The 8th Internet Identity Workshop 2009a

May 18 – 20, 2009

BOOK OF PROCEEDINGS

Version 1

Notes in this book can be found online at
http://iiw.idcommons.net/Notes_09a

Notes Gathered and Compiled by Heidi Nobantu Saul & Kaliya Hamlin

IIW is produced by Phil Windley, Doc Searls and Kaliya Hamlin

www.internetidentityworkshop.com
IIW9 is November 3-5

Table of Contents

Introductory Letters

From Mary Ruddy, Chair Identity Commons Stewards Council

The Internet Identity Workshop holds a special place among Identity Commons working groups. It is an event where anyone and everyone interested in working towards a shared vision of a decentralized, user-oriented identity layer for the Internet can come together and make things happen.

Part of the magic of IIW is that you never know what is going to happen ahead of time – and this event really delivered – featuring demonstrations of new technologies, conversations to create new standards, and discussions to forge new business alliances.

If you are not already doing so, I invite you to continue the energy sparked by IIW9 (2009a) by joining one of our working groups. You can find a list of them and their descriptions.

I would like to thank all the stewards:

- Bob Blakley (IdMedia, Photo Group)
- Peter Davis (SAML Commons)
- Pamela Dingle (Pamela Project)
- Kaliya Hamlin (Internet Identity Workshop)
- Iain Henderson, Dean Landsman (VRM)
- Mike Kirkwood (User-Centered Health)
- Lucy Lynch (ID-Legal)
- Bob Morgan (OSIS)
- David Recordon (OpenID)
- Drummond Reed (Information Card Foundation, XDI Commons)
- Chris Reynolds (Newbies4Newbies)
- Mary Ruddy (Higgins)
- Denise Tayloe (Kids Online)
- Paul Trevithick (Identity Gang, Identity Schemas)
- Bill Washburn (XDI.org)

For their active participation that makes this community thrive.
Looking forward to seeing you at IIW 9 (2009b)!

=mary.ruddy Chair of the Identity Commons Stewards Council
* Skype: mary.ruddy
* Y!: maryruddy2
* P: 617-290-8591
* E: mary at mersitic.com

'

From Kaliya Hamlin, Facilitator & Co-Producer IIW

About few notes about this book - We have added a list of attendees to this book of proceedings.
Each of the sessions has its own wiki page if you want to add notes to a session please do so there and notify us we can add it to this physical book and re post it on the wiki. You can find Photos from the Conference here on Flickr.

The Internet Identity Workshop is now four years old and the Identity Gang that it grew out of has been meeting for five years. Many members of the community have been working on aspects of the community vision for many more years before that.

The energy momentum of the community continues to build and this year major internet portals are adopting technologies that have been evolved in the community. There is an increasing awareness that open standards are essential to preventing identity lockin in walled garden silos. We have come a long way but there is still much more to do to fulfill the purpose of Identity Commons **– to support, facilitate, and promote the creation of an open identity layer for the Internet -- one that maximizes control, convenience, and privacy for the individual while encouraging the development of healthy, interoperable communities.**

We need to continue to work together enhancing the communication between working groups and raising awareness of our activities.
We would not be here today without the contributions of some key people and communities.
* The original founders of Identity Commons Owen Davis and Andrew Nelson along with early pioneers working with them including Fen Labalme, Victor Grey, Nicholaj Nyholm, Bill Washburn, Drummond Reed, Joel Getzendaner, Andy Dale, Christopher Allen, Mike Mell, and Eugene Kim.

* The second generation Identity Commons evolved in the summer of 2006 and arose out of a community conversations that included key input from Bill Aal, John Ramer, Brett McDowell, Dale Olds, Mary Ruddy, Paul Trevthick and our lawyer Dan Perry.

* The thought leadership of Kim Cameron, Doc Searls, Phil Windley, Dick Hardt, Johannes Ernst, Pamela Dingle, Mary Rundle, Bob Blakely, Jamie Lewis, Ben Laurie and everyone who actively blogs and writes about the issues around the technologies that are being developed.

* The community stewardship of key online spaces like Planet Identity by Pat Patterson, our wiki and website maintained by Fen Labalme and the Story of Digital Identity Podcast that Aldo Castaneda produced.

* Everyone diving in and building new technologies, applying old technologies and getting open standards evolved to make it all work. Along with those evangelizing the ideas and working to drive adoption.

* The Co-producers of the Internet Identity Workshop who are amazing to work with Phil Windley and Doc Searls along with the partners we have had for the Identity Open Space events Digital ID World and Liberty Alliance.

The Internet Identity Workshop would not be possible with out the community that gathers or the sponsors that help support our gathering - listed on the following page.

We look forward to seeing you all at the next Internet Identity Workshop November 3-5, 2009.

Kaliya Hamlin,Identity Woman

Sponsors

Microsoft, Plaxo, OpenID Foundation,
Information Card Foundation, Google, Ouno,
Yahoo! Developer Network, OASIS IDtrust, Kantara Initiative.

Session 1

Identity Does Not Matter - Authorization Does

URL Identity Doesn't Matter - Authorization Does
Convener: Alan Karp, HP Labs
Notes-taker(s): Guillaume Lebleu
Other Members: Pak Mark, Steven Herbst, Jens Heusser, Abraham Williams, Hannes Tschofenig, Bob Pinheiro, Pete Rowley, David Primmer, Tatsuki Sakushima, Meadhbh Hamrick, Doug Whitmore, Greg Haverkamp, Tom Brown, Guillaue Lebleu, Keith Dennis, Joaquin Miller, Scott Seely, Jeff Shan

Technology Discussed/Considered: Webkeys, authorization, delegation

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

Session organizer: Alan H Karp from HP Labs
Alan started the session with a few slides on Identity and Access Management Position Statement. His main point is that the two concerns should be separate.

Basic problem: how does a user inform a car rental company to update the rental is updated IF the flight is delayed.

The car rental company does not care who is changing the car rental information as long as they are authorized.

Web keys:
Use Bookmarks for login. https://airline.com/iodksldlsjdlskjd a secure URL with a password.
The user does the same for all the services he uses.
Companies already use Web keys: You can view a confirmation by clicking a URL received in an email.
This Web key can be passed along. The issuer does not care who uses the URL as long as they have received it.

Question for the session:
Do we really need identity? What are the use cases that REQUIRES identity, except for the who did what use case ("who to throw in jail scenario"). Delegation of authority is done by sending a URL.

"Identity is an indirection to authorization"

The challenge is the delegation: how to share a small amount of rights.

If there is a mechanism for proving one's identity.

Identity gets in the way of delegation. With URLs you can delegate delegated rights. I can't prevent the receiver from delegating anyway. They will find a workaround.

Access control problem:

1. identification
2. authentication
3. authorization (ACL)
4. ACLs check

Web keys are like machine language. For the convenience of users/administrators: user roles, identity, etc.

We use identity in two many places that makes identity theft possible.

There is no logging system for delegation of authorizations.

Webkey: sentry system to whom I show a pass.

Voluntary Oblivious Compliance. You have to acknowledge that you are relying on the good action of your people: they can always find a workaround.

Identity is like a center of gravity where you accumulate reputation (ex. Lots of links pointing to you).
Identity: there is no data there, except that it is the guy.

“Aggregated identification is way harder than the way OAuth does it.” Eve Maler

Q: The problem with Webkeys is how to remove delegation. A: you remove the mapping. Q: yes, but I need to break each one.

Identifiers have a benefit of aggregating authorizations.

Authorization management has to be done in the user's domain.

Webkeys represent permissions.
A GET on a Webkey may return several other Webkeys.

Identity does not matter at the time of access control, it matters only at the time you assign it.

Webkey is not security by obscurity.

If you don't want your sister to see your calendar, don't send the email with the Webkey to her.

It all depends if you need to do the evaluation at use time or not. Is the policy contextual?

What about implementing separation of duties w/ Webkeys.

Defining An Architecture for VRM and Volunteered Personal Information & Distributed Identity Based on Relationships

URL Defining an Architecture and Lexicon for VRM and Volunteered Personal Information   Distributed Identity Based on Relationships
Convener: Pat Sankar Rel-ID Technologies
Notes-taker(s): Pat Sankar and Gam Dias
Other Members: Ariel Gordon, Ben Sapiro, Hank Mantchin, Eric Darghi, Jeff(Jeffrey) Shaw, Mary Ruddy

Technology Discussed/Considered: VRM, VPI

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

25 yrs. experience of building consumer DBs - around 10 yrs. ago, concluded that the model won't work. In CRM the promise of vendors building a DB, each building their own view of the consumer, ends up with a silo. So how would it be if you build the data structure on the side of the individual?

The legacy is that organizations hold the data, individuals end up having to run back and forth trying to maintain that data, largely out of their control

Displayed MyDex slide showing all of the silos with similar data architecture and similar issues trying to maintain the accuracy of the data. A well designed customer database has around 400 core attributes.

As an individual, you would need around 3,500 variables that would contain all the attributes that would require you to deal with all of the vendors you would have.

Around 9 years ago, a data architect was given the exercise of "If your house was burned down, what data would you need to rebuild your life". Came back with a model containing around 3,500 attributes.

How many of those were dependent vs. independent variables – e.g. how many depend on your physical address. The 3500 items is a normalized number
When you look closely at this, an individual has a number of personas that cover various firewalled aspect of their lives

Showed MyDex architectural slide containing planning systems and doing systems. A CRM 'single view of customer' is not really that.

When looking at this from an individual perspective, (see green and red slide) an individual contains many layer in their system, some of them manual (paper), some thought based (brain), some of them held by vendors (e.g. bank, insurer), some of them online (google, wesabe) etc.

See current slide – who has what data

Planningdata

Doingdata

Schema

Reputation – setting

Reputation - getting

Interaction

Transaction

History / Time / Log

Geo

Membership

Activities(stream)

Intellectual Property

Permissions

Assets

Deals

Contacts

Accounts

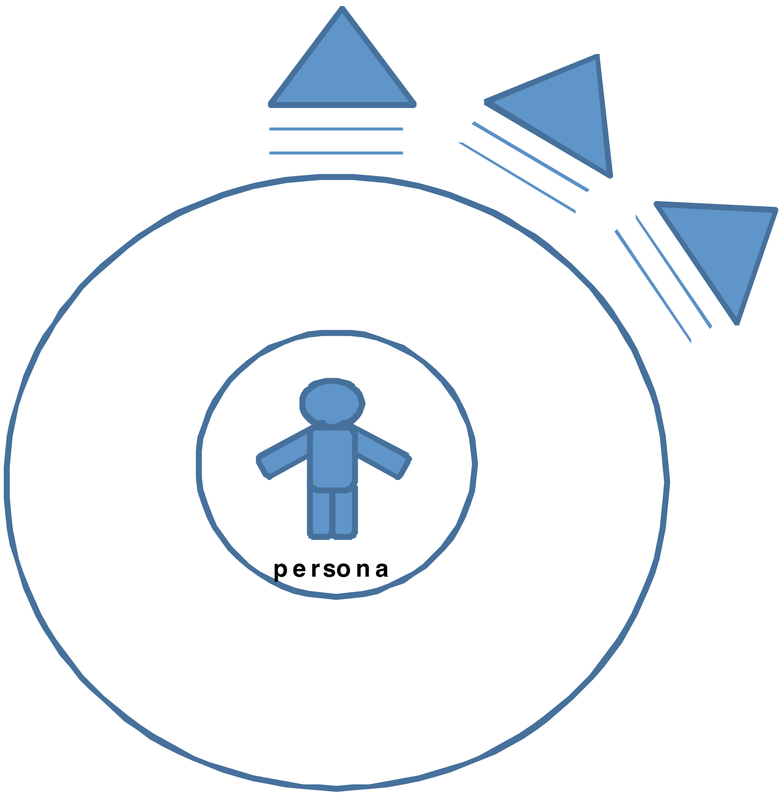
Data Sharing

Preferences (global)

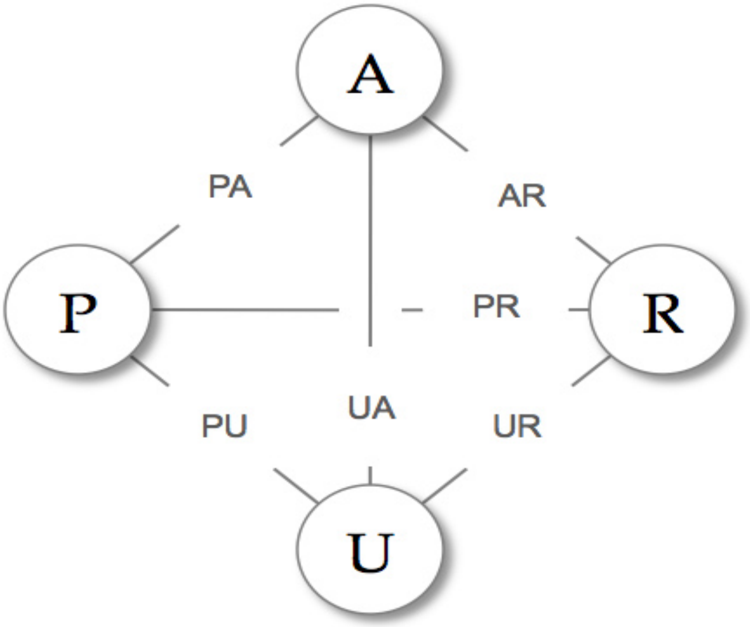
Preferences (local)

Social Graph (all relationships)

Identifiers (unique ids)



An architecture for all of this data looks like a database, so will need C/R/U/D plus lock (permissions infrastructure) “lock” is a DB lock to prevent contention (transactional locking), but also a “lock” where permissions are enforced as to who can see / update / delete. So locking in the ACL sense. (Not worried about transactional locking) Need a framework so you can do something. Then you can issue a card so that you can do stuff against this data.Diamond Frameword -6 different protocols that used different names.



http://www.incontextblog.com/

Four actors

As you can see at the left there are four actors. We introduce them now:

- **U** - A local **U**ser agent. It may be as little as a browser. It may include an OpenID, WS-*, password or SAML IdP, selector client. It may include a local personal data store. It works on behalf of the user.
- **R** - A **R**elying or **R**eceiving site or application
- **P** - A service or data **P**roviding site

Medical Service conversations are coming upon the same set of discussions and conclusions
Raising the BS card – authentication vs. authorization. OPenID and SAML are authentication mechanisms. This diagram is authorizational concepts. There are policy asserters, decision points, assertion points and repositories. The problem is that there should be multiple entities for P, looking at P as a single entity will create confusion. This is a useful diagram as it brings together the concepts, but you do need 3 entities, P1, P2 and P3. By the same token, each of the entities may need multiple instances. The asserting party in this case was the data authority. United Airlines may be requester.

Proposal that VRM does live in the policy later, but we need to understand that policy needs to be under user control rather than vendor control. At the VRM workshop, there was a session on the Personal Datastore, this is the hingepoint of VRM. We may have multiple of those. Vendors all have the CRM side of the system, if two or more vendors want to collaborate to serve the individual, then they will have to exchange data. If you had a persona at in each of the CRM systems, then your central datastore would be able to talk to your personas inside each of the CRM system. One of the key requirements there would be to look at all of the taxonomies and schemas sitting at the vendor side – your schema needs to be able to talk to all of these. (imagine the integration required simply within each of the systems)

First you need to create a system whereby the user can manage their personal data store.
The challenge is that there a known mappings – for example credit card and banking systems.
There is a distinction between known mapping that the systems understand it and the user having some transparency into this system and the relationships

Are we suggesting that the user should be involved in rationalizing their data. If there is a financial incentive, then it will happen. E.g. Visa and the bank. If the user had enough financial incentive, then they will do this.

Can users do the mapping?
There is a new class of service provider (4th party) who are the custodians of the data.
CRM systems are based on some data and the vendor guessing the rest of the way about what you want. A user should be able to make a request of the vendor and rely on that vendor not to upsell, cross-sell, etc. – a pure service. The person at the center of the system, in reality, the attributes of that user are not really owned by the user. The control is the person that controls access to the data. The individual will appoint a party to manage their data on their behalf. In many cases, what entities need are not values of the attribute itself, but confidence that the data is true and accurate. Amazon don't need to have my CC number, but only the authorization from Visa that the bill will be paid.

