IIWIX INTERNET IDENTITY WORKSHOP 9

A WORKING GROUP OF IDENTITY COMMONS

www.interentidentityworkshop.com

Book of Proceedings

http://iiw.idcommons.net/Notes_iiw9

Complied by Heidi Nobantu Saul

IIW Poroduced by Kaliya Hamlin, Phil Windley and Doc Searls

November 3,4 & 5, 2009
Computer History Museum
Mountain View, CA

Table of Contents

Introduction

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

The agenda for this event was created live. This book is the compilation of all the notes from all the sessions. Our next workshop is coming up May 18-20 in Mountain View California. We invite you to join us - http://iiw10.eventbrite.com.

What is this Workshop about?
The heart of the workshop is a practical idealism in working towards the shared vision of a decentralized, user-oriented identity layer for the Internet. Because the web was built around "pages", no tools or standards were created to control how the information about you was collected or used. At the Internet Identity Workshop we bring the people creating these tools and standards so people can safely manage their online identity and control their personal data It is not about any one technology – rather it is a place to discuss multiple interoperating (and possible competing) projects, standards, and networks for identity, data sharing, and reputation.

As part of Identity Commons, the Internet Identity Workshop creates opportunities for both innovators and competitors. We provide an open forum for both the big guys and the small fry to come together in a safe and balanced space.

There are a wide range of projects in the community:

1. Open conceptual, community, and governance models.
2. Open standards and protocols.
3. Open source projects.
4. Commercial projects.
5. Projects to address social and legal implications of these technologies.
6. Efforts to rethink the business models and opportunities available with these new technologies.

User-centric identity is the ability:

- To use one's identifier(s) on more than one site
- To control who sees what information about you
- To selectively share presence and profile information
- To maintain multiple identities and personas in the contexts you wish
- To aggregate attention, navigation, and purchase history from the sites and communities you frequent
- To move and share your personal data, relationships, documents, and other publications as you wish

All of the following are active topic areas at each IIW:

- Improving Existing Legal Constructs
  - Privacy Policies
  - Terms of Service
- Creating New Legal Constructs
  - Limited Liability Personas
  - Identity Rights Agreements
- Creating New Business Models
  - Identity Oracle
  - I-Brokers
- New Citizenship Perspectives
  - Activism
  - Community Event Coordination
  - Community Identity and Data Sharing

Session 1

Open ID Artifact Binding (1A)

URL: http://iiw.idcommons.net/OpenID_Artifact_Binding

Convener: =nat
Notes-taker(s): Breno de Medeiros

Tags for the session - technology discussed/ideas considered:

Open ID
Artifact Extension

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

Idea: Send smaller payload through the browser (indirect communication).

Goal: Support less powerful mobile browsers that may have stricter URL lengths and no support for Javascript.

Question: How to bind the token to the requester? Standard XSRF protection can be used to bind the request to the browser session at the RP. RP must sign requests to prevent artifact being stolen.

Statelessness: Can be achieved for identity select, some state required for claimed id. Allow artifact to be different in the request and the response to support statelessness.

Maximum length for artifacts should be specified.

Doing it through extensions—not possible, it requires changes to add signatures.

Suggestion: Use two different keys to avoid reflection attacks.

What is Gluu – Welcome to the Metaprise (1C)

URL: http://iiw.idcommons.net/Gluu_Metaprise

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

Tags for the session - technology discussed/ideas considered:

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

** What is Gluu

Jargony answer
Federated directory service and SAML infrastructure with identity

But what is Gluu good for?
Making federation accessible for non-geeks Partner identity management SaaS / Outsourcing Organizational collaboration Help organizations share identity information Inter-domain SSO

** Gluu Workflow

Admin registration
Create Organization
Create Community
Invite other Organizations to join Community

** Gluu Background

Founded ID-Vault in 1998
Interdomain Identity Clearinghouse
Post dot-com bust: enterprise LDAP / SSO consulting British Telecom Federation POC 2008-2009 Birth of Gluu 6/10/2009 Welcome to the Metaprise!

** Overview of Gluu Community

Created by organization. Defines what user attributes are visible in community. Organizations specify what groups of users are shared in the community

** Overview of Gluu Organization

Org Attribute information plus Idenity Assurance Indicators

** Gluu LDAP Directory Information Tree (DIT)

Only organizations can see their own data. Community information is published via LDAP.

** Gluu Synchronization Methods

LDAP / SPML / DSML / Web GUI / Appliance

** Community Privacy Options

Community Visibility
  Public
  Private
  Community
  Custom ?
  Opt-in ?
  SAML Shib controlled information release
  LDAP Opt in attribute?
   Identity Assurance
   Publish information to help organizations understand the privacy
   practices of their partners.

Cloud Selector – Fully Cloud Based Info Card Selector (1E)

URL: http://iiw.idcommons.net/Cloud_Selector

Convener: Susan Morrow
Notes-taker(s): Drummond Reed

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

Susan Morrow of Avoco Secure in the UK demonstrated Avoco's new "cloud selector". This is an Information Card selector that operates entirely in the cloud, rather than on the desktop as is the norm for most Information Card selector implementations. (Higgins and Azigo support cloud-based storage of the Information Cards in one's "wallet", but the actual selector software still runs on the client device.)

The advantages of a cloud selector:

- It requires no client-side install
- It is available from all of a user's devices (laptop, desktop, phone, car, TV, etc.)
- It can provide safe, automatic backup of a user's cards
- It can also serve as an online data sharing service

The disadvantages of a cloud selector:

- It does not provide the same level of security as a local selector – it can be subject to phishing and other attacks. (Avoco has some approaches for mitigating this that Susan demonstrated, such as a way to encrypt a sessionID from the relying party site so the session cannot be easily phished or spoofed.)
- Performance may not be as fast as a local selector (although this can be mitigated by good design and implementation).

More information is available in the article on the informationcard.net blog.

Vulnerabilities and Weaknesses in Identity Protocols (1F)

URL: http://iiw.idcommons.net/Vulnerabilities_in_ID_tech

Convener: Rick Smith
Notes-taker(s): Rick Smith

Tags for the session - technology discussed/ideas considered:

- Information Cards,
- CardSpace

Discussion notes:

A little bit of the blind following the blind.

Cardspace-
User clicks on card selector – transmit to relying party the information.
If it's a self-issued card, then the client sends it directly.
If it's a managed card, the data is still sent by the client, but the client sends a token signed by the "manager," or ID provider.

Cards run in a protected space so that the contents can't be sniffed by other unprivileged processes.

Four risk areas:

A. Native code running on client systems, and/or plug-ins on a browser. Attackers can substitute subverted code and intercept personal memorized secrets that secure the cards, or that are used with IDPs to authenticate a managed identity.

