices. They also noted HIPAA reaction. Same behavior.

Leon: It's low-key. Would people be more sensitive when it's higher value data such as healthcare?

Joe: In context you can pull it right out of them like Foursquare did.

Phil: In Cory Doctorow's new novel Pirate Cinema, a copyright law gets passed in England, three strikes and you're off the internet for a year. People lose their jobs. He talks about the consequences of not managing this resulting in pain.

Jay: On 60 Minutes the CEO of Axiom was telling Morley Safer what they know about him. In the next 2 years they will know 100 times more about us. Both Obama and Romney campaigns are mining big data for campaign purposes.

Leon: If an individual has access to copies of my data, what do I do with it?

Kevin: Can you end up editing it for accuracy?

John Fontana: Companies like Axiom and Google think in the aggregate.

Jay: It goes back to intent. Once data is released, it is difficult to control. If I allow Facebook or Google or Axiom access to my record, once it is released, even if I know the intent of the first party, what happens down the line?

Sara: What about sharing the information with the whole world? We're framing this conversation in terms of the user's relationship with the website or website with user, but it's a full mesh.

Phil: We'll all have these little angels whispering in our ears, which is different than how we normally interact with people. We don't have language to talk about what I know from personal experience vs. this new way. "If you behave badly, this will go onto your permanent record."

Jay: It's not much of a joke anymore.

Kevin: What has been rhetorically effective in this realm? Citibank ran TV ads to scare people into buying identity insurance. They ran an national ad campaign, saying you need to pay us for insurance. But they're liable, not me. But rhetorically that was enormously effective. The notion of identity theft is now popularized.

Leon: The idea of ownership and freedom, I control it.

Kevin: The app that showed everywhere you'd been on your phone. Google was doing it. All the carriers are doing this. But because Pete wrote the app, this took off rhetorically in a way that your phone knows where you are. But your carrier knows where you are.

Minoti: Carriers knowing where you are to adapt to—

Sara: identifying people after the tsunami in Japan.

Phil: Six manufacturers of pacemakers, none of them allow you to see your data. Their fear is a liability argument.

Jay: EHR a train wreck in progress. The path we've taken is antithetical to the user owning his own data. It's a situation now where hospitals dependent on EHRs, Minneapolis couldn't get data from my doctor.

Scott: Under Stage 2 of Meaningful Use, a reduction of Medicare payments is coming if data isn't being shared.

Kevin: Electronic Health Records in some cases are being replaced by Quantified Self. People are going around the organization to share with each other. Patients Like Me type Websites, even 23 and Me. People deliberately going around mandated privacy stuff.

Leon: I had a friend who died, a treatment optimized for my personal health.

Phil: There's the data I create, the data you create about it.

Joe: That's from Ian Henderson.

Leon: Volunteered, inferred.

Joe: The chair of the FTC says it needs to be as simple as the cereal box label. You can also look at it when you want it. You don't read the nutrition label every time you buy it.

John: A lot of people don't understand the nutrition label.

Wolff: Closing question. This time next year we might have more work done.

Leon: I would make it task based. Pick your topic and try to make it really specific.

Joe: Information sharing label. Go to www.standardlabel.org, sign up for mailing list there's a link to see the label.

John: I had to try to explain it in words. The metaphor sounds simple. Explaining it was more difficult. The experience of the user drops dramatically. Google: "Standard sharing label john Fontana."

Eno: I used to work at a senior center. There's advocacy groups, the AARP does stuff like that. They

could be a stakeholder. Here's how it could be better. There's particular groups to approach.

Sara: Not all consumers are the same.

Kevin: There is rhetoric going on there. They tell kids not to put their info online. School records, something else. Dichotomy.

John: The problem continues to magnify itself every time another company comes along with fancy marketing language.

Focus on Consumer Personal Data: Turning Fear into Excitement and Delight

Tuesday 1F

Convener: Peter Stepman

Notes-taker(s): Augustin Bralley

Tags for the session - technology discussed/ideas considered:

technology discussed/ideas considered: data types, risks, benefits, models, education, adoption, legislation, further sessions chosen

People don't think about how to use technology/data better
When we present options, people say, why should I trust you?

Volunteer Data - info you supply
Observed Data - Passive data you create, your digital dust
Inferred Data - merging the two
This categorization comes from the world economic report

Actively collected and Passively collected, top level differentiation

People are in denial?

There's a spectrum of awareness of what's going on with your data:
don't understand -> understand there is an ecosystem -> know full extent of ecosystem
Most people are in the middle-> searches are tailored to my data

Then there's the spectrum of care->don't care
Why is it hurting you?

Harvard Law school -> with the absence of harm, we're not going to get anywhere
The mechanisms of harm are not clear

Or incredible benefit. If we convince consumers before the harms hit...

Marketers say: you benefit from letting us have your data.

In general, businesses are not doing a very good job of letting people know what's happening with

the data. Worried that it would scare people.

Unless there is a legal infrastructure, businesses won't do it.

Or show companies that they could make more money with a VRM approach

The legislative stuff won't happen till 2017 at the earliest, what do we do until then?

Health records company
Strategy: free to certain people, nearly free to doctors; benefit: records transferred right away, cheaper. And by the way, this app is super secure.
Oh, and by the way, why not use this system for other stuff too?

Let's look at history:

Benefit and Harm: goes beyond monetary... what about the corrosion of trust, when people actually realize what's being tracked.

Target pregnant girl example: Target responds to creepy factor by filling with untargeted products

Control: whether or not you choose to share data

Does privacy matter anymore? New generations don't seem to care.
Freshmen and sophmore in highschool can no longer "start fresh"

We are not far into the "explosion of data as an asset"
What about the amazing opportunities that we've never had before?

Problem with "data as an asset" is that in fact the use value so far exceeds the sale value, that we ignore the use value.
With our healthcare data, etc. there's so much use value.

"Data is the new oil," is even worse.
There is enormous "value" in the data we have, use or otherwise.

Blue Kai profile, who's looked at it?
There's really nothing scary there, it may be wrong, that data is about you... its value to you is low, value to advertisers much higher.
It's the wrong data.

What this leads to is microsegmentation: "Market of one"
What about the echo chamber effect

Use case: Progressive sensor that you install in your car. Time of day you're driving, how often you brake, how far you drive. Direct correlation between personal behavior and value.
That's personal info, not personal identifiable information. Different value for both types.
Identity is the New Currency - Identifiable data.

The consumers data is being monetized by people in the middle (Blue Kai), not advertisers or consumers.
Works because people believe that marketing is effective.
Flip it-> if the consumers own the data and call the shots: show how this will be more valuable.

How can we leverage scale and the aggregate -> the co-op model?

Metaphor: Driving can be dangerous, benefits are obvious.
People know the risks, but they want the benefits.
But the risks are hidden.
Consumers don't really want to be educated.
We can only win with better benefits: convenience, e.g.

Education: how do you educate a moving target?
It's much more difficult to convince businesses than consumers
How to convince businesses to give up their data without regulation?

More sessions needed:
VRM Developer Roundup - Doc Searls
Business Models for Personal Data
Personal Data Types and Ownership - Kim Little
Personal Data Can Be Fun and Useful (benefits) - Peter Stepman
Personal Data Can Be Dangerous
Education - Alex Levin

VRM Challenge: Let's Fix Subscription Bin from Customer Side

Tuesday 2F

Convener: Doc Searls

Notes-taker(s): Augustin Bralley

Tags for the session - technology discussed/ideas considered:

technology discussed/ideas considered: VRM, CRM, subscriptions, FOSS,

History:
SMTP, POP, IMAP - free, open: replaced proprietary systems
There should be something like this for subscriptions
It can only be solved from the customer-side

Today: the full burden of providing a subscription is on the publisher-side
Some middleman options (Apple), but we shouldn't need to rely on them.

Pain point: NY Times. Old system, authentication hassles, ordering page (lots of form fields), bait and switch

Better solutions: when I'm at my apartment in NY, deliver me the paper, charge me.

Zuora.com -> interested in VRM on the sale side.

Related: How can VRM help CRM?

Possibilities:
1) New business that does nothing but subscriptions: gets large user base, goes to publishers and saves them the trouble of managing subscriptions themselves.
2) Open system, no intermediary. Ala email.

Google, instead of scraping for Google News, they could provide a publishing platform

Subscriptions are like futures contracts. Email is not that.
Let's QA the sell side.

Is all we can do is get better behavior from sellers?

Can we do with subscriptions what we did with email?
Email is a bad metaphor, because it didn't succeed, it's still broken.

Publishers don't want to give up the direct relationships with their customers.
Subscriptions for publishers are horrible, they hate them, don't know what to do with them.
Intermediaries are inadequate.
What can we do on the subscriber side, so that they are standardized, easier?
Getting new subscribers is difficult.

Are you talking about an aggregator?
You should never tell people how they should give you money, ie flexible terms.
Digital news stand, dashboard of subscriptions

Subscriptions have two parts: login and payment flow.
Can we standardize this somehow?

Protocol for matching VRM and CRM for subscription intent and payment processing?

Can sellers match the infinite intention possibilities?
No, we don't want sellers to each have their very own way of trapping you in, selling to you.
Protocols are agreements about how we're going to get along. Standardize.
Leave room for the heuristics on both sides.
Are there businesses that are confusopolies? Mobile carries, e.g.

If we bring more tools, capabilities, protocols to the user side...

Search and Invite model
How many people are there out there like this (anonymous)?
Extend an invitation to this person, with perhaps some constraints
Where does the protocol side end, and where does the business side begin?

The problems of publishers are pretty common.
Standardize the basics, variability on top.

Are we just going after the bait and switch model?
There are tremendous benefits to not playing games (coupons, loyalty programs, etc)
e.g. Trader Joes, Walmart

If you start with the complicated version, you're going to get a complicated solution. Let's start with the straightforward relationship with customers.
Related to the challenges of enterprise software. Successful companies are the middleware companies that are helping disparate systems connect.
What we're talking about is the bus layer between consumers and businesses.
You feed us this stuff, and we'll figure out how to route it

Information Logistics Platform
Middleware for People

Big premise of Kynetx, SnapLogic

CRM is about optimizing internal processes.
Not Customer Relationship Management, Customer Records Management

Once the middleware exists, companies will embrace it.

Maybe we should start with domain names, web hosting.
We want buyers to be better subscribers, give them more choices.
Sellers will find that cost of customer retention management will go down.

Not so much a technology as a business model issue.
Need to get a large user base, before sellers will pay attention.

Getting buyers preferences into sellers systems a challenge.

Helping buyers buy instead of just sellers sell.

HTML vs SGML
APIs are were SGML was.

Anonymous

Tuesday 2I

Convener: Kevin Marks

Notes-taker(s): Tom Brown

We assume we need identity for things to happen
But we're finding out this is not true
A growing culture of constructing meaning, ideas, culture and politics without identity
Examples: Anonymous, 4Chan

The only thing that persists from 4Chan is the ideas
Rise of leaderless orgs (Occupy, Arab Spring)
Now Arab Spring has structural problems with elections since there are no leaders

What does anonymity imply or enforce to the nature of the organization?
Scalability problems?

Anyone can claim to be part of Anonymous
It is not pseudonym because there is no correlation across time among posts

You're only as anonymous as there are other humans you can be confused with

A very messy consensus forming

Capital A anonymous refers to the emergent behavior
With instantaneous communication, some of this emergent behavior is now viable where it wasn't before

reference to recent Clay Shirky article: we can see waves of consensus emerging

As a channel becomes more mainstream, it becomes easier to hide.

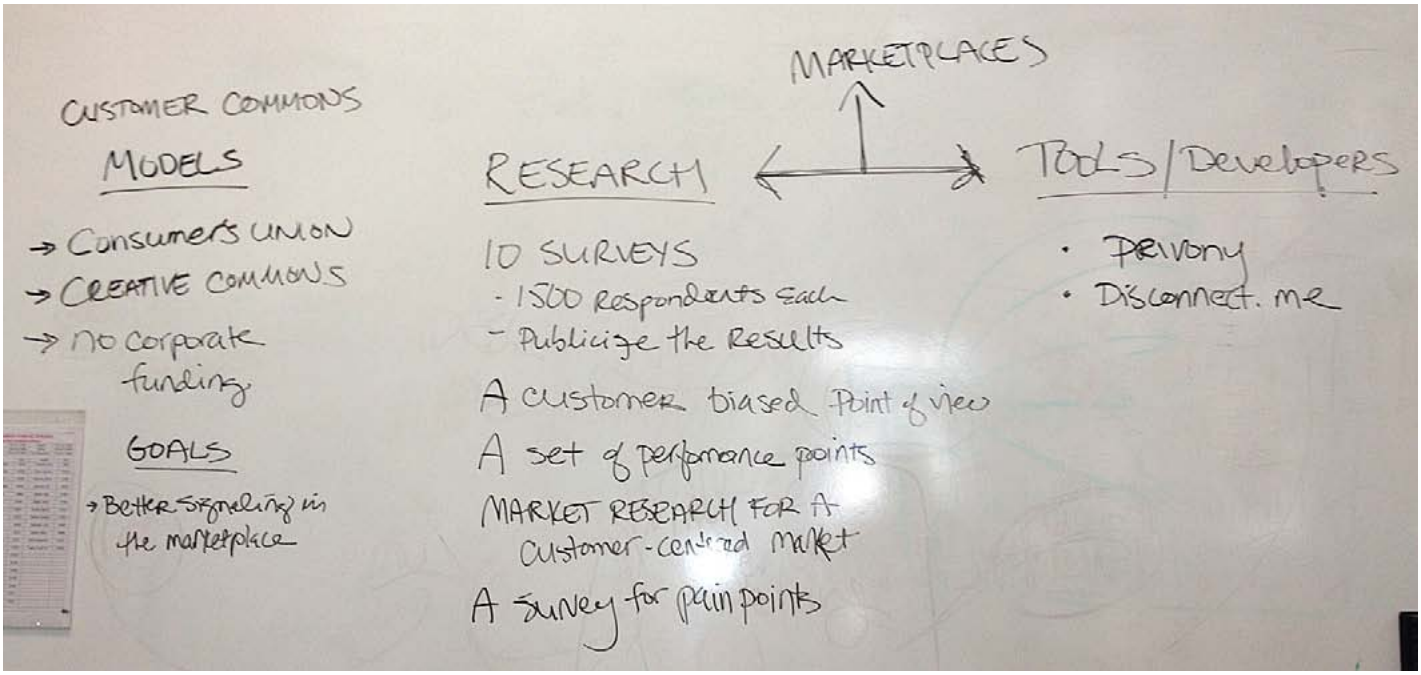
Maybe on reason we're not using signing technology adopted is we want a degree of deniability

Customer Commons + VRM Brainstorm

Tuesday 3F

Convener: Doc Searls

Notes-taker(s): Mary Hodder (photo)



OAuth Security

Tuesday 4A

Convener: Hannes

Notes-taker(s): Paul Madsen

Hannes set the context, explaining the current bearer security model

Hannes talked about multiple proposals for evolving beyond bearer, all more tightly binding the client to the access token presented to the RS

The proposals included

- MAC (Eran)
- SSL Binding (Hannes)
- JWT (John)

The above differ in the nature of the key (asymmetric or symmetric) and the binding mechanism (message or transport).