Distributed Identity Based on Relationships

- The current Identity representation based on what you know, what you have and what you are is inadequate
- This label based identity can be easily stolen or compromised
- Hacking attacks such as phishing and pharming, man in the middle attack, man in the browser attack, replay attack , attacks by viruses and Trojans are the reason for compromising identity (not considering stupid mistakes by users giving away their identity)
- Distributed Identity is based on a new paradigm on who you know, in addition to what you know, what you have and what you are. This is how trusted identity is established in the real world
- Digital certificates, multi factor token, site-key images, soft-key pads do not provide the security that they are claimed to provide.
- The most effective way to protect identity theft from the above mentioned attacks is through mutual authentication.
- In distributed/relative identity we ID the link/relationship and split it (mathematically) in to two or more parts
- The mathematical is known as the Distributed Identity Graph (DIG)
- REL-ID prevents phishing and pharming, man in the middle attack, man in the browser attack, replay attack , attacks by viruses and Trojans.
- The properties of REL-ID are:
    - 2-WAY (or split) IDENTITY REPRESENTATION
    - 2-WAY AUTHENTICATION PROTOCOL
    - ZERO-POSSESS
    - ZERO-TRANSMIT
    - MULTI-IDENTITY (server side)
    - MULTI-IDENTITY (client side)
    - MULTI-FACTOR
    - DYNAMIC IDENTITY (one time use)
- REL-ID properties and deployment are consistent and compatible with the requirements of Lim Cameron's Seven Basic Laws of Identity.
- REL-ID product suite:
    - TruSite: A Website Authentication Product
        - Automatically checks the websites' identity for the end-user
        - Form factors include – IE Toolbar, FireFox Toolbar
    - TruTerm: Secure Branded Online Banking Terminal
        - Secure banking terminal with in-built multi-factor, mutual authentication
        - Protects against all known attacks on Internet Banking
    - TruAccess: Corporate ExtraNet
        - An EXTRANET landing platform for providing access to enterprise applications
    - TruNet: Corporate VPN/Secure Internet Access Point
        - A VPN solution for providing access to enterprise network resources

    - TruMessage: Secure Corporate Messaging
        - A Secure Enterprise eMail solution that removes all security vulnerabilities in the current eMail infrastructure
- httpr:// Instead of or in addition to https://
- Future plan for federated identity, Multi Level Security

Discussion Notes:

Key Understandings

- Use of relationships of links in addition to labels/attributes
- Identity is inherently distributed in terms of high value relationships
- We are really protecting the relationship and not just the label based identity part.
- Even if one link is compromised, the other links are operative
- In order to spoof the bank one needs to steal a million split identities of the customers, and at the same time keep pace with the dynamic changing identity in each case.

Outstanding Questions:

- Why do call mutual authentication as a piece of identity? Why not call it just authentication?
    - This was the problem of separating authentication as part of the identity representation that led to the current limitation. Each relationship link (authentication is just a means for validating it) is a piece of the identity in the distributed identity paradigm.
- How do you generate keys? What about revocation?
    - The keys are generated similar to the RSA algorithm and the secure communication is similar to Diffie Hellman algorithm. However, the REL_ID keys are not limited like the PKI keys. The practically unlimited equal to the number of atoms. Revocation is not needed since there is no practical limit on the leys, and hence there is no need to revoke and reuse.
    - Each party can stop a relationship (terminate a REL-ID) transaction at any time. The client and the bank are on equal footing. However, to create a REL-ID they need to follow a process and establish a prior trust.
- How is the REL-ID split identity generated? What is the Z-ID sever tries to keep a copy of the client piece of the split identity.
    - The Z-ID sever is implanted behind the de-militarize zone of the bank so that when it generates a split ID (Rel-id) it keeps the bank's part and sends the customer's part. BY policy it is not allowed to keep the hashed version of the customer's part.
    - In the current PKI implementation, that is the biggest weakness. Though the private keys are not supposed to be kept, they are kept by the sever, so as to be re-used when the keys are revoked. In REL-ID implementation, since practically there is an unlimited number of REL-ID keys are available, there is no need for key revocation, and hence there is no need to keep the client part. Even if the worst scenario if it is kept, it may be practically useless, because the REL-ID keys change with every authentication. With millions of customers with thousands of transactions, the need to manage billions of keys by itself becomes nightmare, simply not worth the trouble.

Observations/Suggestions:

- If possible do not propose httpr://, instead hide it under https://
- REL-ID may very relevant for Active cards vendors. Talk to them.

Action Items:

- Arrange another session to demo REL-ID and answer further questions

Do people want to own and manage their identity?

URL Do People want to Own and Manage Their Identity
Convener: Ernie
Notes-taker(s): Scott David
Other Members: Kent Jepperson, Nika jones, Chris Messina, Justin Richer, Gulshan Kapoor, Ernie Prabhakar, J Trent Adams, David Eyes, Karon Webber, Katrika Woodcock, Andy Dale, Mike Osburn, Chris Luna, Monica Keller, Laurel Boylen, Mainak Sen, Daniela Barbosa, Love Hornquist, Rachel Murray, Vittorio Bertocci, Rajesh Pandey, Jim Meyer, Will Norris, Terrell Russell, Dean Landsman, Stephen Weber, Mark Lizar, Dorothy Gellert, Anthony Eden

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

People care about identities less than they care about relationships and -------------.

Problem with metaphor – look for metaphors, but carry the baggage. Chris lunt talking about identity issues. Progressive revealing of information over time.

What do people want to manage - The relationships and the amount of trust they receive.

What is identity – Is identity in this context the one person and their outward manifestations, or is it each relationship being its own identity. There is a free speech aspect to identity. Which concept of identity do you care about.

Identity should be invisible. It is not an end in itself.

Benefit of identity is the capacity to take credit – attribution. Way to prove what you can do.

Two camps – Identity cautious – care about identity
Operational aspects – want easiest user experience.

Want folks building the protocols to ______.

Which me are we talking about – managing multiple identities. Which me is involved.

How to you manage multiple persona metaphor.

All try to be integrated people and have disjointed roles that not want to overlap.

Only want to deal with multiple dimensions when needed. Context sensitivity.

It is about context. All enjoy so many contexts, cannot manage them in particular fashions.

What does the individual want now. Most people not thinking in a complex way. They want a simple – fear and satisfaction. Build in the simple. Don't overthink it.

Apply metaphors to simplify the discussion.

Something to enable it and make it simple. Build into the code, the ability to make it simple in every use case.

3 things must get right

1. Some type of identity management – for transactions and attribution/authentication.
2. Must have control
3. Must have transparency – so have comfortable

This is where VRM comes in – decide how much of what data want to reveal at the moment.

No one goes out to buy car because they want to change oil.

Also, people worry about the automatic collection of information "behavioral advertising" That is an issue.

That is where gets so complex. Automated elements.

Difference of identifier and identity.

How would user manage

How make it easier for people who want to manage their identity,

Concept of a selector – Some folks want an identity manager that can trust to do most of the things correctly most of the time.

Have identity management by third party that is agnostic, neutral.

VRM – How do you get to implementation.

Financial model – can manage it yourself, can manage it through third parties. What are the incentives

Moving value around the net. Interested parties would rather not recognize that value, so that users won't require to be paid for that asset.

Make it more like currency, change the dynamics. Money is not copyable.

Gray area between hard fact and reputation.

Good system allows correction.

Future uses of pieces of data that putting out there that cant imagine now. Great argument

People don't want to manage their identity, but want to manage what other folks do with their identity.

Only way to manage is to dilute.

All of this data being collected

Hazards of the communication of information that want to keep things secret. Having privacy

Anonymity is the best shield from the tyranny of _______./

Need to establish what the terms of engagement are – what is the digital deal. The net effect of .

We have the chance to be the first tech initiative to calculate and the benefit and burden

What is the digital deal ?

Session 2

Financial Institutions as Identity Providers

URL Financial Institutions as Identity Providers
Convener: Guillaume Lebleu
Notes-taker(s): Tom Brown
Other Members: Robert Pinneiro, Scott Loftesness, David Eyes, Guillaume L, Tom Carroll, Tatsuki Sakushima, Bill Shupp, Robert Guthrie

Technology Discussed/Considered: OAuth, OpenID

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

Guillaume: Although the vision of banks as identity vaults/providers has been around for 10+ years, today there isn't any bank that is an identity provider. Why? One explanation given is that financial institutions will not accept to take on the responsibility of the liability risk. The question then is: how can we reduce this liability risk? For instance, can we follow M-Pesa foot steps of providing financial services but with limited balances to reduce this liability risk? Or use Pre-paid cards?

Bob: A better explanation is the simply that there is not a business case. If the relying party would agree to pay banks to provide that service, then they may do so.
In other words, "Once banks figure out a way to make money as identity providers, they will become Id providers".

Scott:
Wells Fargo has a digital vault service, but no identity-related service, just a place to put secure documents.

Tatsuki:
Government regulations related to consumer rights to know what information is stored about them provide a great business case for an identity provider to store private customer information and others to rely on them. In Japan, strict consumer rules are defined: consumers must be albe to revoke access to their information. Compliance with these rules is expensive and some service providers may prefer to become relying parties.

Scott:
Equifax seems to be a good identity provider. They haven shown interest (they already provide an 18 year old Information Card). They have verification services. They also have most US residents as customers/users. This is not the case for Wells Fargo, which can only market to its customers.

Guillaume:
Another topic is authorization delegation to bank account via OAuth. Currently, with Mint, you have to provide your online banking username/password. Mint does not store your credentials, but they are stored by Yodlee.

David Eyes: It seems that we are talking about big-i Identity and small-i identity. Banking information relates to big-i Identity.

Guillaume How to transform Identity to identity? Breaking it into pieces? For instance, a prepaid card with limited amount or a virtual currency.

Scott:
Fees are an issue in prepaid case.
Paypal is introducing family accounts.

Identity Business Models

URL Identity Services Business Models
Convener: Bob Blakley
Notes-taker(s): Bob Blakley
Other Members: Daniela Barbosa,Hank Mauldin, Jeff Shan, Chris Lunt, Drummond Reed, Gulshan Kapoor, Pete Rowley, George Fletcher, Katrika Woodcock, Pak Maark, Keith Dennit, Henrik Biering, Lucy Lynch, @tharon, Praveen Alavilli, Mary Ruddy, Phil Windley, Alex Nennker, Steve Williams, Andrew Nash

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

Identity services businesses exist today which offer authentication, federation hub provision, identity attribute vetting, identity risk assessment, user experience augmentation, compliance assistance, breach remediation, and whitelabeled IDP services; companies are already making money in these areas, usually by charging RRs or IDPs on a per-transaction or per-user-per-month basis (often with an initial setup fee).

We discussed other areas where services have yet to emerge, including revocation (I want to ensure that a company has actually erased some data I shared about them), escrow services (a few of these exist including ability to anonymously exchange domain names for money), and personal agents (or "advocates" – like a concierge).

The VRM discussions are relevant here – services which the VRM community calls "4th parties" (we prefer a term like "advocate" or "user agent") are not yet widely available but seem to offer value. There are also a few other kinds of services: user identity risk management (e.g. Lifelock, reputation defender), Social facilitation (Poken), user sponsorship (InCommon identities used by students to access banking services), User-oriented profiling services (Garlick, which collects transaction information for the purpose of making it available to the user rather than to relying parties). We discussed the need to examine the history of emergence of banks, stock exchanges, and credit card networks as models for emergence of 4-party agency systems in the identity space.

OpenID For Desktop Applications

URL [OpenID For Desktop Applications: How? When?]()
Convener: Infinity Linden
Notes-taker(s): Brian Eaton

Technology Discussed/Considered: OpenID, Oauth, Second Life

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

Challenge: desktop app wants to accept OpenID login credentials, but doesn't want to

a) open a web browser at all
b) display web page from OpenID provider

First proposed solution: ask for username and password of OpenID provider, use some standard mechanism to send username and password to OpenID provider. OpenID provider then verifies password and returns "here is their identity."

Objections:

1.doesn't work if IdP doesn't use usernames and passwords
2.messes with the OpenID ceremony (no URL in browser bar, users won't feel safe).
3.OpenID providers don't like it when other people scrape usernames and passwords.
4.Does worse in some usability studies, because users with password managers might have forgotten their password at the IdP.

Next proposed solution: use OpenID + Oauth.

First use of application: user downloads application from www.secondlife.com. SecondLife redirects user to OpenID IdP. IdP asks user to confirm login, then returns user to secondlife.com.

When application starts up, it starts the Oauth dance with secondlife.com, then opens browser to secondlife.com. User already has secondlife.com cookie, so there is no redirect to OpenId IDP. User is then asked to confirm that they want the secondlife application on their computer to access their secondlife data. User says yes.

Application gets Oauth token, uses it to pull data necessary for application to run.

Next use of application: token is saved on computer, so no browser window necessary. Things just work.

Edge case: user needs to switch Ids in desktop application, or application state is lost (user switches computers). Solution is to start Oauth dance, then open browser window to secondlife.com. Secondlife.com redirects user to OpenID IdP.

IdP prompts user to login, then redirects to secondlife.com.

Secondlife.com asks the user to confirm application access (the Oauth ceremony).

Browser window closes, desktop application gets Oauth token and uses it to fetch user data.

Problem: if someone becomes an OpenID RP, and then the IdP becomes malicious/attempts to put the RP out of business, how can the RP recover?

Option 1: signed contracts between IdPs and Rps

Option 2: RP asks for e-mail address, so if they don't like the IdP they can put the user through a password reset process.

Authorization Without Boring Crypto

URL Sharing Permission RESTfully with Web-Keys
Convener: Hans Granqvist
Notes-taker(s): Anthony Eden
Other Members: Terry Hayes, Tyler Close, Alan Karp, Ashish Jain, David Primmer, Karon Weber, Anthony Eden, Scott Seely, Vittorio Bertocci, Joaquin Miller, Eve Maler

Technology Discussed/Considered: REST

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

The main problem trying to be addressed is crypto in authorization. Crypto is considered challenging and causes too many implementation problems.

http://nocrypto.com/wiki

Authorization
Resource: http://example.com/foo
Operation: GET/POST/PUT/DELETE
Assignees: http://tyler.com/ or http://twitter.com/

Verifiers
http://verifier.com/1234 (not quite sure what this is for)

Side Discussion - Use Cases
Data Dominatrix - Authorize a feed of data
Hey, Sailor - Public URL but requires "payment"
... - Authorize content not yet created

Authentication or Authorization – Can We Move To Verification Now

URL Authentication or Authorization? Can we move to verification Now?
Convener:
Notes-taker(s):
Other Members:

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

Identity & Privacy – Who To Trust With All Your Data

URL Identity and Privacy - Who to Trust with Your Data
Convener:
Notes-taker(s):
Other Members:

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

Identity Quartet and User Driven Identity

URL Identity Quartet and User Driven Identity
Convener: Joe
Notes-taker(s):
Other Members:

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

- Achieved Separation of Concerns
- Justified the separation
- Discussed uniqueness and relations between the 4 types of identifiers
- Hazards of using real world artifacts (eg. SSN, bank account #, etc)

Session 3

Higgins Cloud Selector

URL Higgins Cloud Selector
Convener: Markus Sabadello
Notes-taker(s): Markus Sabadello
Other Members: Sorry forgot to do the list

Technology Discussed/Considered:

Higgins “Cloud Selector” http://wiki.eclipse.org/Cloud_Selector

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

The Higgins “Cloud Selector” is a web-based application that allows you to access and use your i-cards without the need to install anything on your local machine. It uses OpenID Attribute Exchange as a transport layer to move claims and entire tokens around.

It’s useful in situations in which you don’t have a locally installed selector, but it also has downsides such as reduced security and privacy.

The Cloud Selector can operate in different modes.. It can work with any existing OpenID RP, and it can work with special RPs that take advantage of IMI features.

It tries to internally map IMI claim identifiers to OpenID AX and SREG attribute identifiers.

A question came up on whether the same user experience could be achieved by a traditional OpenID. The answer was that this is mostly true, except that the Cloud Selector also offers the possibility to transport entire tokens (as opposed to just simple claim values).

Next steps:
- Improve UI
- Display requested / optional claims to user and let them choose the optional ones they want to send

Installed Applications and Online Identity (keeping users happy on the desktop vs on the web)

URL Keeping User Happy on the Desktop vs. On the Web - IIW
Convener: Andrew Nesbitt, Ariel Gordon
Notes-taker(s): Brian Eaton
Other Members: Steven Herbst, Katrika Woodcock, Karon Weber, Peter Tapling, Rajesh Pandey, Tatsuki Sakushima, Gerard Tse, Abraham Williams, Vittorio Bertocci, Meadhba Hamrick, Doug Whitmore, Skip Baney, Andrew Nesbitt, Tom Carroll, Love Hornquist, Greg Haverrkamp, Brian Kissel

Technology Discussed/Considered:

Installed applications and online applications.
We stayed away from specific technologies.