B. Network based attacks – forged transactions or modified transactions used to spoof identity. Most implementations rely on SSL to protect on these. Not all protocols require SSL in all circumstances where it is needed.

C. Subverted or malicious relying party – can the RP turn around and exploit the user's identity to masquerade to another RP?

D. Spoofed IDP – a variant of the network based attack – can an attacker trick the RP into authenticating a user by intercepting IDP transactions and providing a bogus response

TPM modules – there are 300 million machines with TPMs today – we have a way to install secure software and safely manage crypto keys.
Cell phones have a better opportunity to serve as trusted hosts for credentials – we aren't as inclined to put software on our phones (not yet, anyway).

VRM and loyalty cards (1G)

URL: http://iiw.idcommons.net/VRM_Loyalty_Cards_in_Real_World

Convener: Chris Carfi.
Notes Taker: Doc Searls

Chris showed <http://scanaroo.com>, which gives users a way to collect visual versions of their loyalty cards in one app on an iPhone. "Very much a 1.0 product right now." But with lots of potential.

We talked about that potential...

From USER's side, what can be done to improve the experience --and the function.

WE advertise to THEM.

Expressing needs and wants

BugMeNot for Loyalty.

Shopping cart tracking / time shifted checkout (go through store checking out while moving)

Publishing shopping list exclusively to outfits to which we are loyal through Scanaroo (or the equivalent)

Eport/portability of info

"my history" -- a MINT.com for shopping

"Share a Deal"
- location
- product
- time
- store
- me
- price
  - vendors could subscribe to user data

Tagging/Folksonomy... XDI-like

Store Map + item location

Subscribe to 1,2 (at price)

The "Doc Searls" (or anybody) loyalty program. Stores are loyal to individuals, rather than vice versa. Leverage ID standards. e.g... =doc, @dsearls

Concierge/personal shoper

"Find me the nearest X"

Site components (for scanaroo.com or whatever)

Coupons

Data Portability (1H)

URL: http://iiw.idcommons.net/Data_Portability_TOS_EULA

Convener: Steve Greenberg
Notes-taker(s): Elias Bizannes

Tags for the session – technology discussed/ideas considered:
Data Portability, EULA, ToS

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

- We have a traditional world where every service tries to be the "home" store
- Things have changed – we can now export data
- Photoshop plugins, iTunes playlists – not just identity
- Re the EULA terminologu: "Home" means I broadcast data. If anyone else makes a change, I ignore it. The authoritative version of the data
- "Sync" means if you make a change, I update. If I make a change, you update
- "Functional" means it has no desire to store the data at all.
- "Authoritative data" is considered a bad term by audience. What Greenberg means is no importing – it won't accept updates from others.'
- Three types of data: identity, media + content, structure + metadata
- Question raised if this can be implemented in the browser? Like a flagging system to indicate a sites status
- Potential issue: will get too complicated because it can't cover all of a sites data
- Potentially a fifth type of portability: conduit?
- The biggest discussion out of the meeting was that the icons may fail, as it can't possibly cover all the data. It was countered in saying the icons are only part of it – there will be additional detail in disclosures that links off
- Any improvement on accountability and trackability is an impovement on the current situation
- New question: Is the data sent without my knowledge to another provider?
- Should the scope of this work be classed as phase one and as interface work?

Ideal Authz/Authn Consent flow (1I)

URL: http://iiw.idcommons.net/Social_Consent

Convener: Angus Logan + Kevin Marks
Notes-taker(s): Andrew Arnott + Sarah Faulkner

Tags for the session - technology discussed/ideas considered:

- UX
- Consent
- OAuth
- Delegation

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

Request authorization for services from service providers on an as-needed basis rather than all up-front during login. The user better understands why access is needed, and there's a lower fall-off rate during authentication due to the user refusing to grant access to services for which the user does not yet understand (or have) the need.

> Users only see Go and Go Away buttons (sometimes not even the latter). They don't read all the text on the authorization screens.
>
> Google's paper with usability research on this topic.
>
> Questions:

A. How is it done today?
B. What must we tell the user?
   a. What, Why, How Long, To Who
C. How does that get communicated?
D. When do we ask them to choose?
E. Duration of consent? (one time vs. long time)
F. Can a user consent to their friend's data (e-mail address in contact list)?

Notes:

- People are not going to read the text; they may not understand they can opt-out. We need to do the right thing with user's data assuming this rudimentary understanding of consent.
    - Maybe we're not doing the right thing (facebook apps using user's info in ads).
    - Therefore, are there use case clusters that make sense?
    - Cannot expect user to understand the architecture – are we asking users to make decisions they cannot make?

        - Users understand their data and they understand the company they are given to. But does user understand the risk?
- What is the rate of actual acceptance vs. users who decline consent vs. users who bail because they don't understand – do we have data from currently live UI?
- Minimal upfront consent: initial consent flow allows minimal access to data. When service wants to use the next level (post, etc.), the user is asked again to give a higher level of consent.
    - But confirmation dialogues are a failure – "undo" works much better.
    - Progressive escalation model – allows revoke consent (helps combat streams vs. snapshot data like e-mail).
- Reputation trust model – on consent flow, you see friends' accept/revoke info.
    - Need to be careful about when you surface info collection to make sure you have a good sample (i.e. feedback field only on "revoke" page).
    -
- Need a best practices document for OAuth UI
    - Existing advice: Overview of OAuth user experience article -- Search:"OAuth Goog"
- Problem: can lose options – you may want to only share a subset of data, there is no "one size fits all."
- RP's asking just at the time they want to use data can give context to the user.
    - Websites are not going to want to continually interrupt the user. But it may be in the website's best interest to not ask for everything up front, because it will scare the user.
- What is the ideal experience?
    - We assume that the user has a classification system where they understand where to place the app. Users are unsophisticated in who to trust.
- Websites consuming data really wants users to understand what they have granted; they do not want to scare users when they do what was "consented."
    - Give the app a way to explain what they are using the data for.
- Data retention policies?
    - Consumer groups are asking for this; if we ignore it, it will most likely be regulated.
- Facebook: going to give developers access to e-mail address. Want to give developers more trust that the relationship developing with the user will not just go away. RP's need a way to continuously interact with the user.
- UX:
    - Minimal, reversible, understandable, expandable
- Classify the application for the user: explain that the partner is a "gaming" application, so they would like to have the following information.
- Have the user create their own categories of data. But this will lead to a negotiation between the user and the site – users are not informed to know whether they really want to give that permission.
- Asking user "real time" – what if user is not there to give consent?

- Consumers do not understand the value exchange they are getting.
- Paper at SOUPS (available on website) – only thing that consumers read are nutrition labels (presented privacy policy that way and users read and understood). When requesting information, present it in this manner for max understanding.