Phil pointed about potential issues with a web server clients using different keys for each access token it might be using to a given RS - is there an optimization possible?

Group reviewed the document by Hannes & Phil, which describes use case & security requirements

http://tools.ietf.org/html/draft-tschofenig-oauth-security-00

Distinction between a piece of client software (like a native app downloaded from App Store) and a particular deployed instance of that software was made. Sometimes an RS needs to know that a token is being presented by the latter (ie a particular instance as opposed to simply a member of the larger class.)

Distinction between identification & correlation was made. The latter is simply recognition that a particular request is being sent from the same client as seen before.

Discussion of client signatures getting broken by intermediaries - the more pieces of the message you sign, the greater the potential for breakage. On this issue, Chuck says 'dont sign fluff'.

Justin proposes revitalizing MAC spec.

Multimind

Tuesday 4C

Convener: Estee Solomon Gray, mmindd labs, @estee

Notes-taker(s): Darren Lancaster, mmindd labs, @thecommunityguy

Tags for the session - technology discussed/ideas considered:

UX

user experience

user value

multiminding

personal data

Opening thoughts

Transactional value vs. use value

Multi-device world is assumed, 2 often at the same time on the same task

Think about how you orchestrate your life, the tools you use, your digital and non-digital tools, how you achieve, how you manage your productivity, time, attention.

The opportunity: shift modes from multitasking to multiminding

Parents have one mind per kid. Minding a child isn't tasking, it's meeting and responding to needs, achieving outcomes.

Work mind: multiple minds per team member, projects, customers.

All these minds are open and active in parallel.

We're doing work that requires minding, not tasking. Achieving anything requires working through

others, interdependent work, not solo work.

Discussion

Why minding vs. roles? Health or self minds exist, but are not quite the same as a role.

Is this based on academic research? No, based on gender-based research and interviews. The background started from the perspective of reinventing health clubs. Surfaced tons of differences between how the genders manage their lives. Different attention patterns.

Design and discovery experience is required.

Mary: How men & women communicate, research in how women's vs. men's minds develop. Men killed the beast and communicated it. Women were exploring and gathering, communicating a longer story to other women to assist them. There was value in the different style of communications. Their survival depended on these various communication styles. Premise of mmindd labs is providing a more sociological identity; faceted identities. Going beyond just the technical terms of identity. Tools for men & women need to reflect our different operating principles and communication styles.

Drummond: Use a Word Doc to do my task orientations. How do I go from multitasking to multiminding?

Instead of a list, it's a bubble diagram. This is about what is my life's work?

We want to activate the visual mind vs. lists.

Is it about a better goal-setting mechanism vs. living in tasks? GTD (Getting Things Done) is about acting sequentially on a single task at a time. Assume "I" am the engine, but today, most often you achieve through others. We're embedded in teams and families. Loops allow you to achieve a higher intent and assume others are likely involved.

Can you populate the user interface passively? Calendar and tasking is most important personal data, secondary are contacts and relationships.

"You're almost an engine of nothing by yourself"

Drummond: Loops are called personal channels in the Internet Identity world.

Karen: people have told me that talking to me is like ping-pong. What gets lost is where I spend my time, real life patterns, helping surface where I WANT to spend my time. Is this the way I want to spend my life?

The biggest hurdle is inputting data. My data resides in lots of locations, but it's all probably accessible.

I have 13 different projects that I can't handle by myself. We've hit the wall on multi-tasking. Switching minds takes effort.

It's hard to stay in the flow state; easy to get into rabbit holes. Multiminding is tolerating living outside of the flow state as best as we can.

Others know your state, or mind, are you in maker mind, would be extremely useful.

Karen: I get into a better flow state if I'm able to hop around quickly.

Experience layers: will you be partnering with others soon to build these layers? Will you partner with others, like in real estate, to help people know they should consider a new location to move where they will be more productive. This is where this usage case meets transactional layers.

Why loops? Loops circle back, but it's not clear that's the right UI paradigm giving "moving forward". Loops are not specifically interdependent.

MMINDD

a new experience layer

calendars

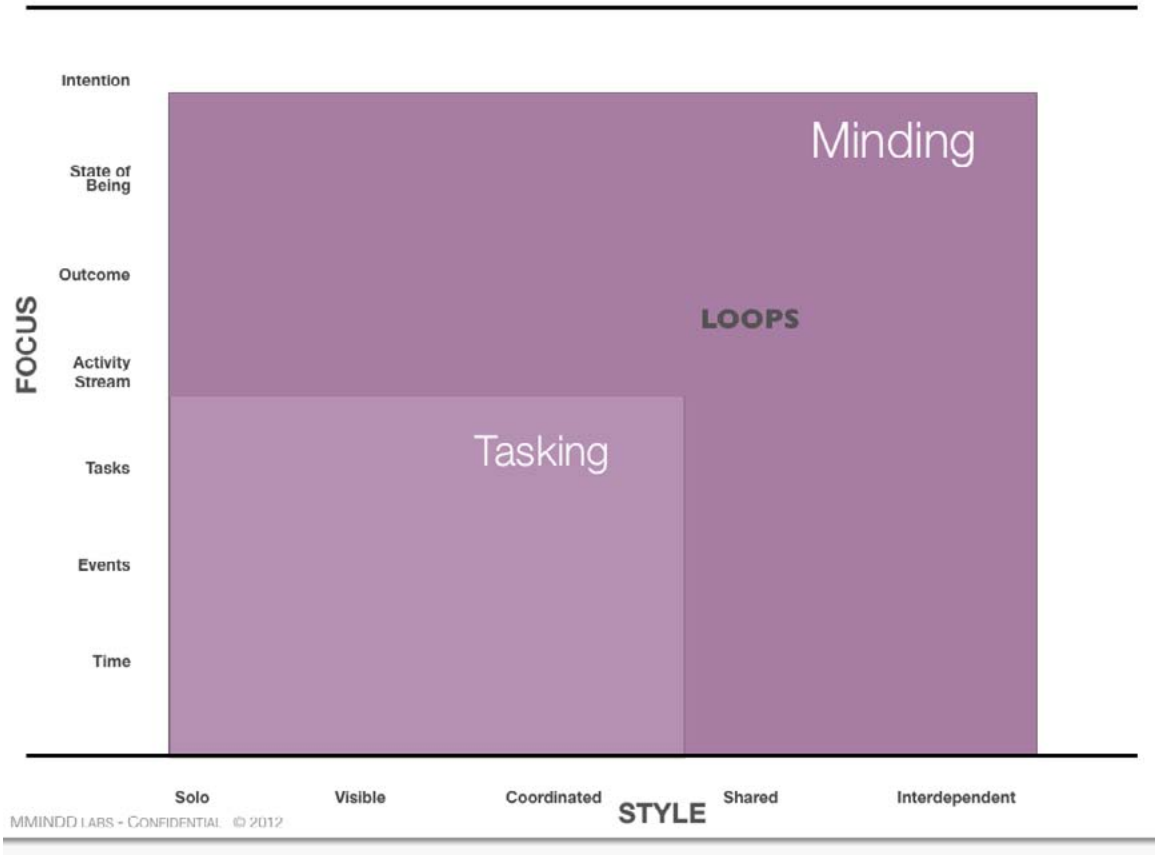
to do's

other personal data/streams

business data /streams

- visual
- gestural
- social
- mindful

attention management for **agile work/lifestyles**



Signing in Without Username and Password

Tuesday 5F

Convener: Steve Kirsch

Notes-taker(s): Jim Fenton

Tags for the session - technology discussed/ideas considered:

Authentication

Steve demoed OneID, an identity service that doesn't have usernames. OneID identifies and authenticates the user via public keys stored on their devices. Steve demonstrated transfer of keys by scanning QR codes, and showed the several ways that OneID can authenticate users, with the addition of a second device for higher risk transactions.

Personal Cloud Desktop

Tuesday 5J

Convener: Markus Sabadello

Notes-taker(s): Leif Warner

Tags for the session - technology discussed/ideas considered:

XDI

- A personal cloud:

- XDI: A data model and a protocol. A way of storing data and exchanging data.

Can think of a personal cloud as an XDI store.

Have two things running on computer - XDI store, and desktop app that talks to that store through XDI messages.

Every XDI address is a valid URL. XRI2.

XDI messaging format is itself XDI, and thus can be stored as XDI, giving an audit trail of updates.

The personal cloud can have “connectors”, to make data from other services accessible through XDI.

Maps some external data source (e.g. Facebook), to XDI.

Requires a OAuth token, then acts as client of the external service’s API.

Q: How do you resolve schemas?

- Not called a schema, called a dictionary in the data store.

XDI dictionary is itself XDI, and thus machine readable, can be readable from elsewhere - has its own address. Globally addressable - anyone can extend anyone else’s dictionary.

Q: How is an individual i-number generated, or chosen?

A: Similar to domain name system, there’s a registry at the root.

xdi.org

http://xdi2.projectdanube.org/

Privacy by Design Documentation for Software Engineers – New OASIS Technical Committee

Tuesday 1C

Convener: Dawn Jutla and Craig Burton

Notes-taker(s): Dawn Jutla, Peter Brown

Tags for the session - technology discussed/ideas considered:

Privacy by Design; OASIS Privacy by Design Documentation for Software Engineers; PbD-SE; Data-as-currency; Personal information-Free Rider Issue

Dawn Notes:

Dawn spoke about the OASIS TC on Privacy by Design Documentation for Software Engineers that she recently convened. She mentioned the TC's initial seeding of ideas around embedding the 7 Privacy by Design principles, ranging from a positive sum scenario to user respect AND the 7 Cs principles (e.g. consent, confinement etc.) as user-centric privacy requirements. Further the TC will be looking at generating privacy by design documentation using modeling and programming languages. The TC's coverage will include, and is not limited to extending UML use case diagrams, scenario diagrams, class diagrams, and U/I diagrams to help software engineers embed privacy by design in their resulting software and services. Emphasis is also put on the use of systems analysis and design documentation to help software organizations show compliance to privacy best practices and regulations.

The group of approximately 16-20 people with active participation from John Biccum (Microsoft), William Yasnoff (Health Record Banking Alliance), Peter Brown (Independent Consultant), and Drummond Reed (Respect Network) discussed some drivers of new privacy requirements. The consensus was that people do not like that they are not getting sufficient economic benefit from third parties' use of their data. We do get free services in exchange (e.g. free email, free social network communication among friends and colleagues) but there is a perception that people are not extracting enough relative value from giving up their personal data as compared to the value that companies extract. We framed this concern as a Personal Information-Free Rider issue. Dawn mentioned that a positive sum scenario for privacy and the advertising business model in use today by popular Internet giants could be created. Peter Brown, passionate privacy advocate, exclaimed that she was perhaps being too polite!

In addition, we highlighted data-as-currency in future business models such as Drummond Reed's Respect Network where the free-rider issue may be rectified. As future collaborative action, Dawn invited the audience members to join the TC and to contribute further to the effectiveness of its output.

This session was a pre-cursor of a joint session with Craig Burton on Wednesday, W1F: Session 1 9:30-10:30, Room F on Identity and API Economy plus Privacy by Design. Please link to that session's notes for more information on the OASIS Technical Committee on Privacy by Design Documentation for Software Engineers and for a larger picture of the importance of embedding privacy by design in future business models.

ADDENDUM:

Below are convenient descriptions of the 7 Privacy by Design (PbD) Principles and the 7Cs Privacy Control Principles that lend to a User-Centric view of Privacy Requirements.

The Seven Cs (7-Cs) for User Privacy Control Requirements

The 7 Cs for User Privacy Control adopted three initial control elements (comprehension, consciousness, and consent), from Andrew Patrick and colleagues' research on human–computer interaction in privacy. Dawn added 4 other constructs from user behavior theories to round out the 7 Cs. Together they describe the ways in which users perceive they have some measure of privacy control; that is, through understanding, being aware, choosing explicitly, giving consent, adapting privacy rules according to context, setting limits, and anticipating the familiar through consistency. The 7 Cs are not restricted to the user interface. They can be embedded at the data and behavioral modeling stages of analysis and design.

CONTROL CATEGORY DESCRIPTION as adopted from [1].

Comprehension:

Users should understand how personal identifiable information (PII) is handled, who's collecting it and for what purpose, and who will process the PII and for what purpose. Users are entitled to know all parties that can access their PII, the limits to processing transparency, why the PII data is being requested, when the data will expire (either from a collection or database), and what happens to it after that. This category also includes legal rights around PII, and the implications of a contract when one is formed.

Consciousness

Users should be aware of when data collection occurs, when a contract is being formed between a user and a data collector, when their PII is set to expire, who's collecting the data, with whom the data will be shared, how to subsequently access the PII, and the purposes for which the data is being collected.

Choice

Users should have choices regarding data collection activities in terms of opting in or out, whether or not to provide data, and how to correct their data.

Consent

Users must first consent (meaning informed, explicit, unambiguous agreement) to data collection, use, and storage proposals for any PII. Privacy consent mechanisms should explicitly incorporate mechanisms of comprehension, consciousness, limitations, and choice.

Context

Users should be able to change privacy preferences according to context. Situational or physical context—such as crowded situations (for example, when at a service desk where several people can listen in on your exchange when you provide a phone number, or when you're in an online community chat room)—is different from when you perform a buy transaction with Amazon.com or in rooms with cameras (where digitization makes the information permanent and unmistakably you) and data context (such as the sensitivity of data, for example, health data) could dictate different actions on the same PII in different contexts.

Confinement

Users should be able to set limits on who may access their PII, for what purposes, and where and possibly when it may be stored. Setting limits could provide some good opportunities for future negotiation between vendors and users.

Consistency

Users should anticipate with reasonable certainty what will occur if any action involving their PII is

taken. That is, certain actions should be predictable on user access of PII or giving out of PII.

PRIVACY-BY-DESIGN's 7 Foundational Principles:

Proactive not Reactive; Preventative not Remedial

The PbD framework is characterized by proactive rather than reactive measures. It anticipates and prevents privacy invasive events, well before they can occur. PbD does not wait for privacy risks to materialize, nor does it offer remedies for resolving privacy infractions once they have occurred – it aims to prevent them from occurring altogether. In short, PbD comes before-the-fact, not afterwards.