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

What problem are we trying to solve?

How do you link your computing device identity to your online identity?

Computing device:

1.sometimes shared, sometimes not. (Smart phones are generally only used by a single person, computers more likely to be shared.)
2.If a device isn't shared, user switching is not as big a problem.
3.All full-fledged PCs have "fast user switching" so you can have one real person per OS session.
4.Expectation: if my spouse uses my PC, s/he switches session.
5.Reality: OS session doesn't change, but browser session does. Spouse logs me out of my browser, but doesn't do the fast user switch.
6.This can mess up installed applications that get confused between the browser session and the OS session.
7. Good installed app behavior: know about both browser-based identities, ask the user which they want to use.

Challenge:

- what if you don't want to create a new user account? For example, my friend is here for 5 minutes and wants to check his e-mail. Proposed solution: click a button that says "Guest" account.

Experience from google:

- approximately 0% of enterprise users actually use "fast user switching"
- consumer number is about 1%.
- google has needed to make it easy for users to switch identities in the browser, without relying on OS support.
- This is a ton of work for web apps to support (a single authentication cookie might authenticate multiple users, it's a pain to code in that environment.)
- users want to be able to cut and paste between accounts
- frequent complaint: can't use gmail account and adwords account at the same time. Users end up learning how to open two separate browsers at once.

Experience from AOL:

- it's not that OS user switching is bad, it's that users can't find it.
- AOL client does a good job of showing the user which identity they are using at any given time.

Question: are users confused by having two identities in the same browser?
Answer: so far it hasn't resulted in huge confusion

User experience: shared computer, iTunes account is always showing preferences for wrong user (showing kids music preferences to someone who doesn't buy kids music. Wife buys kids music.)

Q: should the OS detect when the browser switches identities, and switch the OS identity at the same time? Good idea, bad idea?
A: room is confused. Details ensue: when user switches identity in the browser, thick client apps would pick up the change as well, e.g. User switches e-mail addresses, thick client calendar app switches to new calendar at same time.

Expected behavior might vary by thick client app.

Example: user has 10 tabs open. Spouse walks over to computer, logs out of gmail. Do the other 9 tabs switch identities as well? What about the thick clients?

Some concern that users will be surprised/confused if clicking logout of gmail changes everything on their desktop.

How do we decide which identities switch?
Strawman proposal: only the identity in the tab changes.
Strawman proposal: all the apps using identities from the same provider change.

Q: why don't users use fast user switching?
A: it takes a little longer. Sharing data across OS accounts causes headaches. Users aren't trained to switch. Users don't mind sharing an account.

Boundaries of user data and boundaries of user accounts are frequently different. Different househoulds draw the boundaries in different places, and user account is not a natural metaphor for non-computer users.

User gestures can be a good way to figure out what is required, can give users an option:

- “private mode”: used for birthday shopping, browsing pornography, other stuff that must be private
- “shared mode”: default, everything is shared
- “parents mode”: parents can switch into this mode.

Experience: need three twitter clients installed to manage three twitter accounts. This is annoying.

Proposal: have a “work” profile and a “personal” profile. Lots of people despise this idea, they don't want to ask the user which profile to use, they want to import work data (say, paycheck data) into personal apps (like Quicken/MS Money).

Challenge: OS user accounts have too much privilege and data separation.

Room consensus seems to be that applications need to support the affordance to let users choose the sharing model for data. Simple model of “all applications are separate” seems too simple to express the kind of data sharing that users want, so applications need to have data sharing built-in.

Decisions should be incremental, so that users can figure it out as they go.
Actions should be undoable, so they can recover when they make a mistake.
Results should be obvious, so they understand what they've done.

Installed apps should have a notion of multiple accounts/data sources, and provide a light-weight way to switch between them.

Problem spaces identified:
- Multiple personas for the same person (multiple identities on AOL or second life)
- Multiple users on one computer (shared PC in a household or a library)
- shared resources (shared iTunes library, shared pictures folder, shared webmail account)

User switching:

1) At OS level -> global, also applies to all online accounts automatically.
2) In the app/in the browser
    1. Can propagate to all "connected" apps, e.g. Desktop widget shows calendar of user at browser, switches when user at browser logs out.
    2. Can choose not to propagate
3) Something else...

Filtering the Noise in Activity Streams

URL Filtering the Noise in the Activity Streams
Convener:
Notes-taker(s):
Other Members:

Technology Discussed/Considered: (TAGS)

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

Role As Identity and Organizational Trust

URL Role as Identity and Organizational Trust
Convener: Justin Richer
Notes-taker(s):
Other Members:

Technology Discussed/Considered: (TAGS)

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

- Roles as attributes to identity
- Entitlement and privilege escalation decided by users
- Need for Digital "Day Passes" for visitors
- Hard problem when network is unbounded

Session 4

Pain of becoming an OpenID Relaying Party

URL Becoming an OpenID Relying Party
Convener: Luke S, George F
Notes-taker(s): Brian E
Other Members:

Technology Discussed/Considered:
OpenID, UX

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

Six months ago, there were no practices at all, let alone best practices.

We now have more experience, but we still don't have all the answers.

Things to consider -

- Password
- single signout
- user choice "nascar"
- linking accounts
- delegation, or "the ugly long tail"
- data
  - ○ coppa
  - ○ contacts

- technical issues

Question: should user consent pages offer granular choice?
Answer: granular choice causes success rate to fall off a cliff.

How can users get more control?
Maybe relying parties can ask the user; the user has more context at the RP site.

Example: facebook asks the user what they want to import from Google. User selects address book, but not photos. Facebook asks the user only for contacts. This offers user control without requiring users go through a bunch of checkboxes at the RP.

We lose a few percent of people at the approval step because of their privacy concerns.
We lose closer to 15% if we offer granular controls on the OP approval page.

Best practice: if an application doesn't require contacts, don't ask for them. IdPs should disincent applications from asking for two much data.

Demo embarassment: RP checks whether an IdP account has already been linked to an RP account, errors if that occurs.

Useful trick: let relying parties discover whether the user is already logged in at the OP, e.g. Use checkid_immediate.

Problem: logging out of facebook doesn't log you out of OpenID IdP. If OpenID IdP offers a “remember me” button, you can't log out of the RP site.

Suggested solution from Luke: every single RP page checks whether the user has logged out of the IdP on every page view. This is what Facebook Connect relying parties do.

This terrifies all of the IdPs because of load.

Different relying parties have different needs:

- small sites can rely on IdP to do everyting, even session management
- larger sites don't want that.

Single logout use cases:

- leaving an internet cafe: you want single logout
- leaving one web site: you might not want single logout

Technical challenge: Scott Cantor believes that single logout is “impossible” based on experience from SAML.

Unfortunately, you can't do logout from a single RP if you also support automatic login.

Alternative: maybe make automatic login require a single user click?

Statistical evidence: the more sites that are impacted by single logout, the less users click the “logout” button.

Users are sometimes surprised by SSO; user surprise is a bad, bad idea.

Proposal: when user clicks logout button at RP, RP displays a message saying “you have logged out of the RP site”, and offer a link to signout of the IdP as well.

RP challenge: need to get XRDS file for return_to/realm verification right, or you get an ugly warning from the AOL IdP during sign in. Also need to get a privacy policy in the right place. All of these things require consulting with lawyers to get them fixed.

Problem: users click “Login with Google”/”Login with Yahoo” button even if they haven't used OpenID before and they actually have a password at the RP.
Solution: IdPs should provide e-mail address to allow account unification. Relying parties should only trust e-mails if the IdP is authoritative for the e-mail address.

This is a huge pain for IdPs like AOL that offer lots and lots of e-mail domains.

Signing in to AOL example:
AOL has to prompt for bithdate for COPPA reasons.
Need to ask for display name, and e-mail, and captcha.
Had problems with Google openids because “account” is included in the OpenID URL.

AOL has a list of words that are forbidden in identifiers (for abuse/security reasons), and “account” was on that list. They had to remove it from the list.

Every OP you deal with has some idiosyncracy you have to deal with.

If you bury the UI where normal users don't trip over it, you can make the OpenID ceremony work.

If you put it in your main flow, it drops the success rate, and that's a non-starter.

Problems to solve to get it on the main flow:

- single signout

Attribute Exchange is a “nightmare”, because every OP has their own schema, and the schema is not discoverable. You have to read the OP doc to figure it out.

There aren't enough “good Ops” yet. Good OP:

- support OAuth/OpenID hybrid to get data
- support automatic login to improve return login
- returns e-mail for account linking

Why aren't there more relying parties? It's not useful enough.

Key metric: signup friction has to go **down.**

RP best practice: ignore the URL the user entered, use the claimed ID returned from the IdP. There are too many cases where the URL the user entered can be wrong/mismatched.

Generational recycling: nobody actually gets the fragment stripping right.

Too many corner cases: delegation is a pain to support.

What are we going to do about this?

- better specs?
- Bilateral bug fixing?
- Branding program (consensus: no!)
- interop test matrix with expected results?
- Automated test suite that IdPs and relying parties can run?
- No unit tests ---> poor software quality.

Becoming an OpenID Relying Party

Additional Notes taken by Chris Messina:

Issues

- password?
- single sign-out
- user choice ("NASCAR")
- linking accounts
- delegation or "the ugly long tail"
- data
  - coppa
  - contacts
- technical issues
- Google has found that asking users to make choices during authentication
- Eric Sachs: RP should ask for what it needs and nothing more... basically consent request should be made on RP ("who is asking for consent?" "how important is granular release of data?")
- users aren't smart about making decisions about releasing their data
- google loses 15-20% of people when they add privacy controls; not having privacy controls costs 3%

Demos

Enhanced Transaction Model

URL [Enhanced Transaction Model Using InfoCards]()
Convener: Jeff Stollman
Notes-taker(s): Ben Sapiro/Jeff Stollman
Other Members: Andy Dale, Judith Bush, Keith Dennis, Bob Pinheiro, Mary Ruddy, Bill Smith

Technology Discussed/Considered: info cards

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

Problems with the current transaction model keep the identity discussion going in circles. We have not used a systems engineering approach where we look at the problem from a 50,000 foot level and then parse it into appropriately granular components.

People continue to look to solve a problem for his “silo." As a result, solutions overlap and their interoperability is limited. We need to break the problem down to its granular components in order to prevent the overlap, allowing us to build solution components that are easily composable for each silo or use case.

User is effectively a subject - says they want X but thereafter are external to the conversation

Traditional model includes 3 parties: Subject (User), Relying Party (Service Provider) and Identity Provider.

Alternate model adds a fourth actor – the Information Provider – which may be along the line of Paul Trivithick's diamond model or the VRM 4th party model. Information Provider is a trusted intermediary that caches/aggregates pointers to claims on behalf of the Subject. A Subject may have more than one Information Provider. (E.g., one for medical records, one for financial claims, etc.)

Alternate model also separates Identity Provider (who provides vetting of a Subject’s ipseity) and Claim Providers who vet various assertions about the Subject.

"Ipseity" = your fundamental and unique individual identity. You have one and only one ipseity.

There's something that you're uniquely you and the rest is just claims = they're often transient

Information Provider allows you to choose claims (mix and match) to create a selection of personas that you will use to deal with the various Relying Parties.

Relying Parties might have a similar Information Provider infrastructure (Identity Provider, Claim Providers, Information Provider) to allow verification that they are who they claim to be as well as allowing them to have different personas. Businesses will want different personas to show different faces to different (or even the same) customers. (For example, Kmart owns Sears but maintains each as a separate Persona.)

See attached presentation

Trusted Identity
Transaction Model wit

Expert Identity

URL [Distributed Expertise Location]()
Convener: Terrell Russell
Notes-taker(s): Chris Lunt
Other Members:

Technology Discussed/Considered:

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

- Focusing on the answer will fail the person asking the question
- Finding affinity between the questioner and the answerer and initiating the relation is what's important
- Aardvark is working on this problem
- To combat the problem of getting a critical mass of experts, use authorship of document to seed the corpus. You need to add the expertise into an existing social structure. It is a layer.
- Questions may not be routable by the asker. Nor may they be the best person to rank the result. But it may be good enough
- How do you tag people in a way that gives strength scores.
- How to you create the incentive w/in organizations to do the work to measure and offer expertise?
- Decay of expertise needs to be captured.
- What if experts don't want to be found.
- Is there a way to associate costs for availing yourself of particular expertises.
- What are the currencies in these cases. ("whuffies!")

Action Cards Part 1 & 2

URL [Action Cards]()
Convener: Phil Windley and Drummond Reed
Notes-taker(s):

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

Kynetx Network Services and Action Cards

Action cards are a type of information card that control actions in the user's browser and elsewhere. Action cards can create cross-site, context-aware Web experiences.

Kynetx Network Services, or KNS, is a system for creating action cards. KNS is designed to make it easy to create context-aware browsing sessions that respond to user context to deliver better, more customized experiences. KNS provides an abstraction layer on the Internet for creating cross-site transactional context in support of context automation.

KNS has several important features that make context automation easy and effective:

- KNS is Web site independent. KNS is designed from the ground up to work with any Web site.
- KNS works across Web sites. KNS responds to user context, even when that context includes information the user collected at another site.
- KNS is browser independent. The KNS system works with all modern browsers.
- KNS is context-aware. KNS makes use of permissioned, personal information that the user supplies as well as ambient data about current and past browsing episodes.
- KNS is real time. KNS is constantly working in the background to provide context-aware interactions that are customized to user, page, and moment.
- KNS is secure. Because KNS is based on Information Cards, KNS provides a secure, private environment where context is shared under user control.

KNS provides better, personalized experiences to users and at the same time allows Web sites to be more responsive to user needs. This is the basis for a relationship between visitor and Web site that engenders trust and loyalty. KNS does not mediate that relationship, but enables it by providing a richer foundation upon which mutual reputation, trust, and loyalty can be built.

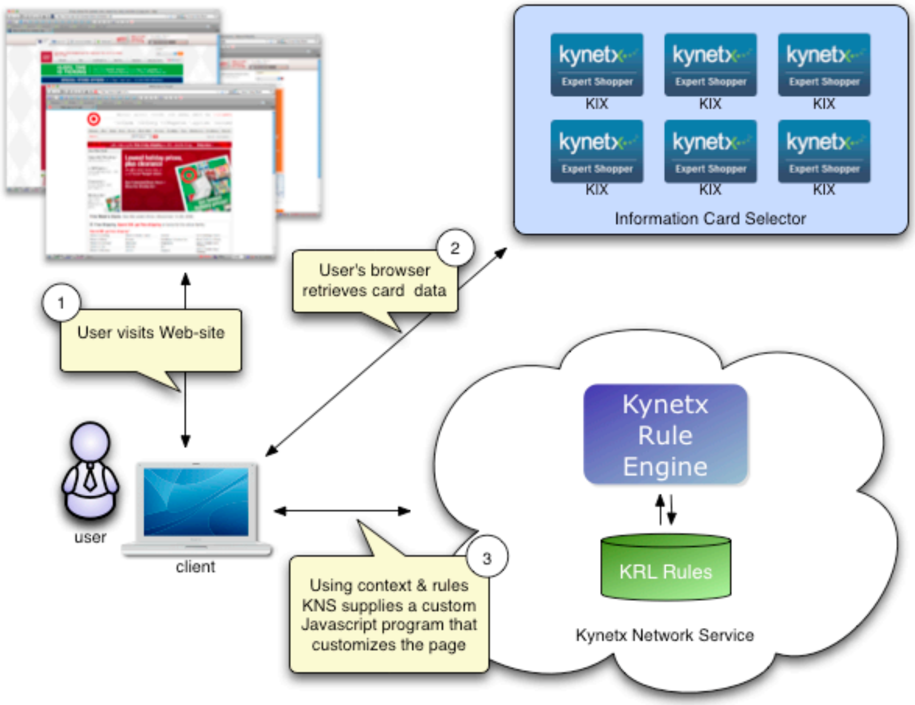
HOW KYNETX WORKS

KNS depends on three inter-related technologies to accomplish its work.