Social INTER-Networking: Identity In Apps that Span Multiple Social Networks (1K)

URL: http://iiw.idcommons.net/Social_InterNetworking

Convener: Rohit Khare

Notes-taker(s): Rohit Khare

Participants: Paul O, Freshbooks; Arne, Google / OpenSocial; Patrick S, Gigya; Jeff vC, Circlabs; Mary R., Microsoft; Julian, Orange Labs; Henrik; Bo M.

Tags: APIs, privacy, terms_of_service

Discussion notes:

http://thesmallbusinessweb.com/ lists the sorts of software companies that would like to interoperate with each other; Freshbooks routinely handles requests for single-signon and import/export with other Software as a Service (SaaS) sites.

Gigya currently offers its customers the ability to integrate with multiple social networks, typically for letting visitors virally promote content they find with their friends. http://www.gigya.com/public/Content/GS/Home.aspx Customers such as ABC shouldn't have to worry about multiple social networks as long as the intermediary (Gigya) reports back trustworthy statistics.

Visitors of such sites largely care about just one partner network, most often; there is the question of overlap: how often do friends recur on multiple nets; and fragmentation: how many networks do friends use for a single purpose. For example, if you have all your college buddies on Facebook, that's all you'd need; but if some were on LinkedIn as well you'd have alumni in two sets.

Circlabs would like folks to enact "value added workflows" that span multiple people without having to 'reinvent all of facebook or ning'

OpenSocial provides a handy language for Viewer and Owner: when a profile box is viewed by the owner, it may have an editor; a non-friend may see less than a friend would.

A group rolodex may be appropriate for small business crm; how to federate without copying? (Google Shared Contacts API came up)

Many folks use the FB/G Connect services primarily to be able to push back to a visitor's activity stream; not necc, to do more complex analysis of friends, interests, and such.

With Connect, many partners choose to upload their entire customer database as hashed emails, solely to let the dominant partner compute which friends of a visitor are also using the site.

JS-Kit echo() came up. Other comment syndications across multiple social networks can lead to infinite loops (copying status from A to B to A to …)

Blending all of the UI elements of multiple networks to a lowest common denominator is a bad idea. Users rely on social and visual cues to manage their relationships. It's a concern raised about a UI like Threadsy too

If we're going to share information across networks, can users benefit by seeing, say, a "guest book" of which friends have clicked through their shares from all of the networks; or warn them by "previewing" how many connections will get to see this item?

Session 2

OpenID Attribute Exchange v.1.x , 2.0 (2A)

URL: http://iiw.idcommons.net/Attribute_eXchange

Convener: Nat Sakimura, NRI
Notes-taker(s): Tatsuki Sakushima, NRI

Attendees:
Nat Sakimura (NRI)
Dick Hardt (Microsoft)
Henrik Biering (Netamia)
Mike Hansen (Mozilla)
Andrew Arnott (Microsoft)
Will Noris (Internet2)
Ragavan Srinivasan (Mozilla)
Breno de Medeiros (Google)
Ilan Caron (Google)
Hannes Tschofenig (Nokia Siemens Networks)
Bharath Kumar (Amazon)
Tatsuki Sakushima (NRI)

Tags:

OpenID Attribute Exchange Protocol and Syntax
Not Schema!

Session Slides:

http://docs.google.com/present/view?id=dhsz4ffx_160d4mqqkc3

AX 1.1? and beyond

=nat (Nat Sakimura)

Issues raised in AX 1.0

- Introduce the concept of more generic schema for sending/requesting properties about attributes.
  - Class: The new attribute property schemas attach to specific attribute types.
    - Each attribute property schema is bound to a unique attribute-type namespace, can be described by a standard key string (does not need to be defined through a URL value).
  - Query-Response: Attribute property values can be transmitted within any request or response type, allowing communication of attribute properties in both directions in direct and indirect communication request/response pairs.
- Direct Communication: Introduce a direct communication method in both directions (OP<->RP), supported via discovery, for bulk exchange of attributes about (potentially) multiple users.

- Privacy Policy/Sreg features: Update AX to include support for RPs to send a link to their site's privacy policy to the OP. This feature is currently supported in SREG 1.0 and was omitted in AX 1.0.

Approach to solve these issues in AX 1.0

Class

- Now: e.g.
  - ax.type.fname=http://schemas.openid.net/name/first
  - ax.fname.value=Nat
  - ax.type.lname=http://schemas.openid.net/name/last
  - ax.lname.value=Sakimura
  - etc.
- New:
  - ax.type.name=http://schemas.openid.net/opensocial.name
  - ax.name.family_name=Sakimura
  - ax.name.given_name=Nat

Query-Response: Request / Response AX

```
$ diff openid-attribute-exchange.xml oax1.1.xml
793a794,796
>                 <t>
>                         In addition, any parameter values may be sent with the Response
as in Fetch Response.
>                 </t>
```

This one line change will allow us to send data to OP and get back the processed data back in the response.

Or: Parameter to Fetch Request? --> This seems to be better way.

Direct Communication

- Solved in Artifact Binding

Privacy Policy URL

- In SREG: openid.sreg.policy_url can be specified in the request.
- In AX 1.0, it cannot, because you have no way of sending such data in fetch request, nor way to fetch data via Store request.
- If Store request can also fetch data, the problem is solved: Just the matter of defining standard type URI for privacy policy.
- i.e., "Bidirectional" solves the problem.

Next Steps

Finish Easy things first, then move onto harder topic.

AX 1.1

- Add parameter to Fetch Request.
- Privacy Policy Advertisement

AX 2.0

- More efficient Schema
- Data format: XML or JSON?

Discussion:

- AX Protocol Proposals and Issues from Nat.
- There are lots of interests in “schema” and “schema registory” but not be covered here.
- Make it more generic. 4 areas to improve:
  1. Class
  2. Query Response
  3. Direct Communication
  4. Privacy Policy
- Avoid key/value pair(limited capability) and support richer data structures/formats like XML or JSON.
- Also “direct communication” and “different syntax for request and response” are required to make this happen.
- Metadata for attributes like “verified email or just email” → a schema issue? But at least a new format and syntax provide spaces for metadata.
- How to implment a notification service for geolocation in AX? → unsolicited assertion to update_url can be used.
- Is “Privacy Policy” is metadata? → policy_url for Terms of Conditions of Attributes given to RP like Sreg has. The group agreed on this addition to AX.
- Should Policy URL is in a signed request or written in XRD to be fetched from RP? → Artifact binding or Contract Exchange for making a signed request.
- Query Response is used to store and fetch data in the same time. → Need richer syntax for a fetch request.