Privacy as the Default Setting

We can all be certain of one thing – the default rules! The power of the default cannot be over stated. PbD seeks to deliver the maximum degree of privacy by ensuring that personal data are automatically protected in any given IT system or business practice by default. If an individual does nothing, their privacy still remains intact. No action is required on the part of the individual to protect their privacy – it should be built into the system, by default.

3. Privacy Embedded into Design

PbD is embedded into the design and architecture of IT systems and business practices. It is not bolted on as an add-on, after the fact. The result is that privacy becomes an essential component of the core functionality being delivered. Privacy is integral to the system, without diminishing functionality.

4. Full Functionality – Positive-Sum, not Zero-Sum

PbD seeks to accommodate all legitimate interests and objectives in a positive-sum "win-win" manner, not through the dated, zero-sum approach, where unnecessary trade-offs are made. PbD avoids the pretense of false dichotomies, such as privacy vs. security, demonstrating that it is possible to have both.

5. End-to-End Security – Full Lifecycle Protection

PbD, having been embedded into the system prior to the first element of information being collected, extends securely throughout the entire lifecycle of the data involved — strong security measures are essential to privacy, from start to finish. This ensures that all data are securely retained, and then securely destroyed at the end of the process, in a timely fashion. Thus, PbD ensures cradle to grave, secure lifecycle management of information, end-to-end. There can be no privacy without strong security.

6. Visibility and Transparency – Keep it Open

PbD seeks to assure all stakeholders that whatever the business practice or technology involved, it is in fact, operating according to the stated promises and objectives, subject to independent verification. Its component parts and operations remain visible and transparent, to both users and providers alike. Remember, trust but verify!

7. Respect for User Privacy – Keep it User-Centric

Above all, PbD requires architects and operators to keep the interests of the individual uppermost by offering such measures as strong privacy defaults, appropriate notice, and empowering user-friendly options. Keep it user-centric – respect for the user is paramount.

Reference:

[1] Dawn N. Jutla, Peter Bodorik, "Sociotechnical Architecture for Online Privacy," IEEE Security and

Privacy, vol. 3, no. 2, pp. 29-39, March-April 2005, doi:10.1109/MSP.2005.50

Peter Notes:

Presenters: Craig Burton, Distinguished Analyst at Kuppinger Cole, and Dr. Dawn Jutla, Sobey School of Business, Saint Mary's University.

Craig Burton (presentation slides here)

5 API tenets:

Everything and everyone will be API-enabled (28bn APIs by 2015), each with a provider (inside > out) and/or consumer (outside > in) type of API;

The API Ecosystem is core to any cloud strategy – Amazon stores 260bn objects; Twitter handles 13bn API calls/day; SalesForce over 50% of all traffic via APIs; etc.;

Baking core competency in an API-set is an economic imperative

Enterprise inside-out

Enterprise outside-in

Open APIs are growing in a "Cambrian Explosion", leading to great number and diversity of APIs available to work with. An intractable management problem in the API economy where thousands of APIs exist in a broken one-to-one or one-to-many publish-subscribe consumption model. Instead, what is needed is a federated, many-to-many evented API model where events automatically trigger a possible cascade of evented API actions. Implied in the automation are event managers that understand rule-based or semantic contexts. These event managers will manage event prioritization and will be needed in future cloud operating systems.

Clearly, the identity of people and things is an intrinsic part of the fix and the future many-to-many cloud-based solutions.

Concern about SAML because the identity model, as deployed on current, admin-centric systems, does not scale.

Dawn Jutla (presentation slides here)

We need to intentionally create a positive sum scenario for privacy, security, and the advertising business model. Several original diagrams illustrate how personal data profiles, in the example of the mobile space, flow among a stack of interdependent and partnering platforms, such as carrier networks, device, operating system, applications and apps, and marketing aggregators.

As governments adopt cloud solutions to lower costs, in many instances, citizens' data profiles remain vulnerable to collection by the stack of popular platforms residing between the citizen and the government online service. Furthermore, cloud vendors will voluntarily keep government cloud service instances separate. However, in many countries, does it mean that the service interaction will not be subject to personal data leakage as occurs similarly in the consumer space?

The 7 Cs Privacy Principles:

Comprehension (user understanding of how PII I handled);

Consciousness (user awareness of what is happening and when);

Choice (to opt-in or out, divulge or refuse to share PII);

Consent (informed, explicit, unambiguous);

Context (user adjusting preferences as conditions require);

Confinement (data minimization and user-controlled re-use of data);

Consistency (user predictability of outcome of transactions)

The International Privacy by Design standard to responsibly embed Privacy by Design in online services. The 7Cs principles are also in Dawn's 2005 IEEE Security and Privacy publication along with a privacy and rules-based architecture for user control that implemented rudimentary Vendor Relationship Management. The very important Privacy by Design principles were created by Dr. Ann Cavoukian, Information and Privacy Commissioner of Ontario. They have been translated in over 25 languages.

The OASIS TC on Privacy by Design Documentation for Software Engineers has been convened by Dawn in partnership with Commissioner Cavoukian. This TC intends to create a specification that will facilitate software engineers to embed and document privacy by design in their output at the analysis and design phase of software development. She mentioned how software engineers may use other standards such as OASIS PMRM to document data flows at early analysis stage. She also showed a Visio- extended screen with icons for Privacy Services that she and her student created to help people to visualize some of the tool specifications that the TC may output.

Discussion around whether privacy is an issue for the software engineer (should they have to be burdened with guidelines for enforcing PbD in their work? Would they even follow them?) or for the software development environment (should PbD rules be embedded into development environments so that an engineer cannot make mistakes and inadvertently collect or release PII).

Possible fit with future personal data services.

New Cryptographic Authentication Method for Mobile Devices with Optional Biometrics

Tuesday 3D

Convener: Francisco Corella, Karen Lewison

Notes-taker(s): Karen Lewison

Passwords are difficult to use on mobile devices, and provide little security. Francisco presented a new authentication method that does not require passwords. The slides can be found at http://pomcor.com/documents/NewAuthMethod.pdf.

Highlights:

No passwords (neither ordinary passwords nor one-time passwords)

Public key cryptography without certificates

Optional biometric authentication, without storing a biometric template

Optional use of a trusted 3rd party

App developers insulated from cryptographic and biometric complexities

No browser modifications needed on mobile devices

Can be adapted for desktop/laptop use via browser plug-ins

Questions from participants:

Does the technique for biometric authentication without storing a template apply to other biometric modalities besides iris? Yes, it is independent of the modality, and can also be used to implement physical unclonable functions (PUFs). See blog post http://pomcor.com/2012/10/07/consistent-results-from-inconsistent-data/.

How are the credentials created? There is a section on user registration in the white paper http://pomcor.com/whitepapers/MobileAuthentication.pdf.

Can the authentication token be captured by a man-in-the-middle attack? No, because the connection from the PBB to the VBB is protected by TLS.

How do you deal with a malicious native app registering a custom scheme used by a legitimate application? We assume that all apps in the device are trusted. If
that is not the case, the PBB can be embedded in the native application front-end to avoid the necessity of interapp communication between the PBB and the native front-end of the legitimate application.

Has this method been subjected to cryptanalysis? We presented it to the NIST Cryptographic Key Management Workshop in September 2012, and we intend to send a paper to a peer-reviewed conference.

Can the method for regenerating a RSA key pair from a biometric key be used to bind a signature made by the private key to a biometric? Francisco wasn't sure.

Identity Ecosystem Framework

Tuesday 4D

Convener: David Temoshok

Notes-taker(s): Eric Scace

What are the participants in the ecosystem?
- users: individuals, businesses, machines/devices
- actors: machines or persons
- groups: generic (as users)
- service providers
- agents a.k.a proxies
- authorities, government
- access providers
- credential issuers
- regulators
- technology suppliers
- advocacy groups
- attribute providers
- relying parties
- noise
- trust framework providers

• criminals
• accreditation services
... and probably more.

What are roles?
• users who want to access something...
• service providers (either providing identity services or employing identities provided by something/someone else): relying parties
• credential users
• regulators
• tech suppliers
• trust framework providers. Led into an expository talk about trust inheritance or transitive prosperities.

What is a trust framework?
• 1 answer: business, legal, & technical rules...
• another answer: what is the bar of acceptability... verified conformance to a set of rules.
• Kaliya: What do you mean by trust?

DaveT: Ficam defined 4 levels of assurance (low to high). Other trust frameworks have done something similarly.

Long discussion about establishing trust criteria for relying parties.

Several speakers asserted that, by focusing on 'trust framework', we are focusing on the wrong thing. For example, one spoke of 'assurance trust'.

Kaliya raised issues around frameworks that rely on increasing amounts of personal data for higher levels of assurance.

The clock ran out as the group delved further into the thicket of views about scope of trust frameworks and assurance... and at expiry many intriguing perceptions were socialized but opinions had yet to coalesce around any one or small subset of perspectives.

Session Topic: OX Open Source Open ID Connect and UMA Demo

Tuesday 5A

Convener: Mike Schwartz

Notes-taker(s): Mike Schwartz

Tags for the session - technology discussed/ideas considered:

Mike gave a demo of the OX OpenID Connect Platform. See http://ox.gluu.org for the latest code and documentation.

The demo showed how an organization could use the OX platform to define custom authentication policies, to define claims (or attributes) and to release these claims to dynamically registered clients.

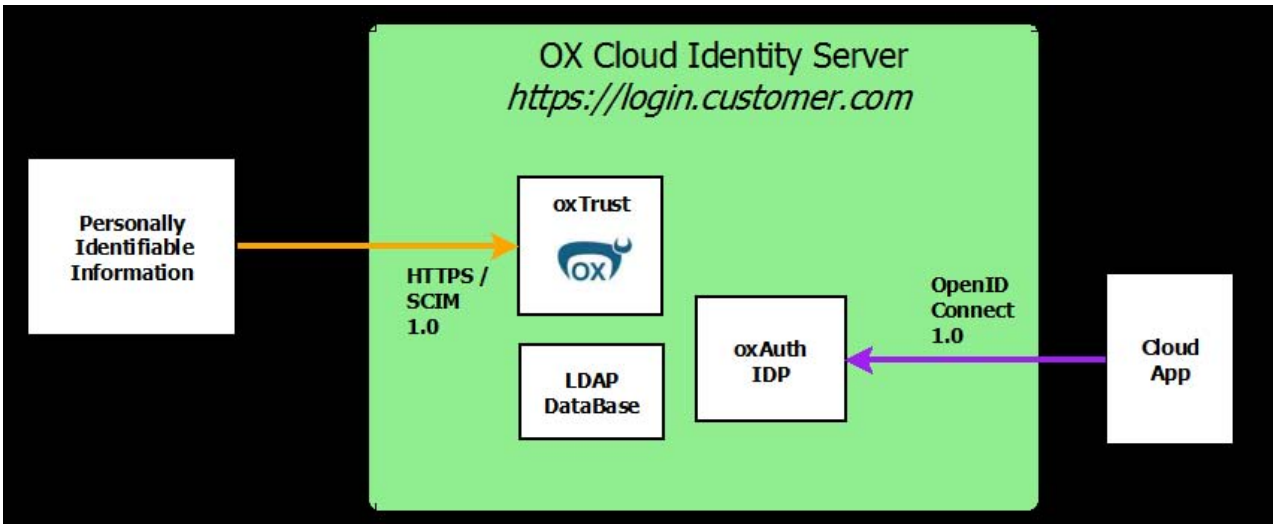
Mike also talked about the roadmap, which includes support for UMA, multi-party federation, and

clustering. Gluu is also moving the code for mapping identity information from existing ldap servers (like Active Directory) from its commercial product into the OX open source platform.

Gluu is working to get its software into Linux distributions like Red Hat and Debian. The deployment is relatively simple: install an LDAP server like ForgeRock OpenDJ, install tomcat, and drop the two "war" files (one for oxAuth and one for oxTrust) into the tomcat webapps folder.

Support for OX is available via the mailing list. Gluu also sells support for commercial deployments.

The attached diagram was referred to by Mike.



Personal Data Analytics and Insights: Using Personal Data to Delight & Enlighten the Consumer

Tuesday 5B

Convener: Peter Stepman

Notes-taker(s): Peter Stepman

We first wanted to create a list of requirements necessary in order to create personal data [PD] analytics services that would be compelling to the person without disturbing or threatening them (the "creepy" factor).

These services touch the core of the person and thus are very personal, emotional, and intimate, and every individual will interpret the service in a different way, so it's important to understand the individual well before starting.

The person must understand the service completely and opt-in

The value and benefits of the service must be clearly communicated and truly add value to the person's life

The service must be clearly intelligent/smart and demonstrate that thought and care has been taken in its development and implementation

The service must be responsive and respectful to the individual

The individual should feel that they are a partner with the service provider in co-creating the experience

When thinking of content/service areas for such PD analytics services, these came up as potential launching points:

Dating (we thought would have the most potential with least adoption resistance in the short-term)

Personality Quizzes highlighting fun aspects

Therapy-Lite (dealing with health, body issues, etc.)