- **Kynetx Information Cards** (KIX) provide Web site independent identity. Specific cards, through the claims they contain, activate functionality inside the browser. KIX are simply any Information Card with appropriate metadata.
- **Kynetx Rule Language** (KRL) is a domain specific language that provides an abstract, linguistic means of specifying contextual experiences by customizing browser content.
- **Kynetx Rule Engine** (KRE) evaluates KRL rules in response to requests from the browser and responds with custom JavaScript code to be executed in the browser.

The interaction of these three technologies provides a means for companies, developers, and even individuals to create contextual experiences on the Web.

As shown in the following Figure, without KNS, users only interact with the Web site (1). Kynetx adds two critical components to generate structured browsing: the KIX in the information card selector (2) and the cloud service, KNS, that customizes the page based on the user context (3).


kynetx
Expert Shopper
KIX
Information Card Selector
2
User's browser retrieves card data
1
User visits Web-site
user
client
3
Using context & rules KNS supplies a custom Javascript program that customizes the page
Kynetx Rule Engine
KRL Rules
Kynetx Network Service

KNS customizes the page the user is viewing.

Kynetix Information Cards

KIX are standard Information Cards that also contain data about an associated ruleset. The Information Card Foundation has given the moniker "action cards" to Information Cards as used by KNS.

KIX are an abstract representation of desired functionality. When a person chooses a KIX, the functionality associated with that card is enabled in their Web browser.

Before a card can affect the browser, the user will download and install a card selector[1] and a browser extension that allows the browser to respond to the card selector and KNS. That one installation of a card selector provides the user with what amounts to a universal browser extension. After that single

[1] Currently KNS works with the Azigo selector because of its unique support for metadata. Kynetx has the goal of being selector agnostic and supporting a variety of selectors.

install, users gain additional functionality by putting small (< 3k) cards into the selector—a simple, secure, and friction-free experience.

The card selector allows the user to easily manage their KIX, including sorting, searching, arranging, enabling, disabling, and deleting cards. Disabling or deleting a card is easy and instantly removes the functionality associated with it from future browsing experiences.

The contextual experiences described in the previous section are all enabled through importing a card into the selector.

Kynetx provides a directory of some of the available cards called the KIX Directory. [2] This directory lists cards that people have chosen to share.

Kynetx anticipates a need to certify cards in some way. One proposed method is to create a certification program that would certify that the functionality associated with a KIX is safe, private, and secure.

Another proposed method would use a combination of information about a card based on an automatic analysis and a distributed reputation system driven by users to create a risk profile. Neither of these have been implemented yet.

Developers might offer KIX for free or for sale depending on the desire of the developer

Because KIX are based on the Information Card standard, supporting infrastructure is available from a number of vendors and their safety and security is based upon 15 years of research and development.

Kynetx Engine

KRE provides an API[3] that allows Kynetx rulesets to be stored, retrieved, analyzed and, most importantly, evaluated.

When a request to evaluate a ruleset is made to KRE, that request contains information such as which cards are installed, what claims they contain, the current state of the browser, and other session information. Based on this request, KRE responds with a small JavaScript program customized to the request. That JavaScript program, running in the browser, customizes the user's experience.

KRE includes a callback mechanism by which rules can communicate success and failure messages back to KNS. KRE provides A/B testing for rules and an analytics subsystem for monitoring rule actions and activity. A/B testing provides developers with the means for testing rules to determine their effectiveness and fitness for purpose. Analytics allows rule developers to see detailed data about how rules are being used and track which rules work and which do not.

The primary delivery mechanism for KRE is a cloud based software infrastructure service that responds to ruleset evaluation requests. Kynetx charges for ruleset evaluations on a CPM basis or on a

[2] KIX Directory: http://kix.kynetx.com/

[3] The API is described online: http://wiki.kynetx.com/pages/Kynetx_Network_Services_(KNS)_API

monthly flat rate per installed card. Kynetx is also willing to license KRE to companies wishing to run a private or semi-private KNS system behind their firewall or for their customers.

Kynetx Rule Language

KRL is the heart of the Kynetx system and the source of its tremendous flexibility and power.

KRL, as its name implies, is a rule language that specifies what actions should be taken when a specific set of conditions is met[4]. A ruleset is a collection of rules meant to provide a particular structured experience. The KIX that are in the user's card selector, along with the Web page that the user is viewing, determine which rulesets are used. Specific rules fire based on the context contained in the request.

KRL gives any developer the power to deliver contextual experiences. This gives developers incredible leverage that drastically reduces their development effort in several ways:

First, because KNS provides a kind of universal browser extension that works across operating systems and browsers, developers are freed from writing complex code in multiple languages. This represents the great bulk of the current browser extension development effort. Instead, they can concentrate on what they really care about: building the functionality they want to deliver.

Second, because KRL generates JavaScript code that has been tested to work in all modern browsers, developers can largely ignore browser compatibility—one of the great obstacles to writing a widely used browser extension.

Third, because of the power of its abstractions and its design for the specific task of building structured experiences on the Web, KRL gives developers a compact and easily used notation that provides real intellectual leverage. In short, one line of code can replace dozens of lines in a more general-purpose language. Changes to browsers or Web sites can be recognized and fixed in KRE once instead of in hundreds or thousands of individual programs.

Kynetx provides a simple interactive development environment (IDE) called AppBuilder[5] for writing and publishing rulesets. Kynetx anticipates that others will also build tools that support KRL.

A simple provisioning process allows developers to create a new ruleset and associated KIX. Then, using AppBuilder, developers add rules to the ruleset to create the structured experience. Developers can distributes cards in a number of ways, including online, in email, or even using social networking tools like Twitter or Facebook.

Benefits of KNS

KNS reduces risk and increases leverage for businesses wishing to offer their customers a contextual browsing experience. In addition, Kynetx supports users seeking better, more contextual browsing.

[4] KRL is documented online: http://wiki.kynetx.com/pages/Kynetx_Rule_Language_(KRL)_Documentation

[5] Kynetx AppBuilder, Kynetx, Inc. http://appbuilder.kynetx.com

Lastly, Kynetx gives developers an easy to user and powerful took for customizing the browser experience.

The following lists some specific benefits:

- KIX, KRL, and KRE provide an abstract means of adding functionality to the browser giving developers tremendous leverage.
- A Kynetx contextual experience is cross-platform and multi-browser without effort by the developer.
- A Kynetx contextual experience is more secure than one delivered by a typical browser extension. The only software running on the user's machine—with access to the user's private data—is the card selector and a single, simple, easily analyzed browser extension.
- The architecture of Information Cards is designed to put users in a position where they can control the release of their private data including any claims that are associated with their KIX.
- Security and privacy are built-in to the underlying technology.
- Context automation generates a trusted, secure environment where high value relationships can be built and maintained at lower cost.
- Users are freed from managing episode context and can turn much of that chore over to the browser.
- Users can customize and enhance their browsing experience using small, easy to manage tokens in the form of KIX rather than through large, bulky code-based browser extensions.

Reshaping the browsing experience to allow people to use the Web in a way that preserves episode context across multiple sites will transform the Web beyond what we can imagine. As we've discussed, three important trends are making this possible:

1. The browser becoming a viable platform
2. Cloud computing
3. The advent of Internet identity

By themselves, these trends will not change the Web. But when they are combined so that their individual strengths play off each other and wrapped in an abstraction like KNS, they promise to change the way people use the Web and increase the value they derive from it.

Context automation is a compelling shift in the world of computing. People who experience contextual browsing compared to the traditional ad hoc experience will wonder why it hasn't always been this way. As an individualized, real-time service that operates across multiple Web sites, context automation offers people freedom from the tedious chore of connecting the "context dots" between multiple sites and, as a consequence, streamlines browsing episodes.

As a platform, KNS provides an abstraction layer on the Web, making it easy to create context-aware, structured browsing experiences. Our vision is one that allows existing methods of using the Web to co-exist with context automation, increasing opportunity and decreasing risk for all participants.

KNS allows businesses to provide contextual experiences for their Web visitors by leveraging the context of individual browsing episodes. KNS gives developers a low-risk avenue for extending the browser with context-aware services that interplay with Web sites.

Kynetx offers a low-friction way for users, businesses, and developers to participate in this coming transformation of the Web.

User Driven Services

URL Characteristics of VRM QT video
Convener: Joe
Notes-taker(s):
Other Members:

Technology Discussed/Considered: (TAGS)

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

- Discussion of the 10 characteristics of successful user-driven services and designing a system that works at web scale. for more really awesome tips...blog.joeandrieu.com

Claims Tickets and OAuth

URL Claims, Tickets and OAuth
Convener: Yaron Goland
Notes-taker(s):
Other Members:

Technology Discussed/Considered: (TAGS)

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

Write up a proposal, it's interesting
Claims based security allows requesters to submit claims about themselves to the service who makes an access decision based on the claims. The claims themselves can come from token servers who hand out claims. Can we support claims and token servers in Oauth?

The group generally felt the answer was yes and this would be good thing to have in OAuth. So a request was made that we write up a proposal and mail it out to the OAuth lists.

Session 5

Identity Brokers

URL Identity Brokers
Convener: Ben Sapiro
Notes-taker(s): None – notes created post session by convener
Other Members: Jeff Stollman, Praveen Alavalli, Pak Mark, Peter Tapling, Hannes Tschofenig, Justin Richer, Michael Hel, Bob Pinheiro, Steven Herbst, Ashish Jain, Ray Valdes, Tom Carroll, Axel Nennker

Technology Discussed/Considered: Identity Broker

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

- There are repositories of identity information that will/may not be exposed to the identity commons
  - Banks that don't see a business model for exposing their reliable identities
  - Government agencies that have highly
- There is a role for an identity broker that:
  - acquires access to these authoritative information sources
  - generates claims on behalf of the user to present to relying parties
- The Identity Broker is an Identity Provider that uses someone else's identity data to support claims but assumes the role of the Identity Provider with associated liability
- The Identity Broker discloses the sources it used to create the claim/assertion and appends it as metadata to the claim/assertion
- Equifax is sort of an Identity Broker but delivers data as is (assumes zero liability) and doesn't tell you how it got the data
- There would need to be an identity proofing process that would query the private data source in a non-privacy invasive manner
  - Presenting user provided data set (my name is X, by DOB is Y, my drivers license is Z) for boolean confirmation by the identity data repository (these are all true, these are not all true)
  - Limiting/throttling the number of queries against elements within a user provided (you queried the same drivers license three times while varying the name and DOB, therefore, you must be fishing, so go away)
  - Would require a strong consent model – "user A, I will query the following data sets to generate the claim you requested, is that ok?"
- Conclusions:
  - Need uses cases
  - Need policy on user privacy protection and pass-through of claims information
  - How does an Identity broker show that it's done a claims transformation while still remaining relationship to the original data (or is it just a legal/trust me approach)?
  - What are the responsibilities and legal obligations of an Identity Broker?
  - What's the mechanism for exposing the Identity Broker's source data so that RP's can make conclusions about the reliability of the claim?

Legal Meeting – Mapping the Gap

URL [ID-Legal "straw man" blog]
Convener: Lucy Lynch
Notes-taker(s): Scott David
Other Members:

Technology Discussed/Considered:

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

Lucy introduced the ID Legal working group.

Notes mapping the gap issue

Questions that technologists and legal/policy bring to the table.

Dan also looking at way to raise and answer questions online – Ways to explore the issues. Blog, hypotheticals, etc.

Dan – E-mailed Lucy a summary of issues.
[link here]
It is a summary of issues in the area of identity.

Dan is working on branded blog relating to identity. Lucy mentioned doing scenarios to post of ID commons wiki. So can have general discussion of legal issues that may crop up in identity. Challenges include ethical constraints. Question of rendering legal advice and atty client relationship. Fear of suits for malpractice. But it is something to explore. Could be a valuable resource. Also can help to educate the client.

He has looked at project management folks looking at scenarios.

Question of how make space attractive to folks to post concerns. Also, how structure so that identify the legal issues.

We moved to Dan's summary for discussion.

Dan went through law journals, blog posts, and mined the various postings. What are conceivable issues that clients interested in. Very general list. Suggested issues that thought were relevant.

Question of level of how out of sync. Laws and technology are. Digital signatures for example.

Personas, avatars, metadata, biometrics, presence, privacy and security, impact of mobile devices, trusted credentials, anonymity incomplete.

Lucy says lets talk about the process instead.

2 points on process

Resource on Q&A
Encourage dialog

Context of ID legal interactive space.

Biometrics
To what extent do best practices fit into identity
Maybe not want to focus that narrowly.

Transaction histories
Identify areas of concern.
First question to ask might be who owns your transaction history. Maybe own and control.

How is it used.

What kind of standard reusable architectures are applied. What architectures at the business, legal and technology level are applied. What kind of standardization could be applied and could it be automated.

Can it be transparent

When architect legal backgrounds, is there any way to make it non-waivable to preserve

Veracity of the identifiers in the payment history. Is it reliable

Whether or not ownership can include the notion of permissions, and the application of conditions based on context. Asset include conditions for reportage and leveraging. Reciprocally agreed means of control. Conditions that could apply to the confidentiality based on context. Based on mutual interest. Need teeth to support. Could consider, what default sets apply if left changed.

Need to put in framework around affinity – Framework of 3x3 matrix touches on assurance, legal structure law, regulation contract and on the other matrix privacy assurance liability.

Interest in future transactions stuff. Should be a standardized contract to use for future transactions. Standardized way to deal with agreements.

Legal differences of transactions that are not denoted in legal tender. Barter and virtual currencies.

What happens after death.

Move to discussion

Treat as something else

Something that can be thought of as property – can alienate
Person hood

EU has different defaults
US if I transaction with you and you are not regulated. Own the information jointly and severally.

Highly undertheorized – None of this is developed.

Robust emergent model – conceptually dominant around personhood.

Best single treatment is from the OECD. Paper on personhood.

If identity is emergent – what use as structure for discussion.

How should we attack the issue –

One way is to do this is summer project of Media lab and Berkman center – civic engagements. Dazza offers software. Using it for crowd sourcing of legal questions.

Also, pattern language on group process. Outlining that and then doing search

Could use bar associations.

When does identity matter.

Question of providing open forum processes – not really a help. What do people think is a plausible deliverable. What are people building? Tell me what you are building and I will go write about it.

But want to create a space to develop a cohesive community. Focus is on community, not just space.

Prompt could be t e presentation of a problem statement. Unique problems here. Presented.

Suggestion of a process where start with a survey-type issue. Here is a legal project related to identity, understand what is already happening and problems not already attacked. Resource for lawyers to get up so speed. Recruited legal minds into the space. Might be helpful to the business folks. Suggestion is way to provide a simple framework. Survey course. What is going on. Use a FAQ to present.

Alternative is a more dynamic/shared learning approach. May look like an understood definition of terms. When have the players in the area. Do these things have context and meaning so that not stumble in without knowing it. What are the customs. Common language. This is a surrogate for custom.

Diamond matrix is

Terminology is still primitive. Common terminology.

Useful to have ideas in a reference project. Unconference on an open public integrated architecture business, technical and legal. What words would you use. Can do this now.

What are we trying to do. Is it community building or is it trying to do something specific.

Pattern language concept – leader defines scope, so solidifies. End cycle.

Many terms are undefined. Could pick some subset.

Concrete work items – survey to figure out current landscape – how approach in various contexts.

Also, shared definition of terms on a small scope. If do the second, get the first.

Definitions – some will have multiple contexts. Some have different contexts.

Everyone come to the list with one or two terms that relate in legal and technological

Good model is restatement documents. Make statement and tell stories.

Lucy will send e-mail to ID legal list.

Each should send a term and a example of how it is used.

Adjourn.

User-Managed Use Case Gathering

URL User-Managed Identity Use-Case Gathering
Convener: J. Trent Adams (ISOC)
Notes-taker(s): J. Trent Adams (ISOC)
Other Members:

Iain Hendersen (MyDex)
Ariel McNichol (mEgo.com)
Sarah Dopp (Cerado)
Jens Haensser (UBC)
Eve Maler (Sun)
Alan Karp (HP Labs)
Vittorio Bertocci (Microsoft)
Asa Hardcastle (OpenLiberty)
@Theron (PeoplePond)
George Fletcher (AOL)

Technology Discussed/Considered:

We spent the time identifying and briefly discussing use cases for identity management around information access and sharing. The goal was to capture the use cases, to flesh them out later, then make them available for the community.