Next Steps:

1. Class. → Go for it! Support XML, JSON not only a key/value pair.
2. Syntax → Make richer.

The Business Case for Data Portability and Interoperability (2B)

URL: http://iiw.idcommons.net/Biz_Case_for_Data_Portability

Convener: Elias Bizannes

Tags for the session - technology discussed/ideas considered:

- Business case,
- modeling,
- portability,
- economics,
- adoption,
- maximizing value

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

Dataportability Business Case
Information Value Chain
P (Data creation -> Information generation -> Knowledge Application)
S [storage]
  [processing]
  [distribution & socialization]

Theory: Specialization leads to comparative advantage

If you get different people focusing on one key part of the chain each, then everyone can get better value, thanks to specialization.

Counter: However, diversification is more profitable than specialization… or at least it appears that way. Because of customer acquisition costs, many companies work to maximize how much they can monetize from each customer by offering more and more services and functionality.

Perhaps improved data quality and the resultant reduced costs is significant. "50% of a Business's cost infrastructure exists to compensate for not knowing what the Consumer already knows…"

John McKean, Author "Information Masters - Secrets of the Customer Race".
www.informationmasters.com

So, is the business case 100% cost savings?

Not necessarily. What about e-commerce that can reduce the % of abandoned shopping carts?

Perhaps the measure is engagement?

Counter: The primary theory doesn't necessarily actually encourage or suggest or explain the business case for data portability. It supports specialization, but that could lead simply to kieretsu-based dependencies between members of the chain. In order to make a case for portability, you'd have to make the case for interchangeability between elements in the same layer in the value chain.

Key obstacles to adopting this kind of model?

1. Does it make sense
2. Cultural? NIH & thinking in specialist models

Recommendation: the Big Switch

See an Identity Selector for Open ID (2C)

Or Experimental Active Client for OpenID – Microsoft demo *(2C)*

URL: http://iiw.idcommons.net/Identity_Selector_for_OpenID

Convener: Mike Jones, Ariel Gordon, Oren Melzer, Chuck Reeves
Notes-taker(s): Greg Horton and Ariel Gordon

Tags for the session - technology discussed/ideas considered:

- OpenID;
- Active Client;
- Selector;
- User Experience;
- Security

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

This is a presentation of an experimental selector for OpenID. The goal is to evolve OpenID together to address known issues:

- To improve both its usability and security
- While providing a smooth migration path

This prototype is meant to stimulate discussion about possible futures for OpenID and is intended as starting point – not the destination.

The selector is meant to be optional—a "better together" value proposition in the sense that it will provide a better and safer experience when present, while not preventing users to access their favorite sites from any computer.

Mike gave a short presentation of the selector being used at Plaxo and several sites using JanRain's RPX. He showed what happens, starting with the situation where the user already had an OpenID but it has not yet been used on that site. The selector includes notice that the Yahoo OpenID provider is "verified" and may be trusted. (assuming the existence of a white list service – see below). The second time you login on that site the selector tells the user the last date/time they logged in to this site using the Yahoo! OpenID. Going to another site (www.interscope.com) – as more sites are visited the selector remembers the user's OpenIDs used in the past. This time logging in using a vanity URL. This provider was "Not Verified" and the user needs to check an extra box "Continue, I trust this provider". Cannot login using that OpenID unless the box is checked.

Summing up what the Selector does. First of all, it remembers your identities for you and shows "last used" information. If I'm using Google or Yahoo, chances are that there will be buttons for those on the RP's "NASCAR", but if I'm using a niche identity provider, I'm never going to see a logo for it. The second thing it does is that it contacts the Identity Provider for me. This effectively helps protect users against being sent to a phishing site by a rogue RP.

How does it work? The Relying Party includes some code in its sign in page (for the prototype, we've reused the Information Card Object Tag syntax and added some parameters in there.) When visiting an RP that's been enhanced to support a selector, and if I use a computer that's equipped, the selector will pop up to manage discovery and build the initial authentication request for the OP.

The prototype postulated a white list of “known trustworthy” OPs. No user trust decision in UX when interacting with white-listed OPs (e.g. Yahoo, Google, MyOpenID) versus explicit user trust decision when interacting with unknown OPs. This is one basis for phishing protection (another is the selector remembering my OpenIDs!)

Mike presented a couple of slides with some of the issues that came up as a result of building the prototype selector. For example:

- Allowing OPs to advertise their friendly name and logo
- Managing OP-specific parameters such as association handles
- Use of unsolicited assertions
- How should selector decide that two identities are equivalent? Compare post-discovery endpoints?
- How should the selector be triggered? Right now using Object Tag. Should look at HTML 5 work on universal login tags

There are also many things that the experimental selector doesn’t do. For example, we’d like the selector to eventually allow OPs to interact with users over a dedicated html surface, as opposed to redirecting the full browser window (which it does today).

There will be more sessions at IIW to work on how to make this work more smoothly.

Participants list:

Name	Company	
Greg Haverkamp	Lawrence Berkeley National Lab.	
Ashish Jain	Paypal	
Dhiva M	ESnet	
Brian Holdsworth	Microsoft	
Nico Popp	Verisign	
Cliff Gerrish	Echovar	
Michael Duffy	The Trust Network	
Dirk Balfanz	Google	
Jamie Nelson	Sun	
Peter Tapling	Authentify	
Ron Carpinella	Equifax	
Patricia Wiebe	BC Government	
Darren Platt	Symplified	
Sharif Youssef	Acxiom	
Kent Spaulding		
David Chadwick		
Vijay Pawar	TriCipher	
Dale Setlak	AuthenTec	
John Bachir	Ganxy	
Yeryeong Park		
Hank Mauldin	Cisco	
Markus Sabadello	Azigo	
Ernest Prabhakar	Apple	
Craig Spiezle	Online Trust Alliance	
Greg Horton	Microsoft	
Mike Jones	Microsoft	
Oren Melzer	Microsoft	
Ariel Gordon	Microsoft	

Enterprise Use of Consumer Identities (2D)

URL: http://iiw.idcommons.net/Enterprise_Use_of_Consumer_Identities
Convener & Notes Taker: Pamela Dingle
Tags:

Notes:

Activity Streams Work Session (2&3E)

URL: http://iiw.idcommons.net/Activity_Streams

Convener: @ciberch - @chrismessina @johnpanzer

Tags for the session - technology discussed/ideas considered:

Discussion notes:

- Agreement to collaborate w/Salmon
- Using http://activitysreams as rel value
- Discussion of design requirements for Activity Stream Website

Attendees

- Ray Valdez
- David Recordon
- Mike Ozburn
- Joseph Boyle
- John Panzer
- Monica
- Brian Kissel
- George Fletcher
- Eran Hammer
- John McCrea
- Joseph Smarr
- Eran Sandler
- Scott Logan

- salmon/PuSH
  - uses ATOM
  - intent is to align with activity streams
  - "salmonella"
  - no anonymous comments
  - can be authenticated by anyone
  - "magic security pixie dust"
  - align these efforts... use activity streams
  - using webfinger for author URI
- discovery/Hammer Stack
  - web-linking
  - rel="http://activitystrea.ms"
- website
  - homepage
    - description of project/problem statement
    - who's using
    - what, why (benefits), how
    - testimonials
  - verbs
    - example representation
  - objects types
    -
  - media types
  - library
  - code samples
  - use cases
  - presentations
  - calls to action
    - wiki

        - mailing list
        - public task list
- logo
- profile photo standard
- OpenSocial/JSON
- implementor's spec
- "upconverting existing feeds"
- IPR

Activity Streams

Structure   Verbs   Feeds   Flow

* Unstructured (twitter status)
* Media Item (posted a photo, video, etc)
* Action-based (read this, viewed this, added friend, etc)
* Comment (pointing at another item)

Subject,	Verb,	Object,	Context
Kevin	Posted	this Photo	on Flickr
	Commented on		

Payload?