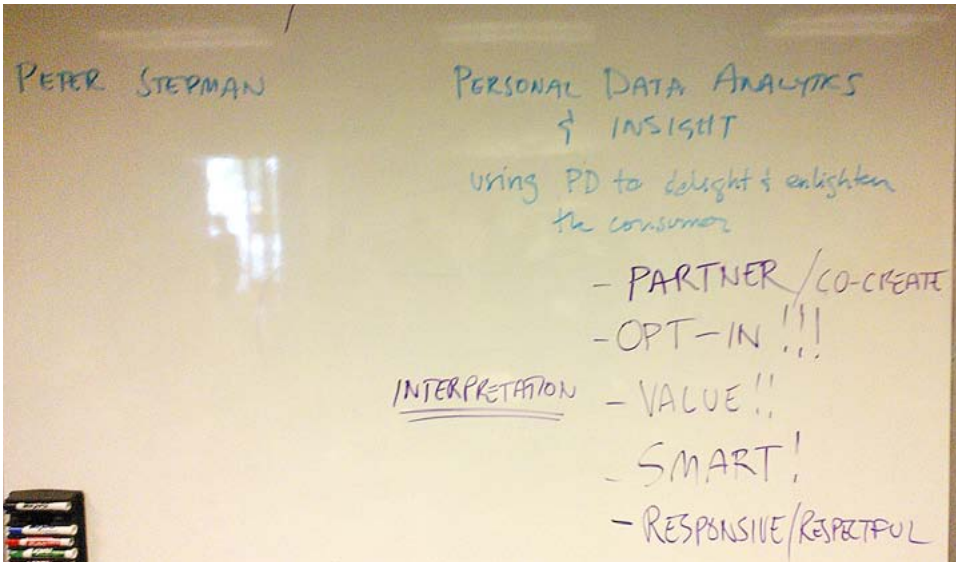
Education: helping people find the right customized path to learning something

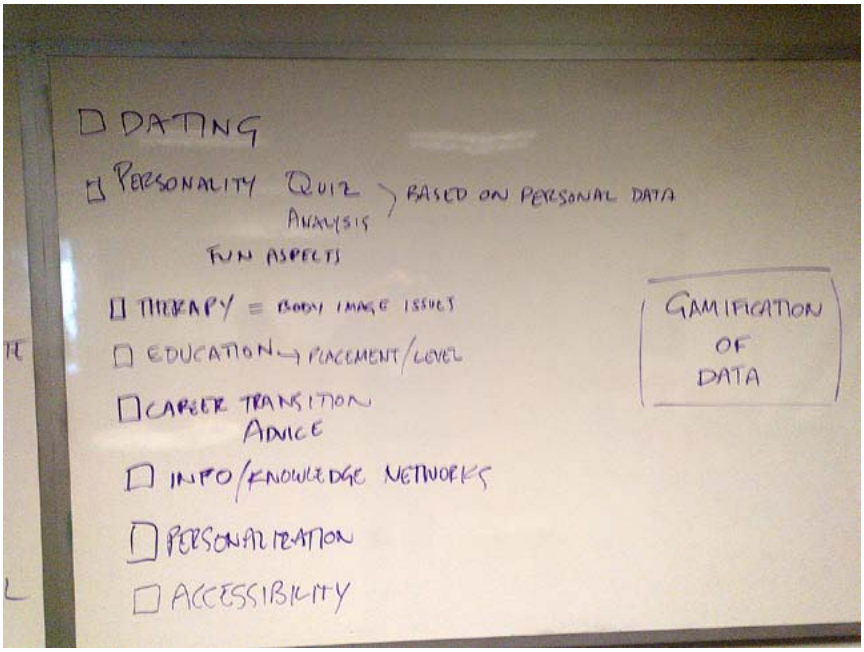
Career training and transition advice

Information and Knowledge Networks: finding exactly what you need quickly

Personalization Services (e-shopping, etc.)

Accessibility for the differently abled





Open ID Connect Session Management & Log Out

Wednesday 1B

Convener: John B.

Notes-taker(s): Mike Jones

Breno de Medeiros gave a tutorial on the current session management model

Mike Jones let the audience know that the purpose of the session is to refine the contents of the OpenID session management spec:

http://openid.net/specs/openid-connect-session-1_0.html

Issue: Is “ops” a separate parameter?

We decided that it should be a separate parameter from the ID Token

Google implementation feedback: RPs are likely to hold on to “ops” as a cookie so we should make sure that it’s safe to do so

Safe across multiple tabs from same RP

Safe for users by respecting cookie same-origin policy

We should add a JavaScript origin to the crypto function that computes the ops

External Browser and Mobile Apps

Wednesday 1C

Convener: Meng Cheng

Notes-taker(s): Meng Cheng

Slides: https://docs.google.com/presentation/d/1qpgQO9k5kbmTd72hlussRUidTUp3KmR7X9xtb1lrggo/edit

If Personal Data Control = Privacy. Then…

Wednesday 1G

Convener: Phil Wolff

Notes-taker(s): William McCusker

What can PDEC and others at this conference do to bring the rest of the privacy community into our space? For example privacy professionals at Kaiser, how do we get them interested in our privacy systems?

What are the benefits we can present to the privacy community?

Risk avoidance (regulatory compliance, brand risk, loss avoidance)

Social/cultural

Economic/ROI

Waste Reduction

How to market to privacy professionals and is it really privacy professionals that we need to tap in to in order to further our collective goals i.e. gain support from businesses…

Identify

Evangelize

Organize/Engage

Status Quo for privacy/security professionals is 'preventing fires'. How do we change this paradigm?

Cost reduction – reduce cost of their job.

Customer satisfaction

Pull versus Push (who should be our advocates?)

Customer Driven*

Internal Champions

CEO

CIO

CPO

CMO*

COO

Outsiders

AARP*

Blue Button

*Most positive response.

Manufacturing Registrations Cards and Digital Birth Certificates

Weds. 1H

Convener: Sam Curren

Notes-taker(s): Animesh

Tags for the session - technology discussed/ideas considered:

Talked about square tag project. A QR code on a bike creates a personal cloud for bikes. A Thing can participate in the internet of things by proxy.

Manufacturing companies are interested in tracking products and components.
The cost of finding a problem later in the supply chain grows exponentially.
For purposes of recall. This is a traceability issue.
what opportunities exist here to allow for to give a better experience up and down the chain...
Sort of a digest that gets enhanced ...
David Siegel - digital birth certificate
Product registration card - the problem is one needs to disclose a whole bunch of private information

Internet of things ... When data is being pumped out

Packaging labels

Curation of the information - context
Gracenotes for the internet of things
Like a CBDB
Chemical tagging, biometric tagging

The same tag could show different information to different users

URL is both an identifier and an interface

Allergy information ... Labels on food ... Disclaimer information and food safety information is already mandated ... So attaching URL to this information may be a good low hanging fruit

Consumer and Public Records and other Identity Data Types

Wednesday 2G

Convener: Anatoly

Notes-taker(s): Leon Brown

Consumer and Public Records and other Identity Data Types

o Experian consumer guy: Anatoly. Free Credit Report.com, Corporate Development and Strategy.

o Public Records: If you Google, public records expose a lot of information. Most not coming from social, a lot is coming from gov't data that is purchased and pushed outside Google firewall. A bit weird to consumers; most think it is Facebook or Social, but it isn't.

o Does there need to be gov't intervention or governance?

o Are there privacy issues?

o Should there be a global solution? 0pt-out costs money in some cases.

o Often personal data has no PII, but is mine.

o Data --> Kim Little discussion. Different rules around different data. Recommend framing data conver

· Personal Information is largest volume of data

· Within PI is Personal Identifiable Information (PII)

· Within PII is Sensitive Personal Identifiable Information (SPII)

· Then there is Personal Health Information (PHI), which covers PI, PII and SPII.

o Is it a private sector opportunity or a governance issue?

o Legislation

· When and how we can use/change data or public records?

· FCRA for public data? Is this a relevant parallel?

- Issues from group
  - Data hygiene
  - Every state has their own laws for data related issues
  - No ??? Motivation to stop it
  - Feasibility to make any technology or data solution work. So many pieces of data that cannot be corrected (even within a credit score or financial report which are strong systems and heavily controlled), how can deal with Personal Information. Should we focus on smaller data set such as PII or SPII?
  - How would a consumer correct data, if there is no central authority for maintaining this data?
  - Who owns the data - for example, what is the correct source for my name?
  - Who is the source of data? Most often the source of data is obfuscated…
  - No liability or responsibility for a data error. For example, if at data entry a name is misspelled it is hard to correct once disseminated
- FTC WhitePaper on white house consumer privacy bill

http://ftc.gov/os/2012/03/120326privacyreport.pdf

http://whitehouse.gov/sites/default/files/privacy-final.pdf

- Opportunity
  - LifeLock of public records?
  - Make it simpler --> Difficulty high to correct anything across 52 states
  - Monitoring new public records: Social à but there is choice
- Detour in to Linden Labs

Personal Data Ecosystem Mapping

Wednesday 2J

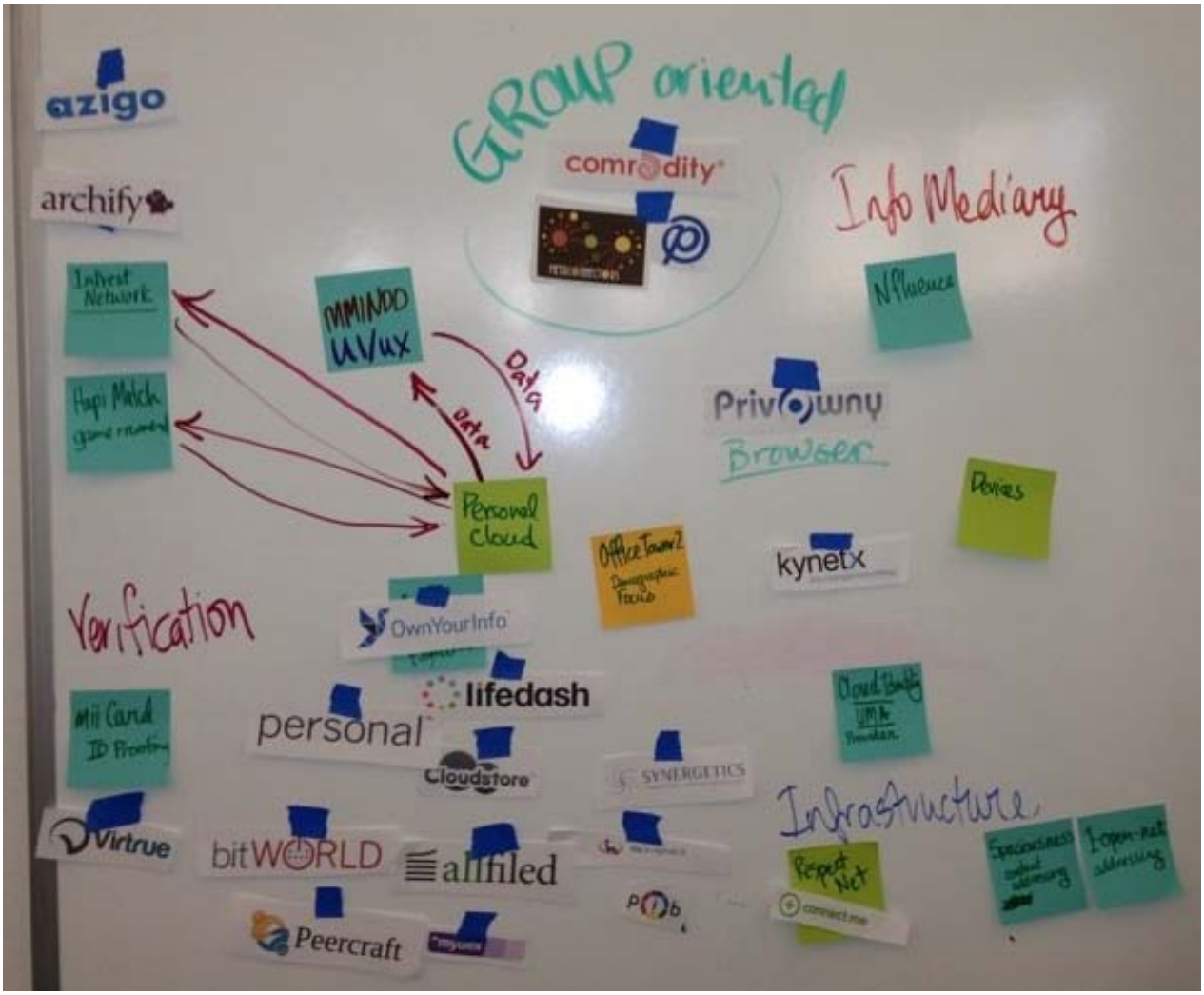
Convener: Kaliya Hamlin

Notes-taker(s): Darren Lancaster, mmindd labs, @thecommunityguy

Tags for the session - technology discussed/ideas considered:

Building the personal data ecosystem map

First approach for the map was segmenting:



Second approach for the map was based on everyone's thoughts on roles/players that are required for the ecosystem:

The main components of the map:

Verification

Info mediary

Infrastructure

Group oriented

Questions that arised in creating the map:

To whom is your fiduciary duty? Who are you responsible to? Acknowledgement that most of us are responsible to the consumer (at least indirectly), but many players (esp. in infrastructure) have a direct responsibility to the data/app/services providers.

Highest volume of players are involved in building personal data stores. A few folks are building something that helps enable groups of people to connect their personal data stores.

Venture funding:

Personal

Data.com

Singly

Others are angel funded.

Educating Customers and Companies

Wednesday 3A

Convener: Alex Levin

Notes-taker(s): Alex Levin

Health
Quantified self

Do you educate on generally what is a data vault or on a specific use case?

Is it okay to do the right thing for consumers without them knowing its happening?

Do you need to know everything about the system? Ex: Banking system

Simulation or role play as a learning mechanism

Duties, rights and responsibilities

How do you bring together multiple services and show the value of having one cloud instead of multiple?

Visual cues to show who is doing security or privacy?

Can you have a way to rate websites on their privacy? How do you reach scale?

What kinds of data do consumers care about? Health records, finance, purchase history, passwords, quantified self

What's important to me and actionable to me in my day to day life?

Mobile SSO?

Wednesday 3C

Convener: Craig Forster

Notes-taker(s): Craig Forster

Tags for the session - technology discussed/ideas considered:

sso, android, ios, passwords, mobile

We had a small but interested group discussing some of the challenges around mobile devices and how the solutions for web SSO aren't possible in the mobile space.

There was an interesting discussion around how entering complicated, and therefore good, passwords on mobile devices is a terrible experience. Over-loading the password reset experience, where a OTP embedded in a link is sent to the email account, was discussed as one option. The issues with this approach were discussed, and how there are similar issues to delegating to the Facebook app but leaving that logged in.

The simplicity required of any given solution was highlighted, due to the issues with typing good passwords on tiny keyboards. NFC was highlighted as a possible solution, as was some of the work from other attendees (OneID etc).

A gentlemen from Pomcor highlighted his work which was presented yesterday around cryptographic solutions to authentication via mobile devices.

The discussion shifted to possible solutions using mobile SSO using current device platforms. We had no-one familiar with iOS in the group, but there was some familiarity with the AccountManager API on Android so a brief overview was given.

The keychain on iOS was mentioned but no-one was familiar with it.

The work about redirecting to the mobile browser then back to the app in order to achieve SSO that was presented in the first session of the day was also briefly discussed. The key security hole is that the redirects aren't secure – this is one technique from Web SSO that doesn't translate to mobile devices.

The need for a secure IPC mechanism on mobile devices was discussed. With this, one could use a web-based SSO mechanism and pass a token to the mobile app. As it stands today, that's not possible.