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

Use Cases Gathered:

- Certification Management: Emergency Responders
- Authorized Service Chaining: Back-Up Services
- Delegated Resource Authorization: Attenuated Delegation
- Healthcare: Doctor Referral Process
- Change of Address: Battered Spouse Scenario
- Social Graph Access: Privacy Tuning by Policy
- End of Service Data Access: Service Shutdown / User Death
- Education Data Access: Parent/Payer of Student
- Social Network: Content Distribution Policies, Control, & Enforcement

High-Level Takeaways:

- Be careful when creating use cases not to incorrectly apply physical world comparisons to digital identity management; they don't always have a one-to-one analog.
- Identity management use cases often have multiple points of view (aka multiple first parties) with their own scenario variants.
- Delegated authority use cases need to clarify the chain of access controls required.
- Access policy variants need to be handled as scenarios within specific use cases, including exceptions (rather than trying to over-bake the use case to cover all possibilities).
- Use cases as patterns for scenario implementations should help re-set much of the discussion around what has been acceptable, and what should be improved in future solutions.
- Data access and transfer points within the use case need to be clearly called out so that they are addressed by user-managed control points.

Value of Identity (end user) and SEO

URL Value of Identity
Convener:
Notes-taker(s):
Other Members:

Technology Discussed/Considered: (TAGS)

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

Self Asserted Attributes - When To Trust Them

URL Self Asserted Attributes
Convener:
Notes-taker(s):
Other Members:

Technology Discussed/Considered: (TAGS)

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

VRM 1st - 4th

URL VRM 1st and 4th Parties QT video
Convener:
Notes-taker(s):
Other Members:

Technology Discussed/Considered: (TAGS)

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

Developing A Secure Discovery Based Messaging System

URL Developing a Secure Discovery Based Messaging System
Convener:
Notes-taker(s):
Other Members:

Technology Discussed/Considered: (TAGS)

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

Session 6

Are there standards for registering to call an API

URL Are there "standards" for Registering to Call an API
Convener: Angus Logan
Notes-taker(s): Angus Logan
Other Members: Everyone. Lots from Microsoft, Google, Yahoo, Plaxo, MySpace

Technology Discussed/Considered:

Being able to automatically register for an API key in 2 scenarios:

1) 4th party (service provider e.g. DISQUS)
2) Developer not present (e.g. the Portable Contacts problem)

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

0) Are "API Keys" / "Registration" required

- Why pre-registration (identify app friendly to consumer, good way to shut off or give more permissions, give stats back re. popular apps)
- Value add: Statistics / nice UI
- ToS compliance
- Business Model
- Throttling / DoS prevention
- Varying levels of permissions (read/write)
- Who is the developer (contact them for issues etc).
- Can group the API keys together for reasons of blocking etc.

1) Is anyone doing this?

- Google auth sub allows you to work in unregistered (gives you scary screen) (progression from pre-registration)
- Unregistered Oauth for Google Friend Connect (no API keys) pass in the domain (no consumer key)
- OAuth discovery Draft 1 (old and was removed from later drafts)
- Anonymous/Anonymous - developers can use it (solves the barrier to entry, but doesn't have upside of API Keys)
- Facebook do the following: you are on 4th party, and pop a window to get the API key (and secret), and copy/paste it to 4th party, and then 4th party can set the properties using a dictionary.
- Open ID Oauth hybrid has something

2) Is this useful (enough to do the work)

- Doing something like OAuth to create API keys is a no brainer and is coming next
- Focusing on non-developer present creation of the API key is what we are focusing on

3) How will people abuse this functionality?

- Create a ton of API Keys for many phishing sites (to fly under the radar of abuse)
- When an API key gets shut down for abuse, create a new one automatically
- ToS violation (terms of service won't be agreed to)

4) What is the current pain?

- Can't call a new service transparently (PoCo is an example)
- 4th party scenarios are tricky (see password anti-pattern)
- Need to update code/config for each new provider
- Can't just copy existing code / use widgets
- Behind the firewall (before you push to production)
- Lifecycle is a dev/qa nightmare
- Similar to certs / b2b problem (agreement of endpoints)
- Barrier for developers who want to party
- This is the password anti-pattern for application developers (e.g. RPXNow)
- Service accounts to get an API Key (need a FB account, or a WLID account
- Prove you own the domain

5) Solutions?

- Lightweight unprotected function which requests some pre defined information and returns an API key. Then when end users go through the flow the experience is taxed (UI chunkiness or rate limited)
- The provider may not know who the consumer is, but the end user may choose to grant permission to them.
- 4th party : have an API to create child API keys (FB have done a lot of thinking about JanRain)
- Messina: Provide liberal access to the data/system, and when there is abuse, make the system selfheal (e.g. rollback)
- ToS work around: we need to look at creating the "creative commons" of data exposed via APIs. I.e. the consumer can read the "rights"/"restrictions" around the dataset. Perhaps described as Standardized Terms of Service (is this being looked at by DataPortability) www.sciencecommons.org and www.opendefinition.org. question: will the lawyers be happy with a system accepting ToS?

6) Moving forward

Things to work on and next steps

- 4th party (and 5th party) provisioning of child API keys
  - setup and email thread w/ FB and G and Plaxo to riff on this and expand
  - Watch what FB does and the feedback, and also socialized what others are looking at
  - enumerate all of the use cases and post to wiki/blog
- Walking up to an SP and doing some type of lightweight thing
  - Plaxo and G will riff on this and push out a prototype :: lead by Portable Contacts
  - enumerate all of the use cases and post to wiki/blog

Protect Serve - For User-Driven Access

URL Protect Serve QT video
Convener: Eve Maler
Notes-taker(s): Eve Maler
Other Members:

Technology Discussed/Considered: (TAGS)

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

The slides I presented can be found here:

http://xmlgrrl.com/publications/ProtectServe-IIW8-19May2009.pdf

The protocol flows discussed can be found here:

http://www.xmlgrrl.com/blog/archives/2009/04/02/protectserve-draft-protocol-flows/

General information about ProtectServe can be found here; this is one place I will post a call for participation once we get ready to start the planned Kantara WG:

http://www.xmlgrrl.com/blog/categories/protectserve/

Thanks!

Eve

Eve Maler
eve@xmlgrrl.com
http://www.xmlgrrl.com/blog

VRM and media

URL VRM and Media
Convener: Doc Searls
Notes-taker(s): Scott David
Other Members: Jeff Stollman, Scott Loftesness, Hank Mauldin, Steve Williams, Scott David, Michael Froomkin, Nick Givotovsky, Mainer Sen, Doc Searls, Dean Landsman

Technology Discussed/Considered:

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

Business model for free media

2 approaches currently

Sponsorship – big pockets support free stuff.
Or appeal to the viewers – NPR, etc.

If music – band Green Day, Radiohead, go to their silo and deal with them in their different way.

Each radio system has its own system

Their fundraising is identical also.

VRM model is Emancipay.

See slides
Additional to the original grant – not want to have IP issues.
Want to add value in public domain

Advantage with iphone is single target platform.

VRM will inform CRM
The "r-button" provides stance on contributions.

Doing this with information cards – See Craig Burton
Graphical indication of intention relating to interaction.

2 stages – will fan out to other media.

Listen log – logging system – what have you been listening to. Most stations don't send data out with their streams. Stations will later want to cooperate in sending out data.

Data collection associated with the media. Need granularity if will pay for media in a new way. Want to make it easy to contribute to media.

Discussion of funding

Give customers their own pricing guns.
Wanamakers did it after the French.

Emancipay is a pricing gun system. Want to equip individual with means to put money on the table for media and declare what it is worth. Can inform what is there with listen log.

Harder with newspapers. Newspapers could not have approved business plan now. Carbon footprint is an issue with both newspapers and online.

Some want to contribute, but don't want to be a member. If so, should be able to impose conditions on the contribution.

Don't want to CRM someone into negativity. Don't spam someone into the negative.

The main purposes of the log are:

Information on what you listened to – situated cognition/memory. Without having to search general website.

Also for let you know what you value – to help you pay, and decide what you like.

Designing it so that the information is not on the phone.

Want to be able to bookmark songs, stories, etc. to be able to reference/purchase easily.

If people can see what using, they will value it more, and if make it easy for them to pay they will.

Can folks be tied in but anonymously. Yes.

Can the logs be constructed anonymously? Cannot keep it on the machine currently.
Question of whether can maintain the log anonymously.

Medium providing data that can be used.

Speaking with Apple. They are friendly with the radio community. Apple receives podcasts from NPR and posts them for free. Within iTunes – the hope is that they would provide the symbol to show the viewers relationship with the podcasts.

Would require a protocol and an API to do that. So, if have already given money to "this American life" and you are on Itunes, see the loop there on I tunes. Want to unpack what that symbol means. Would it make a call to a different window.

Would go to a rules engine.

Information cards and card selector model provide infrastructure.

What is under discussion now is selector based model. Would like to take that to Google and say here it is. This will help with customer service. Apple could be a payment mechanism as well.

Want to have option available to others that have not yet contributed.

Notion that all computer devices with be selector based because expedient. Selector smart enough to display only those that are needed at that time. Have multiple secure back channels controlled by user. That would be useful for VRM construction.

Data set – could be a link
Card
Rule set

Does the R button indicate an action or a state? It is a state that supports an action

“states” are intention to buy, intention to sell, etc.
In this context

See informationcard.net for white paper.(cookie versus selector model)

Question of just speaking of existing business models. If combine VRM with social graph. VRM can combine social aspect with it. Response is that can do it now with infrastructure and buy in for entities.

This is a business model for musicians. Any musician that does this.

What if I tunes charged zero or a fixed price. Want to provide them with a kit to drop in to the existing application.

DMCA – left streaming unsolved. Record companies not like internet radio stations. No willing buyer and seller. Copyright arbitration royalty panel was fashioned. RIAA liked it, stations not like it. Public radio had a carve out. That ran out – copyright royalty board was fashioned. More high power. Still favored the RIAA. In absence of willing buyer/seller.
They set the pricing gun at X price per listener. Sound exchange get the money to the artists. What if a willing buyer system. Can listen to whatever you want, wouldn’t mind paying small amount per song. It is micro accounting – keep track of what listen to and work out what will pay over time. Accumulation of information on what have listened to enable payments.

This could play in the you tube world also.

Take the standards, protocol and API and drop them in.

OAuth for High Value Transactions

URL OAuth for High Value Transactions
Convener: Jeff Shan E*TRADE
Notes-taker(s): Tom Brown and Jeff Shan
Other Members:

Tom Brown	opensourcecurrency.org		
Michael Helm	LBNL/ESnet	Ray Valdes	Gartner Inc
Dick Hardt	Microsoft	Rajesh Pandey	eTouch
Eric DRAGHI,	Consultant	Abraham Williams	Independent
Manish Pandit	E*TRADE	Nathan Beach	Google
Brian Eaton	Google	Siddharth Bajaj	Verisign
Hannes Tschofenig	Nokia Siemens Networks		
Greg Haverkamp	Lawrence Berkeley National Laboratory		

Technology Discussed/Considered: OAuth, Threat Modeling, risk management challenge – extra authentication

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

a. As OAuth begins to be adopted for High Value Transactions, there is strong need to enhance the OAuth protocol to mitigate the risk. In general, the risk mitigation should be transparent to most of users and transactions.

b. Additional parameters for end user client such as
Client IP
Browser (User Agent)
Device ID
…

should be passed from consumer to SP (for each step) for auditing and risk assessment.

c. Result of risk assessment by SP could be challenge, which should result in consumer redirecting user back to SP for extra authentication (so to minimize the changes for Consumer). If user successfully passing extra authentication, it should be redirected back to consumer side to finish the transaction.

d. Scope/Level for Access Token was discussed. But Brain mentioned that it seems to be very difficult to have a generic model to cover all use cases.

e. Security improvement to protect against session fixation with bad consumer implementation. One of proposals is with "Approved Token" approach as documented in

http://groups.google.com/group/oauth/browse_thread/thread/e8506e71c5dc9582#

which is similar to OAuth Core Spec 1.0 Rev A (Draft 3). But Approved Token would be different from Request Token after user's approval, to protect against bad consumer implementation of early binding. And no need for verification code.

f. Token secret is currently not used in signing with RSA-SHA1. There should be enhancement to leverage token secret with RSA-SHA1.

Alternate Identities

URL [Managing Alternative Identities]()
Convener: Infinity Linden
Notes-taker(s): Steve Herbs
Others Members: Steve Ogden, Katrika Woodcock - Msft, Karon Weber-Msft, Gabriel Wachob - SocialText, Doug Whitmore - Apple, Andrew Nesbitt - Apple, Nika Jones - OONO, Laurel Boylen - CHI-MP, Meadhbh Hamrick - Linden Research, Keith Dennis - AssertID, Ashish Jain - Symantec, Hans Granqvist - Netflix

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

Selected Take-Aways:

There is ample evidence of a critical need to allow users to create and manage alternate identities; there are no standard practices for allowing users to do this.

Context (communication channel) is critical consideration underlying alternate identities. *"I like you but I don't want to friend you in Facebook – can I meet you over here?"*

Some users lack an understanding of how the stuff they generate can proliferate. What is our obligation to help them understand? (refers to "Duty of care", i.e., making it harder for users to do stupid things)

Original promise of the internet: open info exchange w/o reference to race, creed… now you come in w/social capital, reputation. This presents a really interesting challenge when an original promise was the blind nature of the Internet. How to keep this promise alive?

There is a need to establish a shared ontology for alternative identities due to lack of clear consensus on the meaning of terms such as pseudonymity, persona, avatar, etc.

Actions:

Participants in the session were encouraged to help work toward a consensus identity ontology. A Google group was established for this purpose named 'idont'.

Stream-of-consciousness notes:
Multiple identities desired
What is difference between identity and avatar?
To us [Linden Research] an avatar is virtual person w/a mapped identity
Network/svc identity is distinguished from this – some conflict on this
Do users think multiple identities are a problem or is it a resource issue?
We're getting request from business users…
Linden research is an enterprise play… announced a behind the firewall solution… think there is a large degree of value in letting users go outside firewall and bring goods back into it

Big issue right now is …we live in horror of having to UIDs in public and private areas
QQ lets you have multiple identities – male and female – acquire with one persona, gift from other
That gets into the social aspects of this – also interested in the technical – what does group think?
MySpace … different contacts are all mashed up, business, friends, not like real world
Parental control kid aspect is another consideration – you don't want kid identities tied to a real person
Think the issue is: how are we building walls between people's multiple personas?
When I was on r_ I had my regular professional account and my __ professional account – these were siloed and it didn't work very well.
A situation: I'm getting harassed and I want to switch avatars – how do I do this?
Does anyone have a system where you have to identify multiple identities?
In CHI.MP I can make as many personas as I want. Users register more often than allowed by our terms of service – we don't have a system in place for tracking – I can go through registry logs and see some obvious clues to whether someone has done this
Yahoo has the ability to create multiple linked IDs to tie in your external services
People can game the system –having Karen Brown and K. Brown is not a problem, but having 70 IDs is a problem
Someone signed up for Donald Trump, and that's Donald Trump's problem
Multiple alias associated w/an open ID model
In CHI.MP's case, you sign up w/one ID, and then for each persona you turn buttons on and off based on what you want to assign to each contact
To invite people to my site I can go through the CHI.MP service
We start out with four personas: public, family, friends, work
I think we (CHI.MP) has done a good job of allowing users to manage personas and switch between them
We don't have ontology for alternative identities… alias persona identity
How handle: "I like you but I don't want to deal with you in Facebook – can I meet you over here?"
…can't you partition your Facebook?...
Its legitimate to tell people you can connect to me here but not there
Did they complain when you kicked them out? Why would they care?
Security consideration: I don't broadcast that I'm out of my home broadly
I had a friend who joined Twitter and she shared her travel plans – and I had to stop her – people just to get what they put out there – people who do are a smaller group
That's ok if going to friends? No – you can't control what your friends do!
…this is where the whole alternate persona thing comes in
When I'm logged in as [my name] I'm really careful…
I don't feel comfortable expressing myself because it lasts forever
There's a difference between open and broadcast…
When I talk to my friends I talk to them in a certain context… but I don't feel comfortable in another context. Context is critical.
People advocate open walls but like garden walls.
The problem is Twitter is broadcast… People need to understand this distinction… But you don't build your network as fast… you have IM for that… *the good news is it spreads so fast, the bad news is it spreads so fast...*
Part of it is context, part of it is understanding when I type into this channel where is it really going….