Producer expresses the relevant metadata and the consumer site interprets this and display it.
Could have a nice default rendering from a site.
Template is separated from activity so that consumers can choose a template to use.
Need a template format. Do we require a template, or can people push unstructured data?
Snippet vs. full version?

Atom structure:

* Title
* Summary
* Content (can be out of band)

How does OpenSocial do this?

Plaxo uses FriendConnect. They lose the original site and think everything came from FriendConnect.
Consumer needs favicon, etc which is currently missing.
Problems with how we deal with backchannel pushes into feeds.
Sites like dig can't justify pushing to many (consumer, user) pairs

Orthogonal things:

* Schema for presenting the data
* A way to format the data
* How the connection is initiated
* Different ways the data can flow

Issue/Topic: Privacy Risk Assessment (2F)

URL: http://iiw.idcommons.net/Privacy_Risk_Assessment

Convener: Jeff Stollman
Notes-taker(s): Steve Holcombe

Tags for the session - technology discussed/ideas considered:

- Privacy,
- Risk,
- FTC,
- Regulation

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

The FTC will soon be holding hearings regarding the risks (physical, financial, reputational) to consumers of data elements (e.g., firstname, lastname, email, birthdate, socialsecuritynumber, etc,) stored by retail companies and/or online search companies. Risks of data breaches to national security may also be considered.

Questions:

Global ramifications of data breach exposure? What is low risk in one country may be high risk in another country?

Should there be U.S. laws limiting retailers to certain storage/usages of data and prohibiting others?

Should liability risks be legislated regarding certain data elements? Certain aggregations of low risk data elements that may become riskier by their aggregation?

Should the FTC establish and assess fines for data breaches calculated by loss of high risk, medium risk, and low risk data?

Kantara will be proposing to the FTC a data breach risk assessment based upon (a) risks assigned to specific data elements and/or (b) aggregation of data elements of varying risks.

Final comment: Privacy risk regulations may support large data storage utilities (who can afford legal staff to meet regulations) because of costs to storing certain data of varying FTC assigned risks that smaller businesses will not be able to meet.

What is the Most Important Question to Ask When a Request Comes In?(2G)

URL: http://iiw.idcommons.net/Question_to_ask_for_request

Convener: Alan Karp
Notes-taker(s): Michael Schwartz

Tags for the session - technology discussed/ideas considered:

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

Most important question: is the request authorized?

Delegate-able authorization: without it the private in the army would be saying "yes sir, mr. obama", that would be the only way.

OAuth consciously conflated authz, authn and identity.
The goal was not to exchange credentials service side gets token "letting it be me for a period of time"

Tyler Close "web key" : REST based federation. Good paper: "ACL's don't"
Authorization based access control is safer than SSO.

Sample Case:

Two Companies: A and B
Memorandum of Understanding between companies
Authz: Only US citizens can perform this action: Use XACML to express policy When user invokes service, he prevents delegation chain.

Alan Karps http://www.hp.com/alan_karp - might be wrong.
Look for papers.

ZBack : Authorization based access control

Legal Layer of the Stack (2I)

URL: http://iiw.idcommons.net/Legal_Layer_of_the_Stack

Convener: Scott David
Notes-taker(s): J. Trent Adams

Tags for the session - technology discussed/ideas considered:

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

Session Objectives:
 * Overview of concepts relating to legal/technology interfaces of identity
 * Identify potential useful work to "Map the Gap" between technology and law/regulation
 * Feed session results into a "Map the Gap" event planned for technologists and lawyers in Washington DC scheduled for February, 2010

General Discussion:
 * Linked information systems are "porous"
  + it is possible for data to be shared beyond the intended acquisition
 * Rapid technical innovation accelerating rate of information exchange
  + Law and culture lag behind technology advancement
  + Lawyers aren't in the business of predicting the future
  + Question of how to manage for "social" stability
 * Technology supports what are essentially "social" interactions / transactions
 * Business systems (driven by technology) require people to function
 * Interactions between people are codified by agreements (convention and contractual)
 * Interfaces between people are codified by legal agreements
    + "Lawyers are in the people-programming business" - Scott David
 * Part of effectively "mapping the gap" involves both technologists and lawyers
 * People need to understand both the technologies and laws
  + corollary: people need to understand technologists and lawyers
  + corollary: technologists and lawyers need to understand people (their needs & wants)
  + corollary: technologists and lawyers need to understand each other

Identified Needs:
 * Common nomenclature and/or translation scheme
 * Agreements for technology interoperability
 * Agreements for data-sharing interoperability
 * Guidelines for:
  + Effective interaction (technical and operational)
  + Violation monitoring / handling
  + Mitigation responses

  + Dispute resolution
 * Identifying cross-jursidictional issues

Research & Evaluate Existing International Work:
 * Policies and regulations (legal)
 * Recommended guidelines (consortia)
 * Best practices (technology)

Next Steps:
 * Identify pain points
 * Potential solutions for the pain:
    + Taxonomy / common terminology across legal/technology gap
    + Scenario planning to understand long-range needs
    + Simple "test case" solution as starting point
        - E.g. Legal boiler plate defining the Attribution - Authentication - Authorization process in line with OMB 04-04 and NIST SB 800-63

Twitter – What's With It (2M)

URL: http://iiw.idcommons.net/Twitter_What%27s_with_it%3F

Convener: Kaliya
Notes-taker(s): Maureen

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

- **Twitter,**
- **Microblogging,**
- **URL shorteners,**
- **Privacy**

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

- Phil's blog on Why he uses Twitter was influential

- Twitter is better than Facebook – more communicative/opt in/opt out without "unfriending" someone

- Twitter Lists changes everything – Kaliya will blog on this

- Bit.ly – url shortener, keeping track of links & who rebroadcasts your links RT@____handle:(tweet)