SCIM

Wednesday 3D

Convener: Trey Drake

Notes-taker(s): Trey Drake

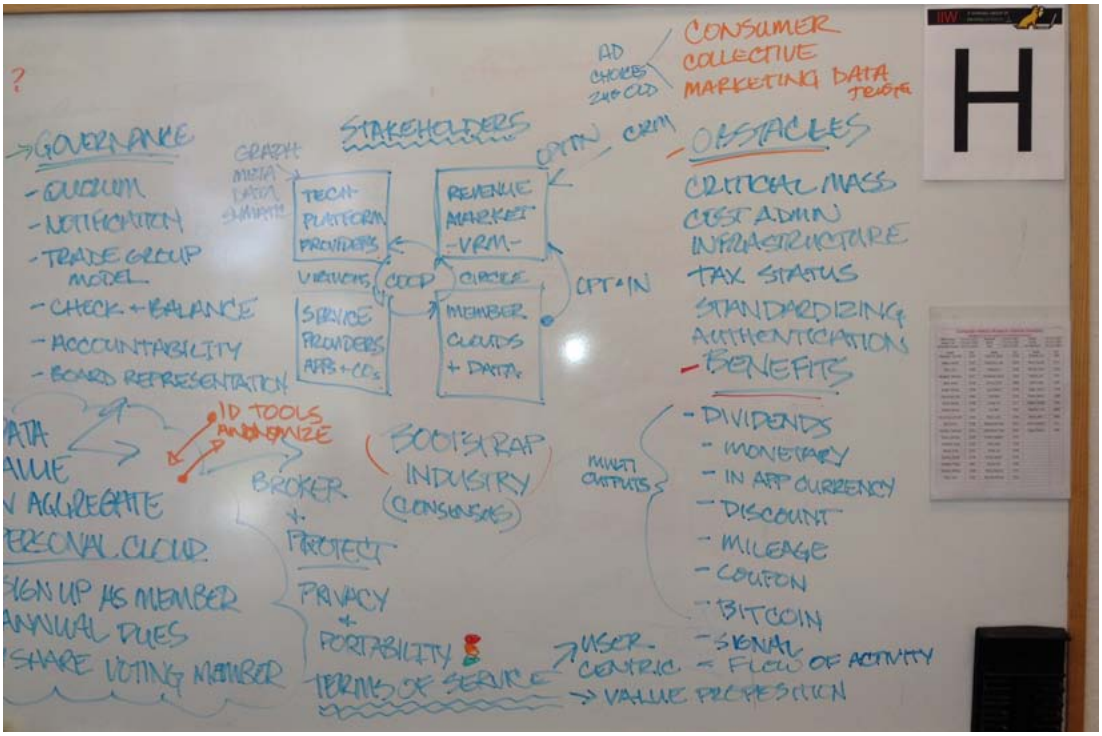
- Overview: What is SCIM's purpose in life: Currently provision identity information from one namespace to another with a single, interoperable protocol and extensible schema.
- What do we want to be when we grow up? A generalizable directory service? Reminder of IETF charter - strong desire to stay w/in the current charter but ensure we can evolve.
- Discussed where we're at the IETF. Moving along though slower than hoped. Isn't that always the case.
- Others want to know what's going on in the design team. Taking a crack at outstanding issues and getting them resolved.
- Do we have the right information and data model? VCard? Odata?...
- Notification service (enable clients to subscribe to changes to their stored artifacts)? In scope? Not in the charter but another highly desirable feature.
- What's the relationship between SCIM and the OIDC user info endpoint? In principle they are the same as they both enable clients to retrieve info about a user stored (typically) at the IDP. OIDC requests are normally in-band and enable user consent/authorization (client shows up with token and user decides if client is able to fetch requested scopes) whereas SCIM more or less plays the "directory in the cloud" role (client shows up with an identifier or search criteria to fetch user, authorization is out-of-band).
- Can we use SCIM as an attribute exchange provider. Sure, but there are no facilities in SCIM for consent, authz, etc.

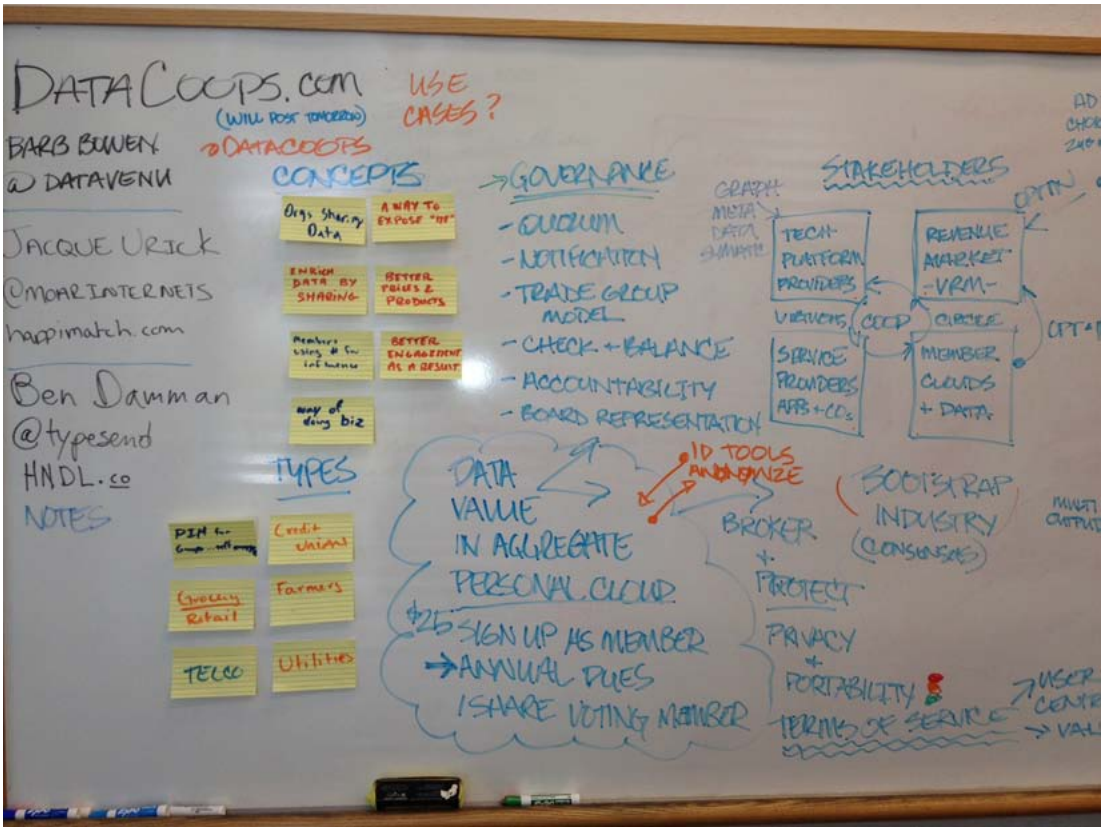
Data Coops & Biz Models

Wednesday 3H

Convener: Barb Bowen

Notes-taker(s): Barb Bowen





Customer 2 Business: Will “Federation” really work?

Wednesday 3I

Convener: George Fletcher

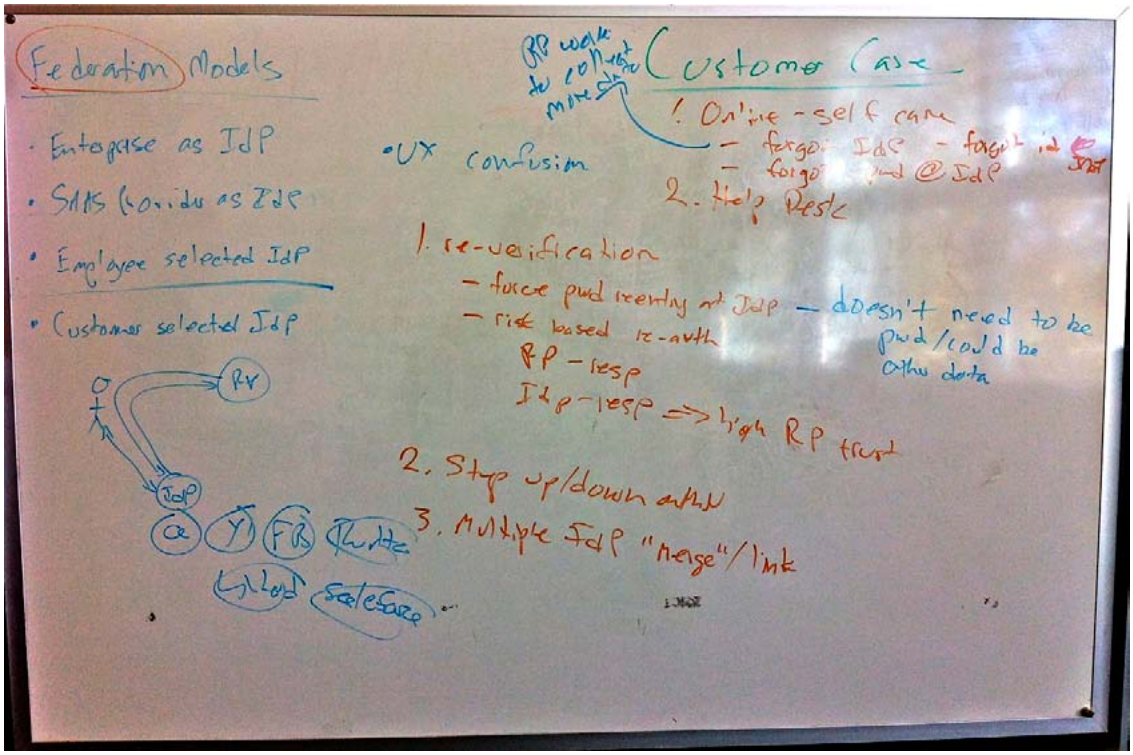
Notes-taker(s): George Fletcher

Possible “federation” models
1. Enterprise as IdP
2. SaaS provider as IdP
3. Employee selects IdP for SaaS provider contracted by enterprise
4. Consumer to Business

Focus is on “federation” model #4

Note that “federation” in the consumer 2 business model isn’t a true federation in that there isn’t a central management of policy and rules.

Use cases not really supported today
1. Consumer re-verification (e.g. when making a purchase to ensure it’s the same user)
   -- at the protocol level may need some signaling from the RP as to the riskiness of the transaction
2. Step up/down authentication (as determined by the RP)
3. Online Customer Care
   a. Forgot IdP flow (as forgot password flow doesn’t make sense)
   b. Forgot identity used at the IdP flow
   c. IdP unavailable flow (the user can’t login to their IdP)
   d. Account recovery by binding a new IdP to an existing account
   e. Limited temporary access (allow user to access service but in a limited capacity)



Social Intentions: Private app on Facebook to express your true intentions

Wednesday 3J

Convener: VS Joshi

Notes-taker(s): VS Joshi

Very good discussion with a very small group.

VS Joshi demo'd the www.trintme.com application.

Audience members suggested ways it can be improved and highlighted its need for the college marketplace..

Key suggestions were to ask for few perms from Facebook and provide assurance that nothing that is done on this private app, is ever disclosed on Facebook walls..

Health Record Banks

Wednesday 4D

Convener: Bill Yasnoff

Notes-taker(s): Mary Hodder

Slides are posted at:
http://www.nhiiadvisors.com/slides/HRBintro.pptx

Showed slides on Health Data Banks / Patient Records

1. Users have records all over, when you travel it's even harder to get data if a problem occurs
    a. losses for users, doctors, health reporting, etc.
    b. goal is comprehensive electronic patient records
    c. fetch and show approach

2. Showed video on health record banks

3. In health care, the patient isn't the customer, they are the product
    a. health care providers think they own the data
    b. they (providers) think they can somehow monetize this data

DISCUSSION:
4. People want to hold their own data.. and control it

5. Centralized data around the person, not in silos of orgs

6. Business models for this:
    a. apps access data.. you get benefit of app, app gets your data (apps could be: prevention advisor, or notification for something important)
    b. fees to users (low)
    c. clinical trials who pay people to participate via a privacy protecting service
    d. service to collect all past records
    e. service to aggregate all your the data and organize it.. for you and your doctors who would

later look at it

Bill will email pointer to slides.

SCIM as User Attribute Provider

Wednesday 4H

Convener: J. Richer

Notes-taker(s): Trey Drake

Goal: Shared, externalizable profile enabling RPs to both consume and augment the same user against different personas

IS SCIM a sensible solution for enabling RPs to get a holistic view of the user. Convenience.

Use case: Col Joe with CAC……notion is sharing of persona/identity across IDPs and RPs

SCIM box “Dick” gets data from RPs

- Q: does the box need the data or does it just need to know where the data is.

- Where does authorization happen? When data is provisioned.

- Lots of authorization issues - broker has knowledge of all user accounts

you can do this today by bouncing around to various user IDPs and collecting data, correlate. Problem with this lots of data leakage.

Why isn’t the answer to just use OAuth2 to front end SCIM and do this with standard scopes

Who’s job is this? IDP or RP? RP of RPs? Who should be weighted more?

RP>broker IDP (get user profile)->if not login to broker then establish a profile->RP broker pulls profile info from IDP->next time user logs into different IDP the RP can then ask the broker RP to correlate

1 login for each IDP relationship and 2 for the broker

In this model each RP has lost control of its data.

Sure SCIM can model complex user relationships

How to do this w/o driving users crazy and being blacklisted by IDPs

World Economic Forum: Update on “rethinking” personal data project

Wednesday 4J

Convener: Kaliya

Notes-taker(s): Kaliya

From Carl:

For those that were interested and wanted to know more there are now formal summaries of the Brussels and China events up on our website:
www.weforum.org/personaldata<http://www.weforum.org/personaldata>

Direct links to the session summaries:
China - http://www3.weforum.org/docs/AMNC12/WEF_AMNC12_IT_UnlockingValueData_SessionSummary.pdf
Brussels - http://www3.weforum.org/docs/WEF_IT_UnlockingValueData_BalancingGrowthProtection_SessionSummary.pdf

Kaliya notes:

New world - different data processor...
Move the model...define appropriate use.
Active discussion in the committee on security and privacy.
OECD guidelines...in process and closing.
Context and collection - big data, actively want to use data.
Other wise people lie...data quality
secondary sources to profile anyways...
it is like the security escalation - cyber security.
lets solve it all now.
something
risks... limited trusted flow
OECD report about the respective value of the data.
How to value it within context.
Better Evidence, Deeper Understanding - more Transparency, - better Decision making -> Changes in attitudes and actions...
What is being measured
What should be measured
How should we measure in an adaptive interactive way.
Internet economy or data driven economy.
What are the risks...
User mental models.
Variables that make up how they think about it.

DATA CONTEXT
* type of data
* type of entity
* trust in Service Provider
* Collection method

* Device Context
* Usage Application
* Fair Value Exchange

This changes along with social norms...
Privacy is not a binary conversation

Accountability
users feel that that accountability must be distributed.
They like right of self determination

ISOC has done a global survey amongst
believe TOS is unenforceable.
choice -> Access -> barrier...