Duty of care plays here – you have a responsibility to protect your customers from themselves
Most social networks don’t comply with rule 10 of the characteristics of User Driven Services
Make it harder for people to do stupid things
…but …When you try to make something idiot proof nature makes a better idiot
Plurk tried to that ‘karma thing’
Do people get too comfortable when you can have multiple identities
In the real world you don’t have such clear barriers
In the future they will all get merged
…I joined Facebook, didn’t touch for 6 mos, then things snowballed… my intent changed over time… oh look, all my high school friends… I don’t want to talk to all my high school friends… there are people who bring up the drunken kegger… everyone’s been at the drunken kegger… hopefully it wasn’t last week or at least you didn’t friend your boss
I scanned Tweets for personality…
What if he didn’t do that?
He wouldn’t work for my company.
This is a conundrum.
I hardly Tweet at all – because of where we are in our company development.
If you’re not in any of these spaces, why are you in the business and why should I hire you?
Original promise of the internet: open info exchange w/o reference to race, creed… now you come in w/social capital, reputation. A really interesting challenge when an original promise was the blind nature of the Internet.
We’re starting toward anonymity…
I run a political blog… participants are concerned with credibility w/in blog, anonymity in general – consistent w/in space but could never Google and get info on the individual…
Pseudonymity – Ian Goldberg: you can’t map your online identity…
Are pseudonymous accounts all about multiple personas? Yes.
We have a million active users and 15m users.

What I got out of this: we need a shared vocabulary, ontology – ongoing debate about this at Linden Lab. People often use vague terminology – more often users misunderstand. Action item: form a mailing list on this.

Yesterday’s first session: what is an Identity (this conference will cease to exist if we figure this one out!)

Set up Google Group…

All join identity gang? – but this won’t solve problem… better to do ourselves… we’ll call it Identity Ontology… idont.

Session7

User-Managed Access

URL Use Cases for User-Managed Access
Convener: Eve Maler, J. Trent Adams, Alan Karp, Paul Trevithick
Notes-taker(s):
Other Members: Terry Hayes, Ariel McNichol, Joe Audrieu, Ben Sapiro, Alan Karp, Tatsuki Sukushima, Jeff Stollman, Paul Trevithick, Markus Sabadello, Asa Hardcastle

Technology Discussed/Considered:

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

Joe's approach to search: a search map gets created that contains all the context of a search (which may have been built up for months), and that needs to be shared. You can also synchronize that data with yourself on another device. You can also have collaborated synchronization, where multiple users contribute to a single document.

- Single-user, multi-device synchronization
- Multi-user synchronization (future)

Joe wants to identify PII he wants to be merged into data sets, at delivery time, that he provides to others, but that doesn't get used when someone else uses the same search map and its auto-fill feature. A search map contains everything related to your search, and those are used to make social recommendations (by agreement with the user).

Fields retrieved only at run rime, variable per user, with only a reference to it archived

You're a small business owner who wants to delegate access into your QuickBooks web app to your virtual assistant, such that they can do some subset of your full set of tasks. If they then farm out some of that work, they further constrain (attenuate) the accessible tasks to that other party such that it's a strict subset.

In the VRM context, we also had the "Flower Power" use case: We want to be able to surprise a friend by sending them flowers, which involves you, the friend, the flower shop, and the delivery company.

We believe FedEx does have the option now of providing a shipping label that has only a bar code rather than printing the address for all to see.

The Confused Deputy problem: http://en.wikipedia.org/wiki/Confused_deputy_problem

Constrainable and attenuatable delegated access

You give someone your shipping address, they hold onto it for a week to ensure the item gets delivered, and you want to revoke their right to use the data after the item is delivered. We think this can be baked into the contract at the beginning, even though the expiration time is variable.
Expiry of rights based on some variable future events

If a company does something you don't like, you may want to change or terminate an agreement. This could happen "eagerly" (proactive revocation by the user) or "lazily" (revocation happens whenever the requesting app happens to check in). Being able to terminate access and usage rights is the moral equivalent of single logout. :-)

Revocation of access rights, to varying degrees of vehemence

It would be useful to share a limited amount of calendar data, for a limited period, with a doctor's office so you can solicit an event invitation. They themselves may have to coordinate the availability of multiple parties, such as the attending doctor, the MRI machine, etc.

Soliciting event invitations through sharing calendar data

How do we enumerate the kinds of access available? How does the printing service know how it can request a photo for printing? What are the parameters of the GET? Does WADL help in a RESTful scenario? The consumer using a service gets to see only the parts of the API that it's allowed to use.

Limited disclosure of service capabilities

We agree that the major proposition here is provisioning recipients with pointers to data rather than provisioning them with the data by value. If the pointer (to, say, an address) is a URL, it's actually harder for a user to provision it "by typing" than it would be for the user to provide the address itself! However, you'd only have to provide it once. :-) But providing it by means of an information card would be very handy.

Using an infocard to convey resource feeds

Sometimes you want to package up a set of information that's commonly needed by a set of consumer parties, such as your credit card data and a claim saying you're over 25. This could be (but doesn't have to be) an Atom document that serves as a manifest for links to the pieces of data. We discussed the pros and cons of information cards (as they are specified today in ISIP and IMI) for doing this; currently cards are limited to single-issuer claims, but it's an artificial limitation. If your personal datastore pulled down third-party-signed blobs and stored them, you could get the "non-auditing" use case for free!

Sharing frequently offered data from multiple sources as a package

We may want to ensure that, if search results hit a sufficiently high number, they can be used; otherwise they can't be. This makes sure that data is obfuscatable to at least some degree.

Constraints on data usage that depend on the nature of the data actually delivered

Failed Identity Businesses

URL Failed Identity Businesses
Convener: Chris Lunt
Notes-taker(s): Chris Lunt (lucky me)
Other Members: Uppili Srimvsan, Peter Tapling, Keith Dennis, Kent Jepperson, Johannes Ernst, Pete Rowley, John Bachir, Nika Jones

Technology Discussed/Considered: (TAGS)

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

- Solving a problem people *will* have is a poor foundation for a business
- Consumers cannot be sold Identity services; it's too abstract
- There is more profit in capitalizing on users misconceptions

Open ID UX - Best Practices

URL OpenID UX
Convener: Allen Tom
Notes-taker(s):
Other Members:

Technology Discussed/Considered: (TAGS)

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

- Single Sign Out is Hard!
- Gradual escalation of privilege is good
- See openid.pbwiki.net for UI recommendation

Confetti - Stop Storing PW / Start Using Delegation

URL Confetti
Convener: Kevin Marks
Notes-taker(s):
Other Members:

Technology Discussed/Considered: (TAGS)

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

Next Generation Open ID - Assurance In the Real World

URL
Convener:
Notes-taker(s):
Other Members:

Technology Discussed/Considered: (TAGS)

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

Contextual Friends Lists and Sexuality On Line

URL Contextual Friends Lists and Sexuality Online
Convener: Sarah Dopp
Notes-taker(s):
Other Members:

Technology Discussed/Considered: (TAGS)

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

Activity Streams – Formalizing Draft Spec

URL Activity Strea.ms
Convener:
Notes-taker(s):
Other Members:

Technology Discussed/Considered: (TAGS)

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

Kantara Initiative

URL [Kantara Initiative]
Convener: Brett McDowell
Notes-taker(s): Kaliya Hamlin
Other Members:
* Judith Bush OCLC
* Lucy Lynch ISOC
* Siddleath B. Verisign
* Bill Smith SUN
* Daniela Barosa DataPortability Project - Dow Jones
* Mark Lizar MyDex VIP-sig
* Dave Crocker Brandenburg
* Kaliya Hamlin - Identity Commons
* Bill Washburn - XDI.org/OpenID

Technology Discussed/Considered: (TAGS)   Kantara, Industry Consortia

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

Brett explains what Kantara Initiative he mostly wanted to be here to answer the question
* New Organization - formed by some in the ID Space - DPP, XDI.org, Liberty Alliance, Information Card Foundation
* wanted a governance structure that integrated intellectual property governance
* clear way to participate and have votes
* for work that is deemed important

Membership - website with proposed charters
Two kinds of groups working groups, discussion groups (discussion groups likely precursor to working groups)

Trustees have Fiduciary responsibility
Leadership council
Membership structure

People joining agree to intellectual property agreement of work. The membership funds things and has a final ballot on recommendations.
Requires specs to got to standards bodies.
The initiative is open and inclusive - not vendor driven.

SAML -> enterprise
OpenID -> social web

Groups....
* ID Assurance
* Telecommunications
* VPI - Policy
* VPI - Technology
* Wakame "hello"
ID-WSF & Open Liberty
* Privacy and Public Policy
* Concordia x-protocol use cases

* Multi-protocol ID selector
* eGov
* Healthcare
* WAF
* IDWSF -> OAuth

Branding Beyond ->Technology
* Response to call for participation
* anything like this has to prove itself

Bill - what would constitute critical mass
* Solve cross protocol issues - "do so in an organized manner"
* for a large number of entities that want to participate in
* can go on list as individuals
If SUN is a member then SUN's IP is committed

Iain - qualitative and quantitative research properly done

Vendor Driven?
as a vendor I don't want a place without deployers loose interested not their business

Kaliya - expressed concern re funding model with the potential for large fights about budget allocation

It is a place for pre and post standards work not just vendor centric end user can come and participate without paying money " get all of the protocols more useful"

Non-technical buckets related to community building
* Privacy
* Assurance - ID Assurance Framework
* Liability - American Bar Association, Collaboration
* Usability - no proposed projects - yet
    * Security elements
    * Privacy Policy Icon Work (easy to use/control spectrum or
matrix) user options beyond yes/no.

Session 8

Detecting User Login State and Preferences

URL Detecting User Login State and Preferences
Convener: Brian E, Luke Shepard (Facebook)
Notes-taker(s):
Other Members:

Technology Discussed/Considered: (TAGS)

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

User Driven Search

URL User Driven Search
Convener: Joe Andriey
Notes-taker(s):
Other Members:

Technology Discussed/Considered: (TAGS)

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

Web 2.0 vs Rich Internet Apps (RIA)

URL Web 2.0 vs. Rich Internet Apps (RIA)
Convener: Brett McDowell
Notes-taker(s):
Other Members:

Technology Discussed/Considered: (TAGS)

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

OAuth for Installed Apps

URL OAuth for Installed Applications
Convener: Nathan Beach, Eric Sachs
Notes-taker(s):
Other Members:

Technology Discussed/Considered: (TAGS)

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

Identity and The Future of Money

URL Identity and the Future of Money
Convener: Giyom
Notes-taker(s):
Other Members:

Technology Discussed/Considered: (TAGS)

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

Session 9

Use case selection and metrics

URL 9A: Use Case Selection and Metrics
Convener: Eve M and AlanK
Notes-taker(s): Eve M
Other Members: Jens H, Judith B, Tom C, Asa H, Lucy L, Peter T, Eve M, Bill S, Tyler C, Alan K, J Trent A, Andrew N, Joe A

Technology Discussed/Considered:

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

Alan presented an example from the physical world that demonstrates the following aspects of sharing that we should seek to emulate in the online world:

- Dynamic (no pre-setup to enable sharing)
- Chained
- Cross-domain
- Composable (merging rights and sharing from multiple sources)
- Attenuated (rights can be strictly subsetted as you go along)
- Accountable

He proposes selecting one or two use cases and explore them in depth to see if they have the characteristics we're all seeking.

We had a short discussion about how hard it is to separate metrics for use cases from metrics for solutions to the use cases.

Eve proposes that we need dynamicism of this sort: A user can choose to publish a URL that a potential data recipient can attempt to retrieve against, where the recipient didn't have to take any steps prior to the initial GET attempt and where the attempt doesn't necessarily result in a successful retrieval.

Peter Davis proposes a specific use case involving wanting to share an album of event (e.g. camping) photos, the subjects of which are minor children, with exactly the set of dads whose kids are in the pictures, without exposing the pictures to anyone else. Trent proposes a variant where the photographer is a professional who has to get signed release forms, such that the list of people with whom you want to show the photos is known. For someone to print a photo, you need to share the photo with them.

Many services do photo sharing today by emailing special URLs to give people (who are not otherwise known to the photo service) to get access to the data.

Eve proposes that a use case metric we should adopt is that keeping the URL secret should not be relied on for the security of the overall system. We started calling this a "suckiness" factor. :-) Peter is going to have to solve this for his camping photos by explicitly constructing a photo-sharing Facebook group for this event that names the people explicitly! Alan then proposes ease-of-permissioning as a solution metric -- "pain-in-the-assiness". :-)

Bill Smith had described the enterprise outsourcing use case on Monday; some companies, especially really small ones, often outsource everything. Peter elaborates: five guys get into a room and declare they're part of a company. Now you have to control access to all sorts of resources (sharing documents, authorizing bill payments, etc.).

Peter describes an enterprise use case where the entire company collaboratively serves in a policy-making function. Any employee can contribute a product idea, and if a really good one arises, people can decide that it needs to be subsequently restricted from the view of the entire company, to protect it.

Asa described managing entrepreneurial discussions with reputation systems (a discussion that took place at the Berkman Center).

The separation of policy decision-making and policy enforcement is important.

There's a database that relies on trusted experts to indicate who is the author of a book, the heir of an author, etc. An author might want to have an agent operating on their behalf asserting the author's rights in the work. The trusted experts perform, in effect, identity proofing.

Revocation of various sorts came up. Peter may want to deprovision the rights of a particular person to access photos, including destroying their cache of photos! And Alan points out that if Wikipedia wants to revoke a "bad" editor's rights, it also might want to roll back any content the person had contributed.

10:15am hour:

We walked through the photo-sharing use case in detail:

Assumptions:

- There is at least one parent on the camping trip who doesn't want photos of their kids put online.

- The person who took the photos can always view photos of their own kid.

- The online photos in question are referenceable individually and in a collection.

- People who want to use a photo you took need to seek your permission to use it, print it, etc.

1. Peter goes on a camping trip, taking photos as he goes.

2. He meets or knows most, but not all, of the other participants in the trip. And some situations involve total strangers (others at the swimming hole that day). Photojournalists takes pictures and then immediately seeks releases.

3. He returns home and publishes a set of photos from the trip, initially to himself.

4. He shares access to the photos with a selection of people, including the parents of the photo subjects, who can then themselves share access to selections of other people.

5. One of the other parents, who had taken their own photos during the trip, wants to add those photos to the set, with all the data-sharing properties you have set up for the photo set as a whole.

6. Grandma, with whom two different parents (her son, Peter, and her daughter) have shared separate photos of their kids, wants to "mash up" the photos into a composite such as an online scrapbook page.

7. Grandma wants to share her scrapbook page, which contains two different photos that have different data-sharing rules attached to them, with her bridge club.

8. One of the other parents is a professional photographer and takes advantage of his Creative Commons copyright license grant to create derivative works to crop and edit the photo. Later, when his kid leaves the troop, you want to revoke his rights to the photo set.

Alternative scenario: Grandma doesn't do stuff online, but subscribes to a service that prints and sends her photos. Peter wants to give printing/sending access rights to the service. (This gets at the VRM individual-to-service data-sharing use cases.)

Having built the use case and its variant, we discussed what metrics any solutions could be measured on. Here's a composite list of the ones we've discussed to date:

- Dynamic (no pre-setup to enable sharing)
- Chained
- Cross-domain
- Composable (merging rights and sharing from multiple sources)
- Attenuated (rights can be strictly subsetted as you go along)
- Accountable
- Usable
- "Security" (practical ability to control access to the desired people)
- The "oops factor" (when security can be accidentally compromised even by sophisticated users -- related to security+usability)

There's a bunch more, largely obvious, that we didn't have time to list.

We discussed reserving the word "suckiness" for the ability (actually the lack thereof) of a particular solution to meet a metric, rather than one of the metrics itself. :-)

Alan suggests that URLs should be used as rights-carrrying objects; several others objected because URLs were designed precisely to "give directions" for where to get a resource.