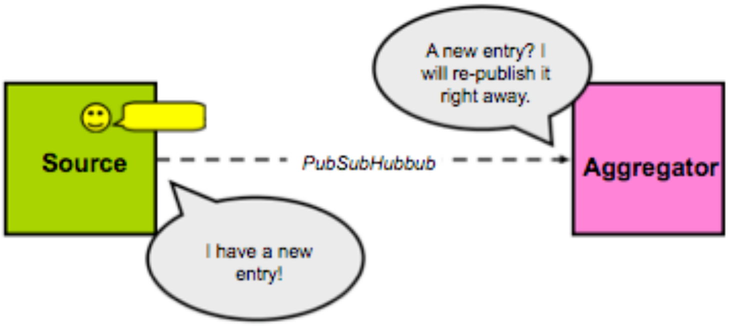
Session 3

Salmon Protocol (3A)

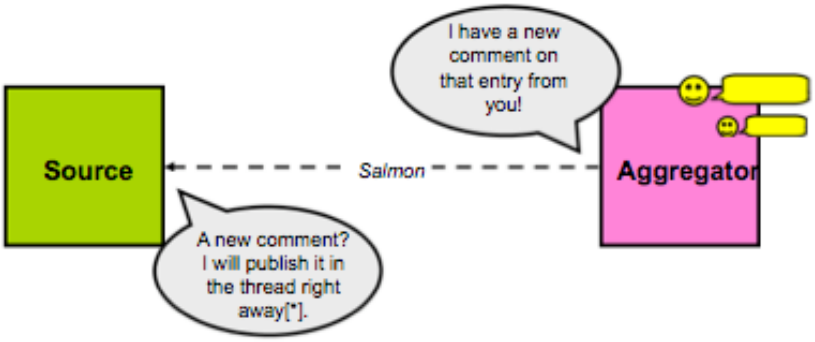
URL: http://iiw.idcommons.net/Salmon

Convener: Johnathan Panzer
Notes: Johnathan Panzer

1. New entry is posted on Source, pushed to subscribers via mechanisms such as PubSubHubbub, and re-published by an Aggregator

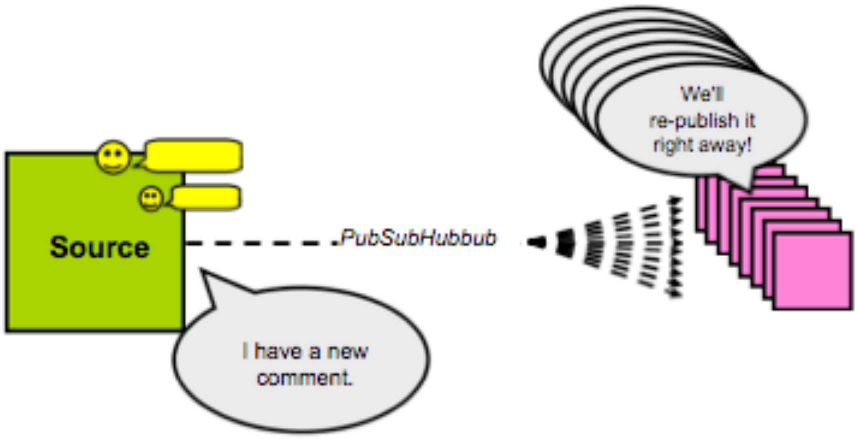


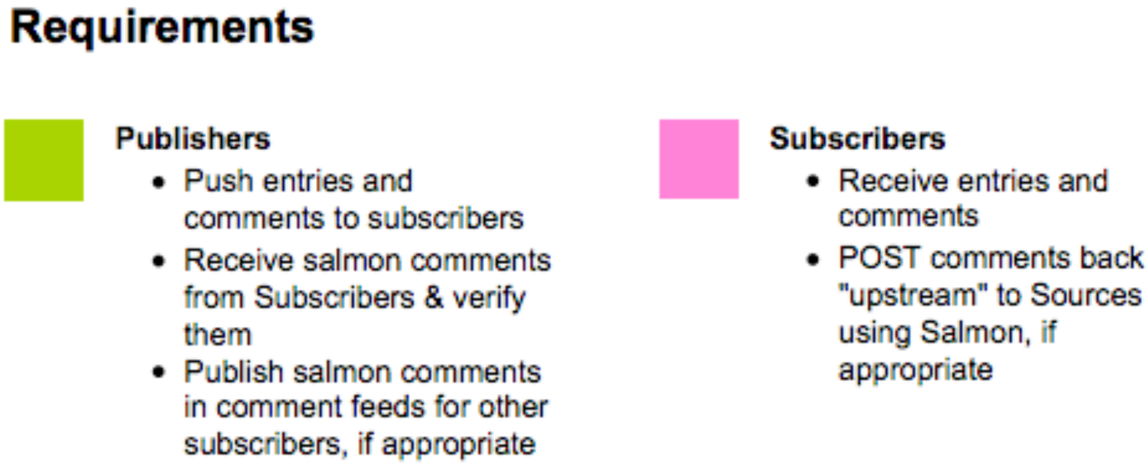
2. New comment is posted on the Aggregator. It pushes the comment back upstream to the Source using Salmon


I have a new comment on that entry from you!
Source
Salmon
Aggregator
A new comment? I will publish it in the thread right away[*].

[*] After using magic security pixie dust to verify provenance.

3. The Source pushes the comment to all subscribers





Requirements

🟩 **Publishers**

- Push entries and comments to subscribers
- Receive salmon comments from Subscribers & verify them
- Publish salmon comments in comment feeds for other subscribers, if appropriate

🟪 **Subscribers**

- Receive entries and comments
- POST comments back "upstream" to Sources using Salmon, if appropriate

Also see the Salmon Protocol Summary:
http://www.salmon-protocol.org/salmon-protocol-summary

Evangelism for Identity (3B)

URL: http://iiw.idcommons.net/Selling_to_Consumers

Convener: Paul Wolff
Notes-taker(s): Paul Osman

Tags for the session - technology discussed/ideas considered:

- OpenID,
- Identity,
- Data Portability,
- Evangelism,
- Marketing,
- Political Activism

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

- Who to evangelize to? B2B or B2C?
- Most efforts so far have been targeted towards site operators (B2B).
- B2B evangelism is still beneficial. Rely on them to educate consumers about benefits / value / etc. (Teach the teacher).
- How to market to consumers? Message is confusing (Too many choices!).
- How to simplify the stack (easy to implement, easy to use).
- What distribution / marketing channels to use?
  - We're an industry. Do we need a foundation (is it OpenID?)
  - What's been successful? Media (Fear mongering)
  - Inject the message into the user experience (i.e. remember sites directing users to update insecure browsers).
- Successful case studies (EV Certs, Creative Commons, Privacy Policies)
- Parallel with history of credit cards (i.e. used to be one per merchant, then VISA and MC convinced users that “membership had benefits”).
- Progressive disclosure: Don't expose everything to the user at once. Ease them in.
- Start with low risk but high value (i.e. start with friendfeed, not banks).
- Messages:
  - “Safe Identity”
  - “Let My Data Go!” - Agit-prop campaign, make consumers demand it
  - “Membership Has Its Benefits!” - VISA and Mastercard approach (it's a club!)
- Next Steps:
  - Get to the root of the problem (data portability? Identity?)
  - Solve the cognitive gap (Life Identity vs. Accounts)
  - Participants exchanged email addresses, another session proposed.