Monday at the OECD - big data event.
On Monday.

Open ID Graph 1.0

Wednesday 5A

Convener: Mike Schwartz

Notes-taker(s): Mike Schwartz

Tags for the session - technology discussed/ideas considered:
Draft Standard

http://wiki.openid.net/w/page/60014791/OpenID%20Graph%201-0%20Standard

Proposed Working Group Charter

http://wiki.openid.net/w/page/60010149/OpenID%20Graph%201-0

The session is best summarized by the above URL and powerpoint slides.

OIDF Workgroup Account Chooser

Wednesday 5B

Convener: Eric Sachs

Notes-taker(s): Eric Sachs

Notes in the slide deck at

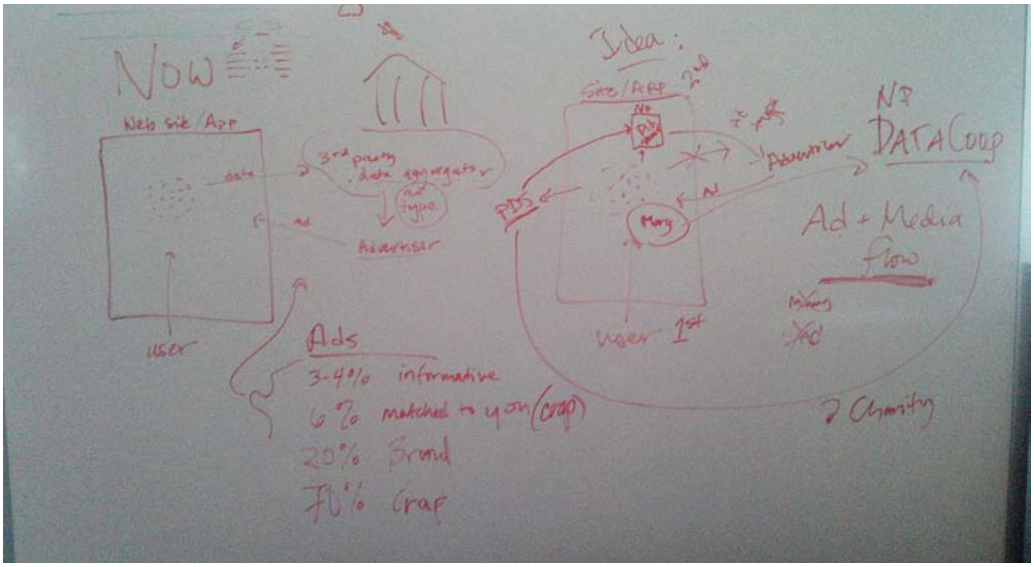
https://docs.google.com/presentation/d/15SvUrlOSgYQW-MNzvBfCOioMikAmh5E19t9VUuhSsqY/edit#slide=id.g30b2f570_1_10

Beyond Prophylaxis: next steps post ad and tracking blocking

Wednesday 5C

Convener: Doc Searls

Notes-taker(s): Mary Hodder



Correct Horse Battery Staple: Strong Passwords…passphrases… are they still relevant/necessary?

Wednesday 5G

Convener: Jay Unger

Notes-taker(s): John Fontana

Jay Unger lead

This will be a discussion, not a presentation

how long will we have passwords?

I think they will be around for at least the next 20 years. What do you think?

Alan Karp

security by secret. I don't need a password. I bookmark a URL, the security moves to how you get into using a computer.

Dick Hardt –

AK – this is preference for single factor log-in

temporary passwords - a one user thing.

???? uses a random password and then hits forgot password. His email becomes his password.

AK - if we can avoid password problem, you might have other problems….

Web keys –

Jay - How do you feel about .... the diff between password and the kind of security questions.

AK - answer all security questions with the dame answer

others do that.

what I have done is create a recovery password.

one person uses a password calculator to generate passwords.

DH - as we use fewer sites and log in with FB or Google, the web is becoming more secure.

AK- what bothers me is SSO but not single log-out. Site does not tell me it is federated. The so has a huge attack surface.

DH – the world is going mobile, the phone is more secure than the PC

jay – not sure I agree

AK – android has done a good idea isolating apps.

dh – more secure, what can happen on it, has a hard ID that a PC does not have.

ID on SIM card?

yes.

dh – where we want to get to with ID, is how do I know it is Jay.

with all the sensors can learn about gestures, what I do.

jay - I travel a lot. Asia is a higher risk environment. I see a lot more challenge behavior than I do in the US.

also privacy issues with behavioral queues.

dh- maybe I was not clear. How I use the phone possibly is a better way to authenticate. How can the device help, it is there with me.

J - …and it is also a store. More than a username and password. You can put dig. Certs on the phone.

J - I have lost cell phones. Many people do.

Dh – lock my phone. It is a brick to anyone else.

we treat authN as binary. We are or we are not.

J- pet peeve for me. With OpenID, ……..

dh- there are bunch of factors avail on the phone. ..when the phone is told to do something, does it have enough confidence for a transaction. If not, it does nothing.

J - I have a dumb phone, a palm pilot. I lost more expensive phones. The question that I have about devices and the role they can play in authn. Most of the lock and unlock can be attacked. If devices are a primary means … for authn…how do you make devices more secure.

dh - locking is not good. More computing mobile, so authN happens at phone. The computer is second class citizen, I use the phone to authN not the PC.

...with gestures get more of a gradient for authN.

J - there are flaws with all of these things.

ak - I have always my phone, my key ring and my wallet.

dh – in ten years the phone is left, the others disappear.

j- lot of 2 factor authN still involves strong passwords. TSA program still uses passwords; banks that use hardware keys also use passwords.

dh nexus is retina scan and card.

J – biometric is expensive and unreliable, lot of false negatives.

dh – I need a gradient rather than yes or no. the phone can learn how I move and how I do things. One of most important ID systems now is looking at history. Look at credit card, bank says – does this look like something the users have already done.

dh – my point, this is state of the art ID now. Credit card is looking at past behavior.

j- if I was at rent car counter in Shanghi and my card is rejected. I am in trouble.

ak – I had a thought, is this dick using device. What if device had a check. You do things a bit different each time. ……

j- you are saying D, that over time something you know will be less and less valuable.

dh- yes, It will be more about how we authN to our devices.

ak- but when that goes away or you need something else.

dh – I could move up into biometrics.

j- if they did 2 factor authN – they could come back and ask for Pin or password.

ak – but you might forget. When it fails, however, the gesture is it turns me down, I won't remember the password.

dh – my point, tint he future, a number of fallbacks to get high certainty it is you.

j – it could be biometrics.

dh – yes, I have to talk to it, move it, swipe my finger.

ak – say if unlock screen, had four scroll bars. I might use two and someone else might use just one.

dh – well, you might.

???? it is multiple smaller factors. I am in an access point I am usually around….. those work in combination if your gesture changes.

j – I worry about it a little. Potential for that authN to be subverted by coercion.

J – what do thin about something you know declining

??? I feel more and more use of biometric devices. . I see bio as part of the future.

???? biometrics might be future, or should could touch your devices or provide your face. ….

j – that is high cost.

???? another way of storing password in brain. Challenge is a playback, you do it fast because you have done it so many times. ….that can not be forced out of you. The challenge is….

Ak – I like the military, the panic password.

j – I have seen that with a bank. I have a panic password, the robber is going to get money. I walk away alive… and it limits liability.

aj – the military one. It takes you into what looks like legit log-in.

j – the bank that does this panic password. Barclays does this in England.

j – this is all good. I still think something you know will be pat of multi factor authentication. I like the idea of what I call pass phrases. Correct, horse, battery, staples is one…. Don't need a wide range of vocab for it to be effective. >less than 1K words.

thank you.

25 years from now we will come back and see if there are passwords.

k – it will be like what dick said, you will authN and you won't even no you did.

I am seeing NFC in use; and I have heard of one country implanting RFID chips.

j – low value transactions will use simple things you know vs. things you have.

dh – I authN to device, it gets me to app.

Fun Applications for Personal Data

Wednesday 5H

Convener: Peter Stepman

Notes-taker(s): Barb Bowen, Peter Stepman

Barb Notes:

Background: Venture Capital Fund in London and L.A. Investing in Consumer applications for personal data. Media background, and incubator for ecosystem

Goal: Brainstorming ideas for gamification elements in apps around personal data.

Model: Introduce gamification to engage user. Playful, competitive and educational points to gain customer interest in building personal and digital identity:

Opt-in

Adds Value

Smart

Respectful

Fun

Possible applications and market sectors for new and fun solutions:

Dataing

Retail

Food/Drink

Sports

Travel Geobased

Therapy Wellness

Gaming

Entertainment

Flaneur/Discovery

Compare

Lifecoach

Learning

How do we avoid the creepiness factor?

What is the line of privacy and exploitation?

Where is the information coming from?

Are recommendations helpful?

Idea- Sherpa button in browser. Selective sharing and following in web browser, a button that gathers relevant data and ignores behavior that is private. Creates a bubble space that gets smart based on your data sharing points.

In the future data gathering and algorithms will bring a more accurate perception for suggestions and future behavior projections.

What if there was a hit me button to search and analyze real time offer data in shopping context. Local and super relevant personas can be created based on location.

Pattern building in addition to personal insight add a level of authentic relationship.

Watching videos and buying books with suggestions and selective disconnect.

Results in search are significantly different based on login or logout status.

There is an explosion in relevance of search based on context and explicit contract of exchange of service for data gathering. Collection and brokering are trade offs for free services.

• How are people going to go off the grid when desired? There may be a future application sector in a screen for incognito mode.

• What if we assigned gamification attributes such as badges to companies and service providers? Net promoter scores as an example.

What insight could be gained from corporate leader boards?

App.net and AngiesList are examples of unique models. These business also have founder with a branded personality.

Peter Notes:

We thought we would add to the list of requirements/success factors created in a previous session. These points could help us create personal data [PD] use cases that were fun and compelling to the person without disturbing or threatening them (the “creepy” factor).

These services touch the core of the person and thus are very personal, emotional, and intimate, and every individual will interpret the service in a different way, so it’s important to understand the individual well before starting.

The person must understand the service completely and opt-in

The value and benefits of the service must be clearly communicated and truly add value to the

person's life

The service must be clearly intelligent/smart and demonstrate that thought and care has been taken in its development and implementation

The service must be responsive and respectful to the individual

The individual should feel that they are a partner with the service provider in co-creating the experience

It should be a fun service (qualified per person)

The service should offer convenience

The service should have a personality or be tied to a trusted, respected and loved personality. Angie's List (www.angieslist.com) was offered as a great example of compelling service tied to someone's personality.

The service should be sensitive and request permission before doing things, especially anything that may be perceived as being "creepy."

When thinking of content/service areas for such PD analytics services, these came up as potential launching points:

Rating companies with a leaderboard

Mechanism for vetting companies/people

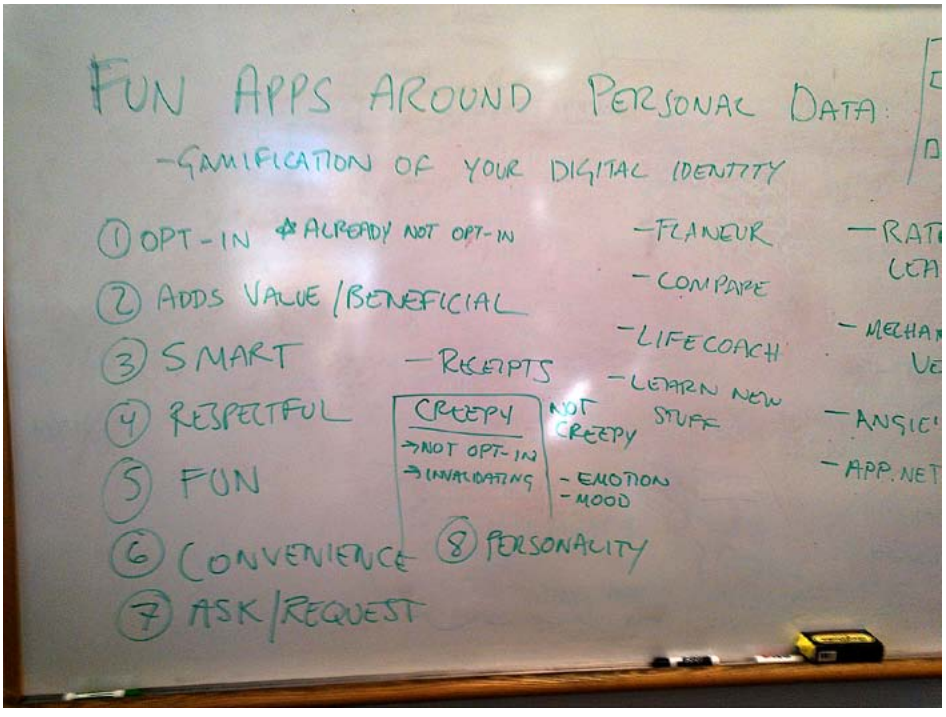
App.Net

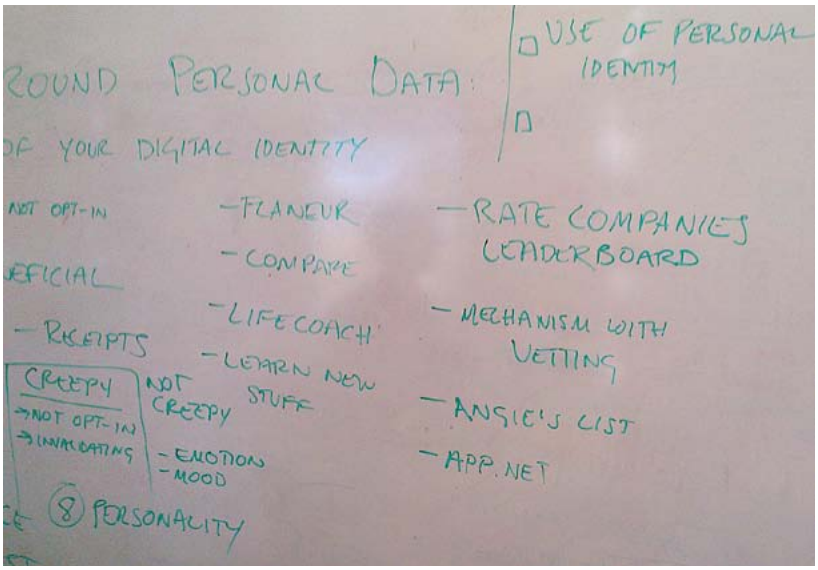
Comparison engines

Life coach

Learning new things

Becoming a Flâneur (strolling along without a clear goal and being open to spontaneous social/cultural events)





Oauth 2 Dynamic Client Registration

Wednesday 5I

Convener: George Fletcher, Tom Brown

Notes-taker(s): Tom Brown

This session combined 2 proposed sessions.