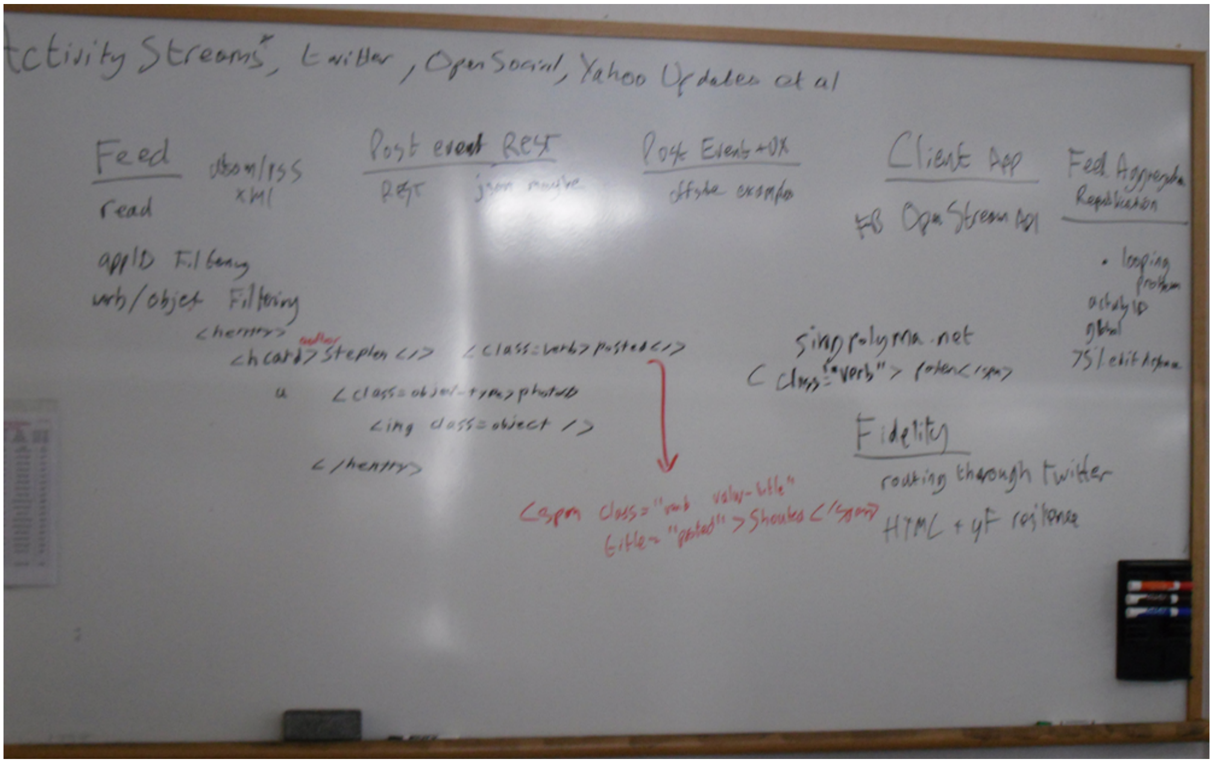
We ran out of time to review various existing and proposed solutions against the various metrics. This is an exercise that can be done offline (perhaps on the community@lists.idcommons.net list?).

Activity Streams – Twitter, Yahoo, API, Facebook et al

URL [Activity Streams, Twitter API, Facebook, Open Social, Yahoo! Updates]() [QT video]()
Convener: Kevin Marks
Notes-taker(s): Monica Keller
Other Members:

Technology Discussed/Considered:

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



At IIW we met with Kevin Marks and a group of folks to discuss the fact that there are multiple publishers and consumers of activities everywhere and how we can actually get compatible representations so we don't lose the semantics around the entires.

We first detailed the Use Cases for Activities

- Reading the feed - aggregators for correlation
  - Need common representation
- Raising activities (Opensocial , Facebook)
  - With popup
  - Without popup
- Desktop client pushing updates (activities)
  - Writing semantic entries with simple clients

- Ingesting feeds and republishing
    - Problems around echoing

We then proceeded to discuss solutions:

> What if we ingest activities with the current tool by extending out support for microformats ? Well the main thing that is missing are the verbs so we can use exisiting microformats and a new microformat which handles the verb

```
<hentry>
<hcard class="author">Steven</hcard>
<span class="verb value-title"  title="post">Shouted</span>
</hentry>
```

There is an effort started in the Microformats community to be able to provide metadata to represent activities. See

http://microformats.org/wiki/activity-verb-brainstorming

Simpler OAuth For Lower Risk Use Cases

URL Simpler OAuth For Lower Risk Use Cases
Convener: Brian Eaton, Eric Sachs
Notes-taker(s):
Other Members:

Technology Discussed/Considered: (TAGS)

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

Notes:

- Basic problem
    - OAuth is really hard to implement.
    - That's a common complaint we hear from developers who want to be OAuth consumers.
- Some proposals to simplify OAuth to increase adoption:
    - Simpler base strings
    - Unregistered OAuth
- Simpler base strings
    - We could make the base string such that it's just tied to the nonce, timestamp, consumer key, token. The idea is that you sign these values and they're good for only a certain amount of time.
    - OAuth access tokens never change. Thus, we can't really do PLAINTEXT signatures because that would cause the access token be sent over the wire.
    - OAuth session extension simplifies the signing (because we can get away with not signing) but complicates the session protocol.
        - It's hard to bake the protocol flows into the libraries today. It's much easier to create a simpler base string.
    - An OAuth SP could have a policy saying that as soon as the user signs out of the SP site, the access token granted to the consumer is revoked. That would prevent the access token from being "all powerful" forever.
        - The whole value of OAuth is to enable the consumer to access data in absence of the user.
    - Major thing that trips people up: People cannot figure out how to sign a request.
- Unregistered OAuth
    - Saves developers from having to register consumer keys and secrets.
    - Even with unregistered OAuth, you're still required to sign requests. So, this doesn't some your problem.
    - It could be hard to get away with this from a legal standpoint.
    - We could have an automated way to get a consumer key and secret. (see notes from the session Angus led yesterday)
    - The problem isn't necessarily the complexity of the protocol. If we could provide good libraries.
    - Plaxo provides HTTP Basic auth so that developers can experiment, but this is really simple.
- What do you do when the SP returns a 302?
    - Some of the problems go away if you use the simpler base strings (just CK, token, timestamp, and nonce).
    - SBS approach would include no URL encoding
- What's the problem with libraries?
    - Every service provider is a touch different.
- Most of the extra security that we added to OAuth is to make it possible to provide security for SPs who don't want to setup SSL. Perhaps all these extra stuff are more difficult than just setting up SSL.
    - We have a choice: We can implement the scalable OAuth session extension or can try to really simplify signing.

- Alternative proposal: If we just said HTTPS is mandatory for SPs, then we could really simplify OAuth.
    - For a typical website, all devices from which the user signs in must support HTTPS.
    - Either HTTPS would have to be used on both the authentication server (i.e., the OAuth dance part) and on the data API server, or HTTPS would have to be used on the authentication server and the session extension would need to be used with the data API server.
        - This is no less secure that sending session cookies via HTTP and using those session cookies to authenticate the user.
    - If we require HTTPS, we can just use a plaintext signature or completely eliminate the signature.
- If we said "scalable session extension with PLAINTEXT signature over HTTPS", how hard would that be?
    - Or just pass along the access token.
    - Have the consumer periodically refresh the access token and stick it in the header.
    - A developer should be able to use curl() to get this to work.
- Proposal: PLAINTEXT + Session Extension
    - Long-lived session handle goes to accounts system over HTTPS
    - Short-lived access token goes to services (optionally without HTTPS)
    - No signatures, timestamp, or nonce ever on any step.
    - Dance always over HTTPS without consumer secret.
    - This would be OAuth if you can mandate SSL.
    - Accounts system will return a long-lived session handle and a short-lived access token. When the short-lived access token expires, you have to go back to the accounts system and present your long-lived session handle to get a new short-lived access token.

Session 10

What Should An OpenID RP Do When An Account At An OP Is Compromised?

URL What does and RP need to survive compromise of user@idp?
Convener: Luke Shepard and Breno
Notes-taker(s): Bill Shupp
Other Mebers: Luke, Breno, Allen Tom, Bill Shupp, Anthony from chi.mp, lots of others

Technology Discussed/Considered: OpenID

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

Key understanding: An RP needs a way to communicate to the OP that it has been compromised, or perhaps request from the OP when the last time credentials for that user changed. This is necessary so that when an RP blocks an account, it knows when the account has been "reset" at the OP.

Outstanding questions are where this fits in the protocol, and how this data is communicated from the OP to the RP. Suggestions included modifying nonces to expose it, adding an optional request parameter to checked_* modes to expose this, and abstracting the data do "credentials change more/less than X time ago".

Here's are the unedited notes taken during the meeting:

What does a RP do when user@idp is compromised?

 * What tools does the RP need when this happens?
 * User/Pass logins usually reset a password and send an email notification. Not
   available in OpenID.
 * Do you add additional PAPE levels after a compromise has been repaired?
 * Should OPs provide a security endpoint?

 * What's the value of resetting the password?
  * Email + OP providers have less value
    * Password reset is still useful, even if it doesn't solve this case
  * It's useful to separate the attacker from the user
 * Another attack scenario is when an attacker phishes an account, then sets up an
   OP to link to the account, providing a backdoor (worse case)

 * If your account was created with OpenID only
  * Communicate with the user directly if AX/SREG provided an email
  * Create a communication mechanism with the OP
  * Other mechanisms for identifying the user, send one time pass to cell phone

 * Does the RP want the responsibility of extra credentials? Or does the RP want
   a cooperative approach with the OP?
  * If OPs are notified, the attacker (as OP) could collect data on the RPs
    process/state

 * Should there be a way of exposing to RP the last credential change time at OP?
  * Could be a nonce based on the state (within PAPE?)

  * Should there be a history of changes?
  * OPs should have flexibility around how much information to expose

* Should we be trying to arbitrarily put trust data in the protocol?
  * RPs need concrete, objective measures to know that a password/credentials reset has occurred at the OP
    * OP could certainly lie about it, but including a date could be useful

* How is this credential change communicated to the OP?
  * In checkid_setup?
  * Should the OP just provide this data in each response, so that the RP doesn't need to make the request?

* Response term name.
  * Instead of referencing it as "last credential changed", it could be "last time verified good"

* We are interested in short windows of time here. Maybe use ranges? Like "credential change is > 1 day old"
  * Optional "older than you care about" value?
  * Value is abstract, not concrete.
  * OP has the option of not sending this

* Possible flow:
  * Do checkid_immediate to see who they are
  * If needed, do another checkid_immediate to see when the credentials have changed
  * If not satisfactory, do checkid_setup requesting credential change

The Future of Human Identity (how people change in 10 years)

URL Identity in 10 Years - How People Change
Convener: Chris Lunt
Notes-taker(s): Chris Lunt
Other Members:

Technology Discussed/Considered: (TAGS)

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

- A history of surprising Behavior
  - Handles
  - Blogging
  - Email addresses on resumes
  - Consumer domain buying
- Emerging Trends
  - Amazon “Real Names”
  - Personal name collision in the global namespace
  - Virtual Goods/Currencies
  - “transparent generation”
  - Activity Streams
  - Concurrent Presence (twitter/SMS + real world)
- Unresolved Issues
  - The value of face-to-face vs. virtual interaction
  - Implicit vs. Explicit activity streams
- Next
  - Will people keep considering virtual and real-world identities as seperate
  - How will be people decorate their virtual identity
  - What are people capable of learning: will users ever manage access control?

OAuth for Enterprise

URL OAuth for Enterprise
Convener: Eric Sachs
Notes-taker(s): Eric Sachs
Other Members:

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

- GAE, Amazon, Azure, Salesforce, Google Apps, etc.
- The enterprises need a way to determine which application in the cloud is requesting access.
- Ping Connect
    - Create a token server
    - This is an analogy to scalable OAuth
- Scalable OAuth
    - You still use the access token in the query string or header. The key difference is that the access token is short-lived and must be refreshed.
    - It's good security practice to have a separate service (a local STS) that stores the long-lived token.
    - The local STS is part of the consumer's organization and is run by the consumer.
    - The STS is usually completely isolated from the outside world and never makes any outbound requests nor receives inbound requests.
- We don't want 2-legged OAuth to redo SAML, WS-Trust, etc.
- Background
    - Overview of WS-Trust
        - Two organizations: A and B
        - Private keys for each
        - STS in each org
        - A tries to access B. B says "You need token from STS." A fetchs token from B's STS.
        - Authentication is the signature from B's STS.
    - Kerberos
        - Two orgs: A and B
        - Based on symmetric ticket
        - A requests ticket from TGS (Ticket Granting Server) for access to B
        - You get long-term ticket to get a short-term ticket. Moreover, you never get a truly long-term ticket. You still have to represent the credentials every so often to renew the long-term ticket.
        - Ask for cross-realm ticket. Then ask TGS at other realm for a service ticket that's good for services in that other realm.
        - You don't ever want a situation in which the TGS or STS server is very tightly protected.
- *[At this point, my laptop battery died, and I couldn't find any power outlets nearby. So, these notes are unfortunately incomplete.]*

OSIS Testing

URL OSIS Testing
Convener: John Bradley
Notes-taker(s):
Other Members:

Technology Discussed/Considered: (TAGS)

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

Session 11

WebFinger

URL WebFinger
Convener: John Panzer
Notes-taker(s):
Other Members:

Technology Discussed/Considered:
XRD, LRDS,….

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

http://www.abseractioneer.org/2009/DS/webfinger-white-board-at-iiw.html

Better notes soon – see code.google.com/p/webfinger

Personal Hype Quotient - OAuth in Use

URL Personal Hype Quotient:
Convener: Mary Hodder
Notes-taker(s): Mary Hodder
Other Members:

Technology Discussed/Considered: (TAGS) Personal Hype Quotient: OAuth use

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

Discussion of 5 API's used
* twitter API
* Google Open Social API
* Long URLl Please API
* Google App Engine API
* OAuth

Security of OAuth
How OAuth Works
* problems with authentication (vulnerable aspects)
* what was needed (with google of OAuth) App Engine we had to write our own API in Python to work with OAuth and Twitter.

Visual e-id Certificate Image

URL Visual e-ID
Convener:
Notes-taker(s):
Other Members:

Technology Discussed/Considered: (TAGS)

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

Info Grid Sneak Preview

URL InfoGrid
Convener: Johannes Ernst
Notes-taker(s):
Other Members:

Technology Discussed/Considered: (TAGS)

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

Internal and External Identity In The Enterprise

URL Internal and External Identity in the Enterprise
Convener: Justin Richer
Notes-taker(s):
Other Members:

Technology Discussed/Considered: (TAGS)

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

Session 12

Identity Broker Uses Cases

URL Use Cases for Identity Brokers
Convener: Ben Sapiro/Ashish Jain
Notes-taker(s): Ben Sapiro
Other Members: Alan K, Bob P, Alavilli P, Vittorio B, Ray V, Ashish J

Technology Discussed/Considered:

Identity Broker Uses Cases

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

IP needs to have some sort of accreditation

why would the RP pay?