User Managed Access (3F)

URL: http://iiw.idcommons.net/User-_Managed_Access

Convener: Eve Maler
Notes-taker(s): Eve Maler and Jeff Stollman

Tags for the session - technology discussed/ideas considered:

- #UMA
- #UMAF2F
- #identity
- #privacy
- #policy
- UMA,
- Kantara Initiative,
- user-managed access work group

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

We reviewed the basic proposition of User-Managed Access as captured by the ongoing work of the Kantara Initiative's UMA Work Group (http://kantarainitiative.org/confluence/display/uma/home).

The WG held a F2F meeting yesterday, and we also reported on the very latest protocol design decisions and got feedback on them.

We invite interested people to join the group and contribute; it's free to join. Just visit the UMA site for the group participation form, background materials, requirements and use cases documents, and fledgling spec text.

Goal is to create support for user-permissioned data sharing.

Three domains IDM, VRM, and Social Web 2.0 have desire to share data to make life better.

Avoid digital shadow (data that gets out about you that you don't want out there). For example, data that is stolen and used for Identity Theft.

Three elements:

1. Host (site that hosts person's data – a use can have many hosts for different data or the same data)
2. Requesters (sites that want your data) E.g., requester may be someone who wants to access your calendar feed to keep updated access to your calendar. Requester might be you, someone else or company

3. Authorization Manager (broker agent that manages transaction between Host and Requestor. Serves as Policy Decision Point and Policy Access Point. Enforces terms and conditions, not just policies.

Benefit to user: You can set something once and it will persist. It will also provide auditability of whom you have authorized and what transactions have taken place.

KantaraInitiative.org has lots more data on what has been documented. Go to groups and selected "User Managed Access.

Nat: his research shows 2% remember everything that they authorize; 50% remember only first few authorizations

Paul Bryan gave a detailed walk through of a generic scenario. Detailed scenarios are detailed on the Kantara Initiative site. Provides claims-based negotiation between the Requester and the Authorization Manager.

ID Report gets verified identity of both parties to support a transaction.

Email sucks, so what's next? (3J)

URL: http://iiw.idcommons.net/Email_Sucks_What%27s_Next

Convener: JAM
Notes-taker(s): JAM

Tags: Why email sucks, why email's good and what we would create if we could.

Discussion notes:

Here were some things which we came up with about email:

- Good - Distributed
- Good - Standardized
- Bad - Hard to prove authentication
- Bad - SPAM!!
- Good - Used by nearly everyone
- Bad - Not real time
- Good - Easy to use
- Bad - No way to enforce "no forwarding" policies
- Bad - Not designed for a lot of uses, i.e. public threads.

We came up with a small plan as to what we wanted to do. Who knows if that will get anywhere, but it's still interesting to think about. What we came up with was something similar to Wave, but with better "access controls" and we wanted it to be peer to peer.

Session 4

Attribute Aggregation (4A)

URL: http://iiw.idcommons.net/Attribute_Aggregation

Convener: David Chadwick
Notes-taker(s): David Chadwick

Tags for the session - technology discussed/ideas considered:

- Grouping attribute claims together
- Authenticating the user
- Service Provider Policy

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

It was agreed that multiple attributes from multiple IDPs are needed in a single session.

Most IDPs (probably all) are also SPs, and most only issue a single attribute to users. (Passports and driving licenses are the exception rather than the norm).
This means that with Information Cards the user needs to be able to select multiple cards in one go.

Paul showed a video from a French consortium, FC2, that have built a demonstration version of a multi-card Information Card selector.

The Card Selector must be capable of authenticating the user to the highest LOA level possible (4) but should only authenticate the user to the lowest level that is sufficient for the current SP.

The authentication needs to go from the user to the selector, and from the selector to all the IDPs whose attribute claims are needed.

The two signature technology from Identica could be helpful.

Many organisation use the back channel today, and this model may still be helpful for picking up extra attributes. The card selector could be an enabler for setting up back channels.
This could be coupled with the Kantara UMA work so that the user's policy on card selection is always followed.

The SP's policy needs to say which attributes are wanted and which issuers are trusted to issue them. The policy also needs to say what Level of Assurance (LoA) is needed for each attribute.

The card selector should pre-select the cards that are most appropriate for the SPs policy.

It would help the user experience if the card selector could automatically evaluate the SP's policy and carry it out automatically with little or no user involvement. Only involve the user in exceptional situations. The card selector could have defaults built in so that it automatically knows which set of cards to send to a particular SPs.

One problem that was identified is that users may go for one supercard that gives them most accessess to most SPs with with least hassle. Maximum privileges rather than least.

But this can be countered by having a single attribute card that can be asserted at the 4 different LOA levels depending on the strength of the user authentication in the current session.

OpenID Security Issues: Protocol and Browser (4B & 5B)