There are 3 outstanding specs related to dynamic client registration

OpenID Connect (push)

UMA original (push and pull)

Oauth 2 IETF draft (push)

Lots of commonality across specs

Self-asserted: hard to verify (client type, for instance)

Oauth 2: how client id and secret is distributed is out of scope

You have 2 different classes of clients (beyond public vs. confidential) that need to be treated different

Should AS restrict what data it gives out based on what was provided? (web page, phone number, etc.)

Security:

DOS attack

scope

client mimicry – human facing metadata ▫ mitigation: explicitly display return to url

authorization trust of registration request

IETF draft will probably reabsorb OpenID Connect additions

The complexity for the AS to do the right thing is growing.

The use case of a native open source mobile client with authorization code flow, not using a custom scheme was considered where the open source project did not want to mandate the callback uri. It was suggested that if the mobile app does not send a callback uri, then the provider will provide its own for the browser authorization. It was noted that facebook does something similar for callback uri.

There is no place in the Oauth spec where you send Json. Perhaps pushing form data is better.

Justin will proceed with resolving remaining differences among the specs.

Session Topic: "A Whiter Shade of Gray" - Mapping the Identity Ecosystem Framework (Input for NSTIC Plenary Next Week)

Thursday 1D

Convener: Peter Brown

Notes-taker(s): Eric Scace, Peter Brown

Tags for the session - technology discussed/ideas considered:

NSTIC; Identity Ecosystem; Terminology; Mapping; Frameworks;

Peter explained the genesis of this conversation. It started as an informal lunchtime discussion the previous day about whether "Framework" in the two concepts "Trust Framework" and Identity Ecosystem Framework" meant the same thing and whether clarifying any differences would give insight into the conceptual model for the proposed NSTIC identity ecosystem framework.

That conversation continued later that day and looked at all the NSTIC governance documents, particularly the terms used. The conclusion was that, in order to avoid confusion with use of the term in "Trust Frameworks", we would analyse what the term "Identity Ecosystem Framework" was actually intended to convey and concluded that it is a set of guiding principles, normative prescriptions and practices. These cover:

Liability protection for individuals (as well as work needed on clarifying what 'liability' implies);

A "baseline for trust frameworks";

Ensure compliance with FIP/Ps and prevent PI re-aggregation and correlation;

Compliance criteria for service providers seeking an ecosystem Trustmark;

Accountability for, and Remediation following, fraudulent issuance and use of (trusted) credentials;

Operating Procedures;

Requirements for Accreditation authorities;

Responsibilities of the Steering Group to administer, curate and manage policies and standards for the ecosystem;

Steering Group to "confirm requirements with a broad group of stakeholders"

The placeholder name for this collection was "NERDs".

Eric Scace continued…

Definitions:

The Identity Ecosystem contains “white” entities:

Whose interactions with each other fully comply with the IDESG NERDs; and,

Whose behavior, as seen by an outside observer, fully comply with the NERDs; and,

Which are currently certified (or otherwise measured by an outside, qualified entity) as fully compliant, and may thereby carry a “white flag”.

The Ecosystem likely contains “black” entities:

Whose behavior be design is intended to be malicious.

The Ecosystem likely contains “gray” entities:

Whose interactions with any other entity (white, gray or black) may functionally comply with interoperability specifications of the NERDs; and,

Whose behavior, as seen by an outside observer, may not comply with the NERDs;

Which are currently not certified as fully compliant.

Observations:

The subset of the Ecosystem containing only white entities should be sufficient to meet the NSTIC goals.

An organization may operate both white and gray entities.

Gray entities may interwork with white entities:

Interworking does not, by its existence, cause a white entity to become gray.

The flow of attribute or persona (“persona info”) from gray to white does not cause the white entity to become gray, as long as the Persona Info is treated in compliance with the NERDS upon receipt by the white entity.

The flow of Persona Info from white to gray may cause the white entity to no longer comply with the NERDs and thereby become gray. The circumstances when an outside observer can determine such a non-compliant flow no causes a white entity to become gray (and thereby lose its White Flag) shall be included in the NERDs.

Errors (instances when an entity or interaction does not comply with the NERDs) occur without malicious intent.

NERDs and their implementation shall be error-tolerant. A defined threshold of errors shall be acceptable by design.

White entities do not lose their White Flag if errors remain below threshold.

Malicious penetrations occur.

A black entity may falsely carry a White Flag. The NERDs shall tolerate this event.

The carriage of a White Flag by a otherwise-gray entity makes that entity black.

A white entity (even a white entity carrying a White Flag) or gray entity may be penetrated and its operations may thereby become black.

The NERDs shall tolerate penetrations and false white flags.

The subsequent discussion covered:

The value of talking about an ecosystem is precisely that ecosystems contain parasitical or destructive bodies that need to be handled. While no-one in a normative framework is going to "fess and sign up" as a 'black entity', they can nonetheless be identified within an ecosystem. Whilst the designation "ecosystem" works well for IDESG, the idea that this ecosystem can be "steered" by a Steering Group is less obvious.

If the ecosystem is built on stakeholders being involved in different 'organisms' of the ecosystem (such as Trust Frameworks), how do the stakeholder groups work in IDESG? The current breakdown is a purely functional, if not totally artificial, choice of groupings that seem to bring together the most important groups. The long ter success of the IDESG however will come about through organic growth from within the ecosystem, not from imposition from on-high.

One major concern is incentives: where is the incentive for the honorably "good guys, white entities" (who are already trusted, well-known, and with high reputations among stakeholders who are important for them) to seek certification within Frameworks that might also be populated by entities with lesser reputations?

While a 'white entity' might receive and handle, for example, attributes acquired from a gray entity – and subsequently handle them as would be appropriate for a white entity, what happens if a white entity hands off attributes to a gray entity? Would this also be OK? How?

General conclusion is the need for the ecosystem to be error and fault tolerant, permissive in inbound traffic and strict in outbound traffic (some similarities with early days of the WWW).

Could there be two types and level of Trustmark? A first, high-level, bare-bones Trustmark valid across the board; a second one that is more detailed and Trust Framework specific. The main issue is transparency and being able to determine – whatever the characteristics of the specific Trustmark – what it stands for and allows.

Is there too much emphasis on the Trustmark? What is really important is reputation, less the specific evidence as that is often context specific.

Education and Beyond: How to Manage New Privacy Risks on Rapid Moving Trends

Thursday 1I

Convener: Nori

Notes-taker(s): Leon Brown

Tags for the session - technology discussed/ideas considered:
Education and beyond

o Akiko Orita - Keio University, Hiroki Sakai, Takashi Kosumi (Yahoo Japan Wallet developer), Tom Liebe (developer at Pacific East), Masanori Kusunoki (Y! Japan)

o Education - a trade-off between policy, free market solutions (including reputation/self-policing) --> If there a profit in doing good

o Trade off between use value versus risk

o Educate - corporation/learning eco-system

o Example: Address, Name, Phone number is enough data to identify an individual.

o Microsoft had an incentive for Do Not Track - by pressuring Google by having a nicer alternative to Google Search may increase Bing searches, which Microsoft monetizes

o Informative to consumers: better understanding, or economic model, to allow consumers and users of free services, and assess the value to them for the free service.

o Children have a far different value for privacy.

o People in EU started seeing issues differently when the gov't started inventing rights/policy for use of data, and gave rights to users.

· "Crack/Cry" How long to crack your data, how long would cry if it was destroyed or hack?

· There is a tension between to decide value.

o Value is something technologists talk about, not real consumers. Consumers just know that 'companies can't do it.'

o Policies between users of Policy data can be effective as consumers will not understand it.

o Japan planning Japanese SSN by 2016/2060. How to exchange information between gov't and local gov't. Investigating usage of personal data. Tax and SSN and HC will be different. SSN will be based on □□□.

o Q: do you think you can educate consumers? Education data users consumers?

Possibly personalized education/learning eco-system

o Stakeholders in Educating

· Business

· Education

· Gov't

· Community (OpenID)

Wallets

Thursday 2F

Convener: Doc Searls

Notes-taker(s): Barb Bowen

Sid- Apple is the largest holder of credit card data. Can we make an app to distribute with Apple Passbook as the largest provider to maintain a VRM wallet relationship?

Apple has a method to make you aware of loyalty and incentive cards when you are in the point of purchase locations (Starbucks an example app). Also had experience with Microsoft project that was not released because of typical big company fail.

Square device is a disruption point. The interchange rate is 2.75%

Recent invstment at 5Bn valuation. Visa is investor. Physical commerce and ecommerce.

Square focused on their customer, the small merchant. The regulatory contracts and minimums make

the experience seamless.

The Square I/O bus implementation was an interesting hardware solution. Powerful from the user point of view.

Doc- sees value in 1 to 1 mapping for sales transactions. Taking a fee for a consultant.

Sam- observes that we carry our phone everywhere. The smartphone as the wallet and loyalty or credit cards are apps. The wallet really is the phone. We will be able to carry many things that would normally not fit in a wallet.

APPLICATIONS

Club cards are easier with an app. An app will scan the physical cards and load them into your phone. Every commercial app is in effect a loyalty card. An ipad can be a complete point of sale system.

Instead of having a bank issue a chip, The cloud could be an id and federated cloud based system. Once you get back to the cloud you could add a great deal of functionality. There is a level of physical security.

Is there a wallet api? There is a disruption point with wallets, Google Wallet

and Passbook are not complete. Go directly to commerce?

Regulatory gap analysis is the approach Square took in the market. Branded payments with generalized capability, avoid redundancy. Bar code apps are a universal distribution concept.

A square tag on your own wallet. Square tag = url encoded tag, as identifier. Any machine readable tag

ISSUES

Privacy-Security-Identity-Anonymity are huge market issues.

Two technical issues. Piracy is an issue. Participation in the internet of things with fraud.

Security in money systems is a point of corruption. Micropayment and dividends are a less competitive disruption point. Merchant markets have a huge opportunity to disrupt.

M-peza Kenya (320 million US) G-cash in the Phillipines. Banks are tied to telcos.

40% of the spend is through cards, so these are privatized transactions.

INNOVATIONS

Innovate disruption for the actual value. Light wallet, extend and add functionality.

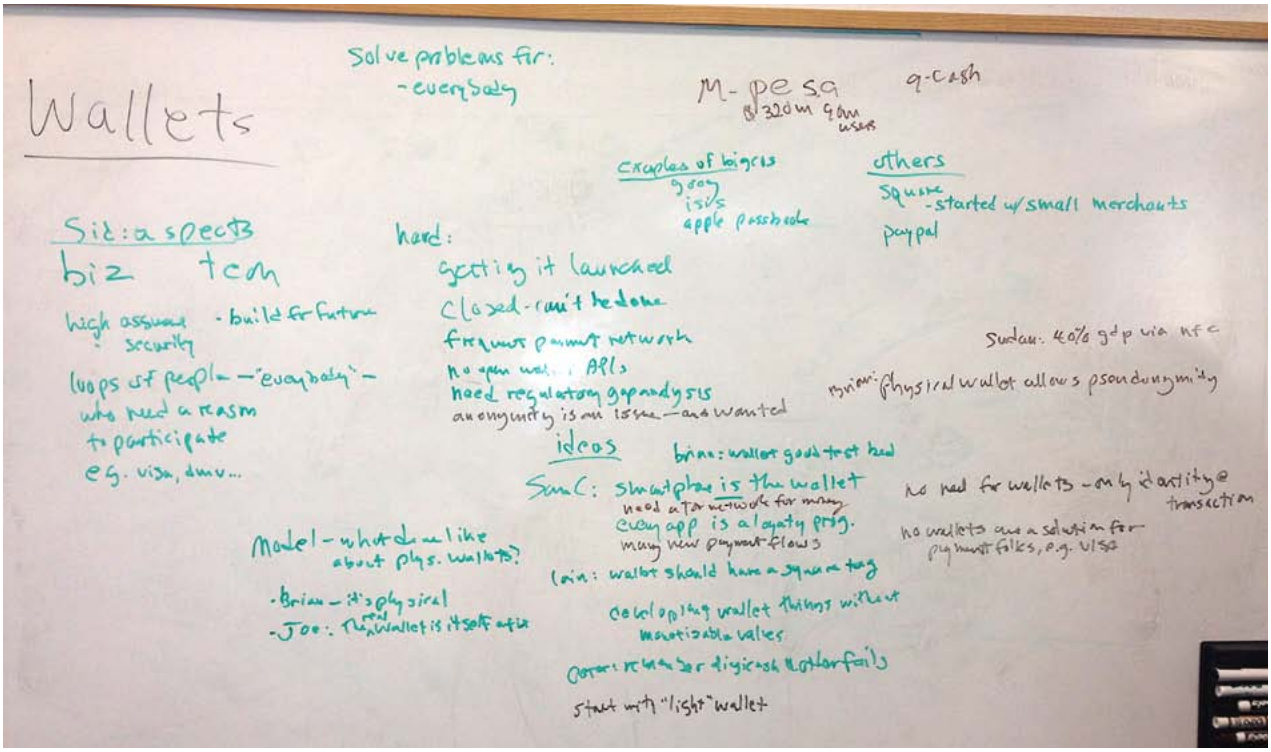
There should be different payment flows. The key is not mapping all the payment flows. The physical card is a pain point for credit card companies. The chip system is the physical card standard. NFC readable chips.

Bank chip inside phone, Crypto inside the chip. Secrets ISIS secure elements.

Multiple tenants. There could be several like Gemalto.

Cash does not leave an audit trail, or cross reference with other identities, or follow through purchase history. (Example DUI arrest tied to patterns in alcohol purchase data)

VPN networks are faster. Deep packet inspect. VPNs are encrypted packets. Capture is possible offline.



Webfinger

Thursday 2J

Convener: Evan Prodromou

Notes-taker(s): Markus Sabadello

Evan gave an overview of the Webfinger processs.

The idea is that you discover information about an entity in a two-step process, which involves retrieving XRD documents from a well-known location.

Problem: 2 round trips are required.

There's a philosophical difference between Webfinger and SWD.

Webfinger: You retrieve a document.

SWD: You ask for a specific thing.

The concern within the OpenID Connect community is that the discovery process must be simple enough.

Currently: 3rd IETF draft.

Likely scenario: Have both in the foreseeable future?

Webfinger has JSON now, but didnt have it when SWD was invented.