Alcohol sellers online
verification that you're a child by accessing a school database
Red flag automation for

you do not have correct control of the data collection

An industry based IP - all the banks want to have one single phase
all the attorneys have one single issue

you become a very attractive target if an attacker can get onboard and generate identities via you

the more datasources you aggregate, the more useful you are - but the more risk you will be faced with

not unlike OpenID OP vs IdP debate - but unless you actually issues Identities, you're just an Identity Owner (not a provider)

An IP can perform correlations across multiple data sources

This is done in federation. Example – citizen of EU --> Italian IdP (using on behalf-of)

the main value is providing access to the data, not in aggregation (that is clearly secondary)

some of these are claims, some of these are too close to be background checks
- Is sex offender
- is criminal
- education history
- employment history
- DOB/Age/Over18
- Address verification
- Credit Check
- valid insurance
- reputation

- driving record
- frequent flyer miles
- # of linkedin connections
- citizenship
- property ownership
- marital status
- connections to a group
- affiliations/membership
- professional status
- email ownership

(these have to be actively consumed by a third party, otherwise it's just information)
(if the information is about the requester, it's a claim, otherwise not)

would require in-place access to data (no copies)

would require strong legal contracts forbidding mix and match to achieve information leakage

need to expose which sources you queried but not what the answers were

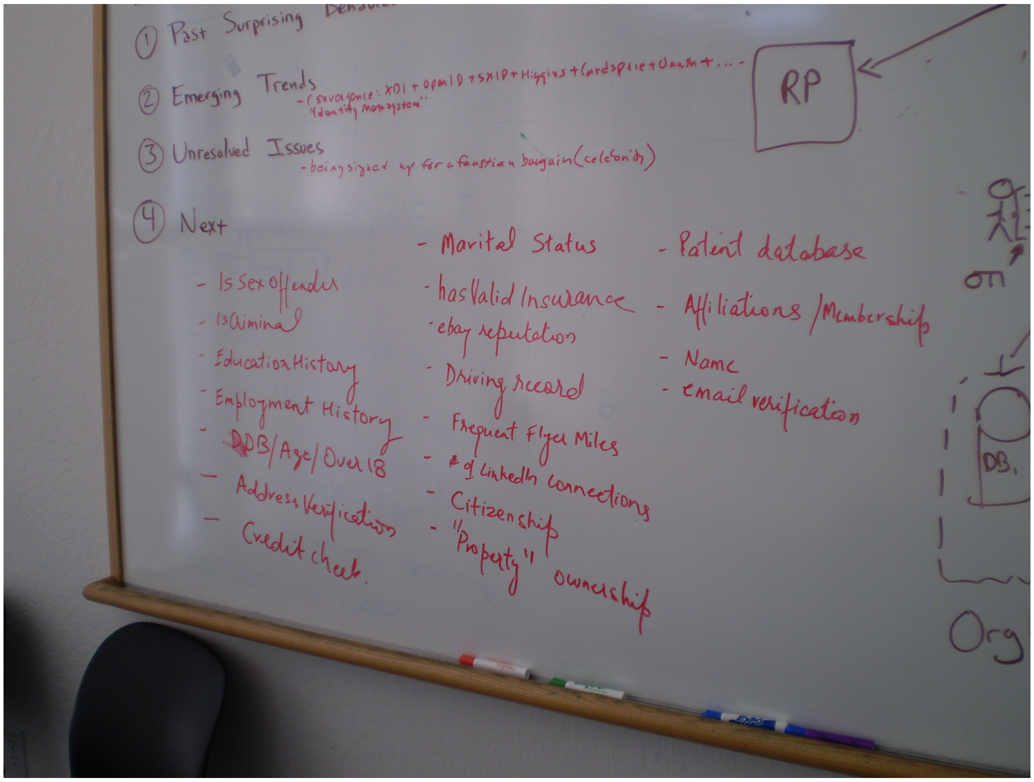
pricing could be commensurate with assurance level (did I ask gold level or silver level information sources)

pricing could be commensurate with granularity of information exposed (boolean versus scored)

Identity Broker is actually a claims broker (strict definition)

would need a process to feed in annotation/corrections and handle disputes

how do we resolve inconsistent data (database does A does not match B and C)?



(1) Past Surprising

(2) Emerging Trends
- Convergence: XDI + OpenID + SXIP + Higgins + Cardspace + OAuth + . . . -
"Identity Metasystem"

(3) Unresolved Issues
- being signed up for a faustian bargain (celebrity)

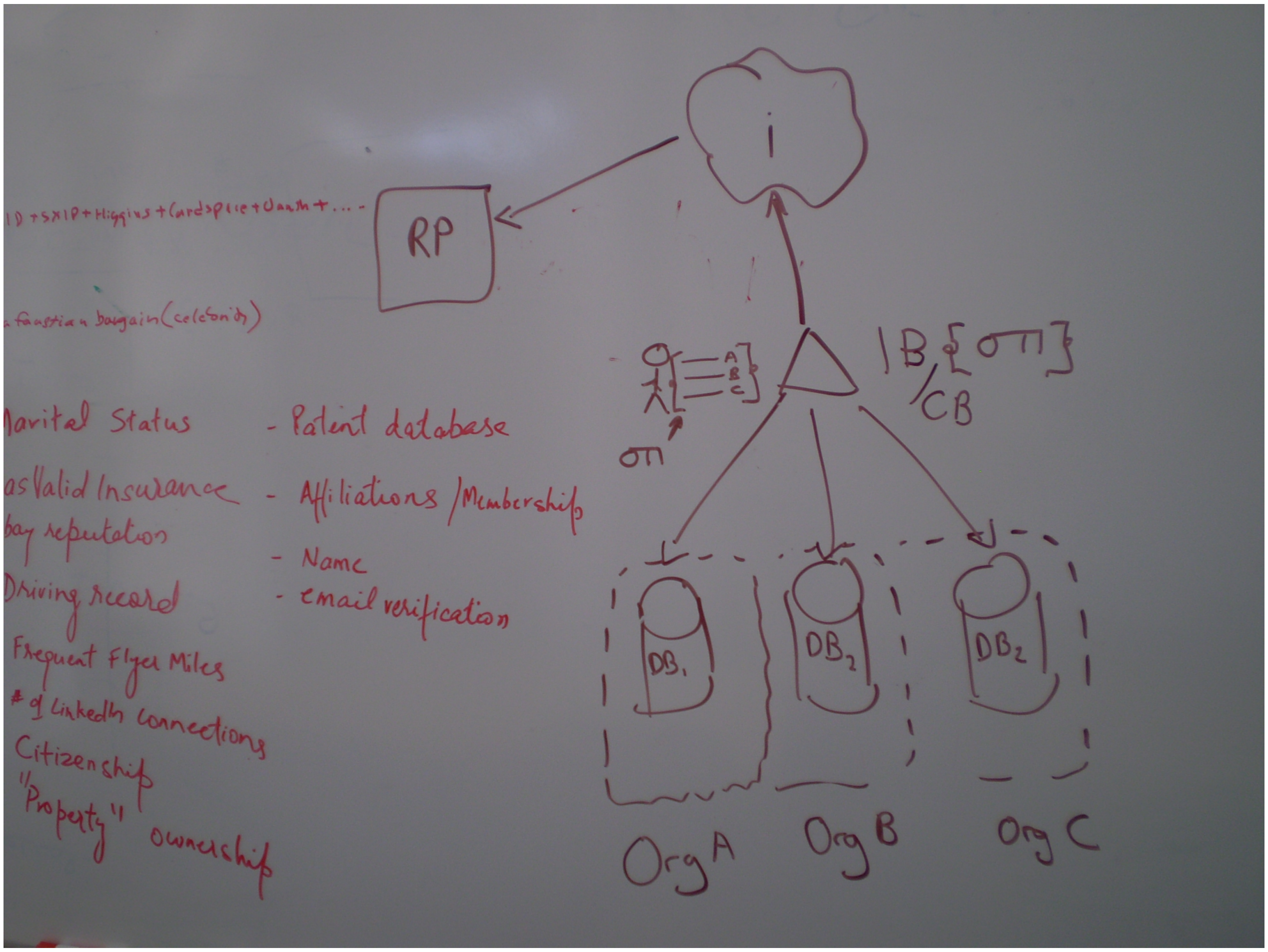
(4) Next

- Is Sex Offender
- Is Criminal
- Education History
- Employment History
- DOB/Age/Over 18
- Address Verification
- Credit check.

- Marital Status
- has Valid Insurance
- ebay reputation
- Driving record
- Frequent Flyer Miles
- # of LinkedIn connections
- Citizenship
- "Property" ownership

- Patient database
- Affiliations /Membership
- Name
- email verification

Left Side of Board



Right Side of Board

NASCAR Demo with Action Cards

URL NASCAR DEMO with Action Cards
Convener: Phil Windley, Drummond Reed
Notes-taker(s):
Other Members:

Technology Discussed/Considered: (TAGS)

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

Open ID Social & Mobile

URL OpenID, Open Social and Mobile
Convener: Jeff
Notes-taker(s):
Other Members:

Technology Discussed/Considered: (TAGS)

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

Open Liberty Wakame V1.0 "FUN"

URL Open Liberty Released - Wakame QT video
Convener: Asa Hardcastle
Notes-taker(s):
Other Members:

Technology Discussed/Considered: (TAGS)

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

Validation Extension for Open ID

URL [Validation Extension for OpenID]()
Convener: Henrick
Notes-taker(s):
Other Members:

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

Open PGP and Thawte Key Signing

URL [OpenID PGP and Thawte Key Signing]()
Convener: Singpolyma, Will Norris
Notes-taker(s):
Other Members:

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

Identity Broker Use Cases

URL [Use Cases for Identity Brokers]()
Convener: Ben S., Ashish J.
Notes-taker(s):
Other Members:

Technology Discussed/Considered: (TAGS)

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

WHISPER Priority Messaging

URL [Whisper Priority Messaging with XDI]()
Conveners: Markus and Drummond
Notes-taker(s):
Other Members:

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

Attendees

Trent Adams, Outreach Specialist, Internet Society
Praveen Alavilli, Software Development Engineer, Amazon.com
Robert Anderson
Joe Andrieu, Founder & CEO, SwitchBook
Martin Atkins, Software Engineer, Six Apart
John Bachir, Software Engineer, JJB Media Ecology
Siddharth Bajaj
Dirk Balfanz
Skip Baney, UI Engineer, Apple Inc.
Daniela Barbosa, Chairperson Data Portability Project
Nathan Beach, Associate Product Manager, Google
Lucian Beebe, Product Manager, LinkedIn
Vittorio Bertocci, Sr. Architect Evangelist, Microsoft Corporation
Henrik Biering, CEO, Netamia
Bob Blakley, VP, [http://www.burtongroup.com
Ryan Boyd, Developer Advocate, Google OpenSocial
Joseph Boyle
Laurel Boylen, Director of Community, Chi.mp Chimp blog
John Bradley, OASIS TC's
Tom Brown, software developer, none
Judith Bush, Software Development Manager, OCLC
Tom Carroll, VP Product Management, Azigo, Inc.
Judi Clark, Digital Coach
Tyler Close
Dave Crocker, Principal, Brandenburg InternetWorking
Sam Curren, Lead Developer, Kynetx
Andy Dale, Software Engineer, OCLC
Peter Dapkus, Product Manager, Salesforce.com
Scott David, Partner, [http:// www.klgates.com K&L Gates LLP]
Peter Davis, Research Fellow, NeuStar, Inc
Breno de Medeiros, Software Engineer, Google, Inc.
Keith Dennis, President, AssertID blog
Rachna Dhamija, Usable Security Systems
Gam Dias, Founder, Xpollen Inc
Cassie Doll, Software Engineer, OpenSocial, Google
Sarah Dopp, Project Manager, Cerado, Boffery, ...Blog
Eric DRAGHI, Consultant
[Blog: http://www.dunlaps.net/darius Darius Dunlap], Darius Consulting
Anthony Eden, [http://blog.anthonyeden.com Blog
Johannes Ernst, Founder/CEO, NetMesh Inc.
David Eyes
F. Randall Farmer , Social Media Strategist, MSB Associates, Blog
Austin Fath
Jim Fenton, Distinguished Engineer, Cisco
George Fletcher, Chief Architect, AOL, LLC.
A Michael Froomkin, Prof., University of Miami School of Law, Blog

STEVE FULLING, Founder & CEO, Kynetx
Dorothy Gellert, Internet Services Architect, Nokia
Cliff Gerrish, President, echovar
Steve Gillmor, Editor, TechCrunchIT
Nicholas Givotovsky, founder, silentrhino
Yaron Goland, Program Manager, Microsoft
Ariel Gordon, Principal Architect, Identity and Security Divisio, Microsoft
Hans Granqvist, Community Engineer, Netflix, Inc
[Website: http://bengross.com/ Ben Gross]
Robert Guthrie, Independent, Independent
Jens Haeusser, DIrector, IT Strategy, University of British Columbia
Kaliya Hamlin, IIW, [Http://wiki.idcommons.net Identity Commons]
Eran Hammer-Lahav, Yahoo!
Meadhbh Hamrick, Protocol Architect, Linden Research, Inc.
Asa Hardcastle, Technical Lead, openLiberty / Wakame Blog
Dick Hardt, Partner Architect, Microsoft
Greg Haverkamp, Computer Systems Engineer, Lawrence Berkeley National Laboratory
Terry Hayes
Michael Helm, Network engineer, LBNL/ESnet
Iain Henderson, Co-Founder, Mydex Community Interest Company
Steve Herbst, UX Research Director, Microsoft
Tom Holodnik, Security Architect, Intuit, Inc.
Love Hörnquist Åstrand
Anne Hutton, security engineer, LBNL
Ashish Jain, Symantec
Kent Jepperson
Joe Johnston, Technology Advisor, The Pachamama Alliance
Gulshan Kapoor
Alan Karp, Principal Scientist, Hewlett-Packard Laboratories
Nishant Kaushik, Identity Architect, Oracle
Dave Kearns, Analyst/Writer, Virtual Quill
Monica Keller, Manager Web Development, MySpace Blog
Gregg Kellogg, Principal, Kellogg Associates
john kemp
Rohit Khare, Hacker, Ångströ
Michael Kirkwood, CEO, Polka Blog
Lou Klepner, President, Gateway To Gov / CivicID
Kristen Knight, VP Product Management, Kynetx, Blog
Dean Landsma, President, Landsman Communications Group
Ben Laurie, google
Guillaume Lebleu, Systems Architect, Diebold
Rich Lee, V. P. Busn & Technology, OPBT, LLC
Mark Lizar
Scott Loftesness, Partner, Glenbrook Partners, LLC
Angus Logan, Senior Technical Product Manager, Microsoft (Live Services)
Scotty Logan, IT Architect, Stanford University
Chris Lunt, CEO, Nombray, Blog

Paul Madsen
Eve Maler, Emerging Technologies Director, Sun Microsystems, Inc.
Pak Mark, Investor
Kevin Marks, Developer Advocate, OpenSocial, Google
Betsy Masiello, Policy & Economics Analyst, Google
Henry Mauldin, Cisco Systems
Theron McCollough, President, PeoplePond
Brett McDowell
Mika McGraw
ariel mcnichol, Founder, co-CEO, mEgo Inc
Chris Messina, DiSo Project, Blog
Jim Meyer, Director, Engineering Services, LinkedIn, Blog
Kai Mildenberger, President, Orbitwerks, LLC.
Dan Miller, Sr. Analyst, Opus Research
Joaquin Miller, Chief Architect, Lovelace Computing Company
Dan Mills, Labs Engineer, Moaill, Blog
Robert Morgan, Identity Architect, University of Washington / Internet2
Chuck Mortimore
Andrew Nash, Snr Dir Identity Services, PayPal
Axel Nennker, Deutsche Telekom AG, Laboratories
Andrew Nesbitt, Software Engineer, Apple, Inc
Will Norris, Blog
Steve Ogden
Greg Oxton, Executive Director, Consoritum for Service Innovation
mike ozburn, President, Opnli, Blog
Rajesh Pandey
Manish Pandit, Principal Architect, E*Trade Financial
John Panzer, Technical Lead Manager, Google
Daniel Perry, Attorney, Law Office of Daniel Perry, Twitter
Bob Pinheiro, Independent Consultant
Ernest Prabhakar, Web 2.0 Product Manager, Apple
David Primmer, Software Engineer, Google
Drummond Reed, Director, Information Card Foundation
David Recordon, sixappart.
Justin Richer, Sr. Computer Scientist, The MITRE Corporation
Darran Rolls, CTO, SailPoint Technologies, Blog
Pete Rowley, Principal Architect, Microsoft
Mary Ruddy, Founder, Meristic, Inc.
Terrell Russell, claimID.com
Markus Sabadello
Eric Sachs, Product Manager, Google OAuth Blog
Tatsuki Sakushima, Manager, R&D, NRI Pacific
Ben Sapiro
Jeffrey Schwartz, disrupter@large, Disruptive Strategies
Scott Seely, Architect, MySpace
Jeff Shan, E-Trade
Luke Shepard, Software Engineer, Facebook

Bill Shupp, Lead Developer, Digg, Inc.
William smith, Sr. Director Business Strategy, Sun Microsystems
Uppili Srinivasan, Sr. Director of Architecture & Development, Oracle Corp
jeff stollman, consultant, secure identity consulting
Peter Tapling, President & CEO, Authentify, Inc.
Don thibeau, executive director, The OpenID Foundation
Allen Tom, Principal Architect, Yahoo! OpenID Blog
Paul Trevithick, CEO, Azigo
Hannes Tschofenig,Nokia Siemens Networks
Gerard Tse, Software Engineer, Google Inc
Ray Valdes, VP Web Services, Gartner Inc
Gabe Wachob
[Website: http://walkah.net/ James Walker]
Bill Washburn, consultant
Karon Weber, Principal Designer, Microsoft
Stephen Weber, Intern, Mashlogic
Phil Windley, CTO, Kynetx
Douglas Whitmore, Software Engineer, Apple Inc
Abraham Williams, Blog
Steve Williams, Independent, =sbw
Katrika Woodcock, Designer, Microsoft