Latest Webfinger draft:

* XRD is moved to appendix, JSON is preferred

* It's possible to retrieve either host-meta.json or host-meta with "json" Accept header. --> confusing?

* JRD should be required, XRD optional

Both Webfinger and SWD are likely to co-exist for a while.

Which location out of a list should be picked?

In the original XRDS format, there was "priority".

Maybe in Webfinger just try the locations sequentially?

Doubts whether major players will support the latest Webfinger?

Major players currently don't support SWD, but will probably in the future.

Kynetx use-case: Need to discover someone's Personal Cloud, which involves an "event channel" GUID. A custom "rel" type is used in the JRD. The GUID is stored as the "href" field in the JRD. You can also have "properties" in an XRD/JRD, i.e. key/value pairs associated with the resource.

Advice: Vision of Webfinger is that you would have many more "rel"s for everything, e.g. blog updates, profile page, etc., rather than just the "event channel".

Reminder: Webfinger addresses are not necessarily e-mail addresses. The idea was to use identifiers that look familiar to users. Internally, they use the acct: URI scheme, but that's not exposed to the user.

Webfinger can not only be used with acct: URIs, but with any URI from which you can extract a domain name.

All information in Webfinger is public, which may be a good or bad thing. Is there a need for private discovery? Is there a need to authenticate a client before formulating the Webfinger response?

Another related effort: Dialback Access Authentication, to authenticate HTTP requests based on a Webfinger discovery system. Drawback: A roundtrip is required to verify the request.

UE for ID/PDE UX & Tech for Identity Across Devices

Thursday 3G

Convener: Phil Wolff

Notes-taker(s): Animesh Chowdhury

One UX to rule them all

Strategies and solutions for UX for identity

Problem desc: value in having a single sign on .. Example is GE ... Makes all sorts of devices ..l big and small, specialized and mass market ... Shared washing machine use case ... Some desire for unification ...

Identities

Spectrum of experience ...

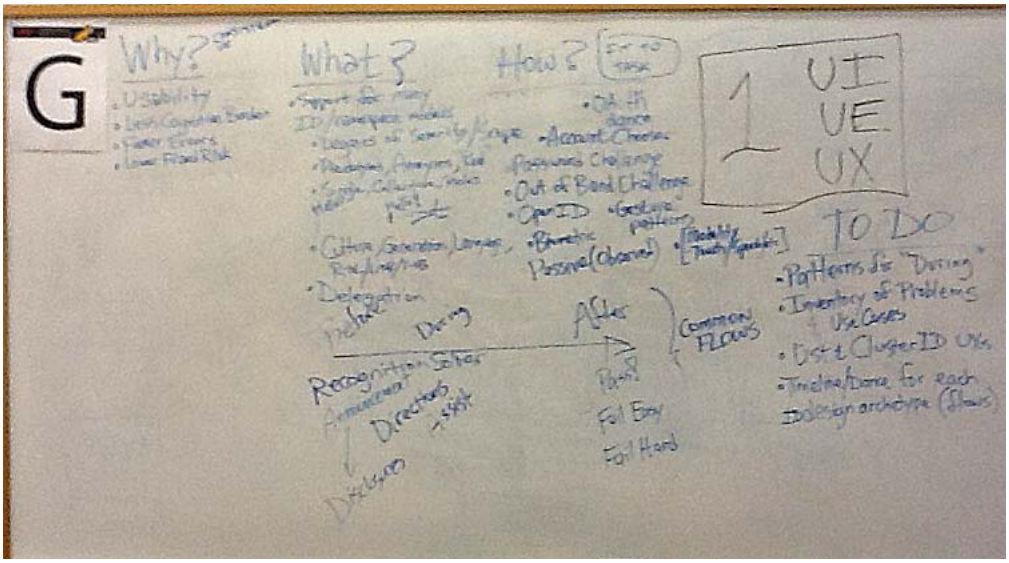
UMA

Presence is

Big categories of interactions - identify the major areas , then identify the emerging patterns in each of these categories

Requirement to identify ... Degree of authenticity required for the scope of the task

common flows for most recurring use cases



Account Recovery

Thursday 3H

Convener: Jim Fenton

Notes-taker(s): John Elkaim

Sub Topics

-"Security Questions"

- Email recovery

- Telephone Agents

- Physical Recovery Tokens

- In person reset

Achieve higher LOA

- SMS recovery

- Physical mail

Main domain

Domain registrar

DNS service

Password reset

ATM card (Recovery...)

It is easier for user to recover without a password security questions (Password for another password)

CyberID cyber punk

Password Managers...synch (Keypass Iphone)

Password recovery is inherently vulnerability. You are exposed even if you don't want it.

Certain Apps don't use SSL to communicate the data or store passwords locally

Different level of recovery depending of data sensitivity, physical verification (Bank vs a New york Times)

Panic code...at ATM allow max withdraw and inform authority of theft (Barclay UK)

Which IDP to use for recovery? What is your identifier often it is already taken

Users can get SIM cards without credentials in Ireland while in Switzerland extensive verification is requested passport...

Not on the black list authorize link with device with anonymity

Ultimate Realization of User Managed Contracts

Thursday 3I

Convener: Dazza Greenwood, Doc Searls

Notes-taker(s): Eric Scace

Reporting on work from MIT Media Lab. Dazza sketched out some of the problems (UMA binding obligations, for example) which led to investigation of the following.

Suppose that:
• in a profile page (into which people can enter) for an app, the core rights & obligations are located...
• in an OAuth site or equiv one can see all apps that one has granted access to, and the nature of those apps, in a admin panel.
• merge the above with the contract (between user and service provider, e.g., of a personal data store) itself.

Preliminary work:
• top §§: description of parties (individual & e.g., User Managed Access service provider), scope/ description of interaction, term.
• §X: particulars of rights (prototype = OAuth scopes of 7 dimensions) granted for each app, dynamically generated according to the snapshot at the requested moment in time (current scenario is the priority at the moment, or scenario as of yyyy mmm dd hh:mm GMT available in a data store... a.k.a. "temporal reconstruction").
– this section now gives the complete dashboard of all contracts in force at the time. Similar to 'my account' pages.

General discussion followed.

• Simplifying terms of use is a long, difficult slog.
• Mechanism for proposing & agreeing to a change of
• How to solve false repudiation issue. Could use external service that does joint authentication between the parties that cannot be subsequently repudiated.
• Could get rid of permission ceremony when user has pre-authorized a certain set of tolerated settings for generic use (e.g., certain subset of attributes, relying party must limit use to only current session, cannot retain nor disclose, etc)
• Could include a default setting of parameters for 'any other app' (e.g., 'do not subscribe me to newsletters', 'do not track', &c)... which a browser plug-in, for example, could help convey.

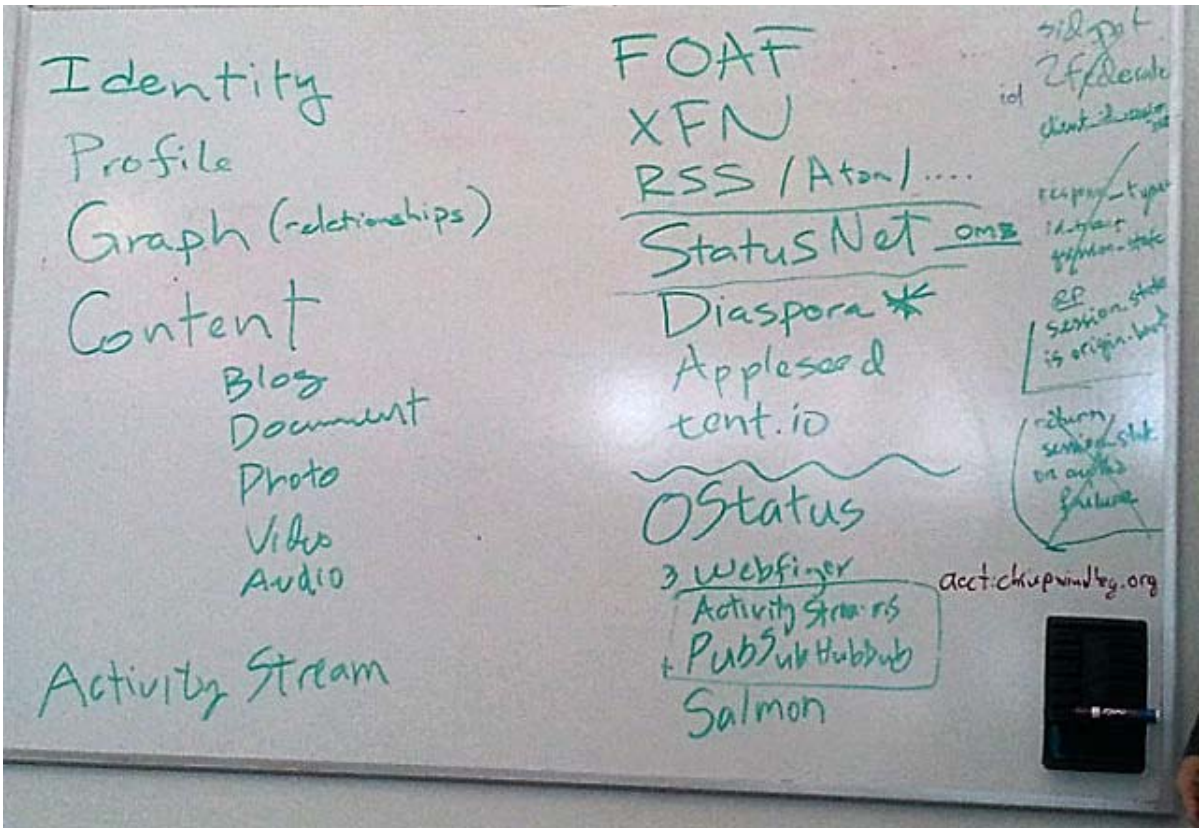
Notetaker:
E. Scace, who understands a rather sketchy level of context & thereby notes that the accuracy of the above is subject to validation by the speakers.

Fed. Soc Web Sum

Thursday 3J

Convener: Evan Prodromou

Notes-taker(s): Markus Sabadello



Goal: Provide social web functionality without dependency on a single system. In other words, have a topology like e-mail.

Functions: identity, profile information, social graph (friends, etc.), content (blog, documents, rich media), activity stream, publication and subscription model.

Technologies: FOAF, XFN, RSS/Atom/...,

Projects: StatusNet, Diaspora, Appleseed, tent.io

Current mentality: Build one piece of software that can do everything, with its own protocol, extensions, etc. This approach has resulted in some disappointment.

Better approach? Agree on an extensible protocol supported by multiple implementations.
This was the idea behind OStatus (= a suite of protocols: OStatus, Webfinger, ActivityStreams, PubSubHubbub, Salmon). This is different from earlier "monolithic" approaches.

OStatus has been successful and is widely supported, e.g. by Wordpress.

Problems of current OStatus?

* E.g. PubSubHubbub doesn't support private feeds.

* Immediate spam on publicly hosted StatusNet instances.

* Onboarding: How do I get my existing social graph from e.g. Facebook into my StatusNet instance?

* Operations requiring a "global view" on the system, e.g. monitoring a global hashtag.

* Make it look better for the user.

StatusNet and Diaspora are AGPL: Nice for free software, but less nice for people who want to make incremental improvements while protecting intellectual property.

Important feature for broader adoption: Introduce a notion of groups on the protocol level, which is independent of a specific implementation.

Goal should be not just to build a replacement for Facebook, but to build something that can do more. The Federated Social Web may look different from what we currently think of as social networking. E.g. just like blogs evolved into social networking, a federated social web may be quite different from "traditional" social networking.

Advice: Use decentralized software, e.g. publish your social content on Wordpress, support existing projects, keep experimenting.

POSSI: Publish, Own, Site, Syndicate, Everywhere

What to do to improve current shortcomings of OStatus?

Work on a new version? Consider XMPP?

Why don't Facebook, Twitter, Google+, LinkedIn talk to each other?

Incentive only for smaller communities to join a bigger internetwork, but not for big players to cooperate with each other.

So, the strategy for the Federated Social Web should be to build on small communities that want to grow into a bigger internetwork.

Group Therapy

Thursday 5H

Convener: Peter Stephen

Notes-taker(s): Sid Sidner

Tags for the session - technology discussed/ideas considered:

Personal Data Stores, VRM, Salesmanship

Sid Notes:

How to talk to people about the positive aspects of personal data store?
One approach:

Listen first to find another current starting point

Ask a question.

Map to identity/PDS world view

Add in new information

Don't sell through the close. (What is the "close"? What do you want from them? What is the action? What do you want them to leave with?)

Check for understanding.

(What about making this 2-way, collaborative?)

What can we do together?

Terminology is a big issue.

Many people have the same question.

Working on digital identity helps us (forces us) to understand human identity.

Know your audience.

Make it relevant to their universe.

We don't even know what human identity/PDS means. Trying to figure out digital identity/PDS causes us to learn more about the human side.

Use metaphors for complex concepts.
If you are doing something innovative, there are no words. Metaphors are needed instead.
Metaphors:

We first do the old way, w/ new materials

Then we do a paradigm shift

PDS's are ready to go to a paradigm shift. The value is in the use; not the sale of it. The value is in

the transaction, not in the ownership.

The use of my data means an exchange of value.
Nobody can use my data as well as I can.

Keep It Sweet & Simple.

Lots of VRM discussion:

Buying when, where, x, x

Hulu (the video service) is now asking in the browser, what do you want to see?

Japanese national ID system:

Discussions are very fragmented

Avatars are often used online in Japan

Bibliography:
Push by David Siegel
The Structure of Scientific Revolutions by Thomas Kuhn

Peter Notes:

The idea of this session was to come together and talk about issues we have at communicating our vision to people outside of the community in the hopes of transferring our excitement so they may virally spread the message further. We discussed some of our frustrations initially, but then heard some positive experiences from the group, and eventually came up with a strategy on effective and inspirational communication.

Listen and ask questions

Know and understand your audience's point of view and context. Perhaps do some research before beginning the conversation and use as much insight as you can get

Add a piece: Continue from your audience's story by adding a piece of yours, but keep it simple

User metaphors that relate to your audience in order to communicate complex concepts

Don't sell through the close—know when to stop – have empathy for your audience and learn to read signals of information overload

Check for understanding

Decide what the close will be:

What is the understanding you want to achieve with the audience?

What is the action you want the to take? Their next step

What is your next step?

Does your audience have any advice/feedback for you? Listen carefully and be open to criticism.

When talking about VRM and Personal Data, we thought it would be good to communicate:

With Personal Data, value is in the use and transaction, not in possession

We are creating a value exchange, a value network