URL: http://iiw.idcommons.net/OpenID_Security

Convener: Breno de Medeiros, Michael Hanson
Notes-taker(s): Michael Hanson

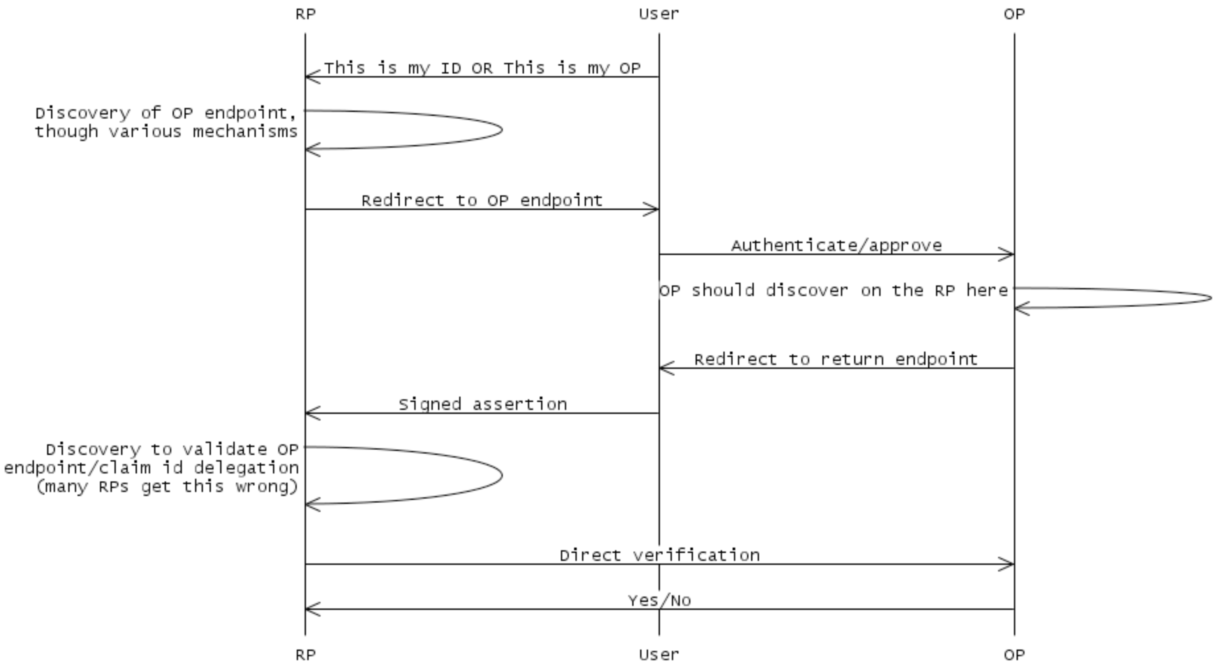
Tags for the session - technology discussed/ideas considered:

OpenID Security – Phishing – HTTP - Strict Transport Security - Content Security Policy

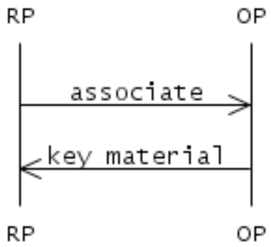
Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

OpenID Security discussion is held on this list:
http://lists.openid.net/mailman/listinfo/openid-security

Protocol Discussion: Flow for authentication:


RP
User
OP
This is my ID OR This is my OP
Discovery of OP endpoint, though various mechanisms
Redirect to OP endpoint
Authenticate/approve
OP should discover on the RP here
Redirect to return endpoint
Signed assertion
Discovery to validate OP endpoint/claim id delegation (many RPs get this wrong)
Direct verification
Yes/No
RP
User
OP

Flow for association:



Threats:	Solutions:
DNS Spoofing: discovery could be intercepted, leading to MitM attack on metadata exchange Is this unique to OpenID? No, not really, but because OpenID is so dynamic, the DNS threat is more serious for OpenID than for other systems that rely on DPS.	1. Use HTTPS. This is a best practice; see GSA document (link?) 2. Use signed XRD? Working group looking into it. 3. We should make a security upgrade recommendation to the spec. ?
Web defacing/social engineering: a not-sufficiently-diligent RP could be fooled into following a bogus claimed ID link. Can be difficult to detect. The metadata is invisible, and an attacker that has taken control of the webserver can use cloaking to only serve up the corrupted content to some parties.	1. Don't allow dynamic metadata negotiation? Negates much of what OpenID stands for. 2. Better web security in general. Not really something we can do. 3. Signed XRD? Allows dynamic discovery but prevents casual defacing. Reduces to a previously-solved problem (trust framework for XRD distribution), but it is a hard previously-solved problem. There is nothing in the spec right now about trust frameworks. If signing is optional, the OP has no way of knowing that security has degraded.
Security degrading: An attacker could replace a signed XRD with an unsigned one, or from HTTPS to HTTP, and the OP may not notice.	1. Best practices (again, see GSA document) 2. Library work/better support
Session swapping: An attacker causes a user to log into the attacker's account: attacker starts the process, catches the response, and introduces that to the user, so the user signs in as the attacker at some RP. Attacker can that harvest data from the user, etc. The RP can't tell which browser the login started from.	1. RP-initiated authentication should use standard XSRF techniques, but there are protocol pieces that could make it better. Not well specified what should happen to parameters in the return URL: If an OP implements support of the return-to URL, could the attacker not put state into the return URL? Some disagreement here. 2. Introduce some nonce that is in common between the user agent and the RP, and make sure they match? 3. It is believed that there is no way to defeat this attack for unsolicited assertions with the current spec.
Login XSRF	Similar to session swapping.
Threats that derive from a compromised OP: If the OP is evil, it can log in as the user.	1. For Yahoo's proprietary SSO protocols, each RP has a pre-associated user-specific shared secret; if you break into the OP and have access to the OP's database, you can still impersonate. No such defense exists for their OpenID implementation.
Open redirector (with checkid_immediate)	1. Best practices
Association poisoning: a rogue OP could deliberately cause a handle collision.	1. Spec improvement? Recommendation.
RPs do not check to make sure all fields are properly signed.	1. Best practices 2. Audit? test-id.org has many tests (q.v. discussion of trust frameworks)

General Discussion:

Formal threat analysis? Some Stanford grad students did a study:
http://www.stanford.edu/class/cs259/projects/cs259-final-newmanb-slingamn/report.pdf

There was a discussion about supporting unsolicited assertions without enabling session swapping.

The spec is a bit vague on which extension parameters should be signed. The namespaces aren't signed in many cases. Attribute exchange is often not signed.

We need guidelines for what gets signed and what RPs should expect to be signed.

Part 2:

HTTP/S Issues

Server conveyance of HTTP policy to client
HTTP extensions, in process:
* Client-security policy
* Origin header
* Cross-Origin resource Sharing
* Content Sniffing
* Strict Transport Security ("Forced HTTPS")

Client/Browser Issues

1. Stronger transport binding in browser extensions?
 * Holder-of-key in a selector?
* Access to SSL keying material?
* Binding of keying material to transport (SRP)?
* Hard to do on shared hosts - not an issue for secure domains?

2. New client approaches: active selectors?
* Consistency for user is key
* OP in a popup box: easy to spoof?
    Best practices exist to try to make it better: e.g. address bar must be displayed
    Do we need a popup phishing blacklist?
* Run in privileged chrome? e.g. toolbar
* If the RP could really know what ID to use, the experience could be better/safer, but users don't understand the question
* How does a selector authenticate to/from the browser extension?

3. Rich Apps and OpenID: We need another session for this.

Building Action Cards (4C)

URL: http://iiw.idcommons.net/Building_Action_Cards
Video URL:

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

Tags for the session - technology discussed/ideas considered:

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

It was more of a demo. This is probably the most relevant write-up I have:

http://www.windley.com/archives/2009/09/the_forgotten_edge_and_the_purposecentric_web.shtml

The Forgotten Edge: Building a Purpose-Centric Web

Abstract *Since it's inception, the primary metaphor of the Web has been one of location. By framing the Web as a collection of places, we have necessarily caused Web development to focus on servers. But people don't get online to go to a server. They get online to get something done—achieve a purpose. This talk argues that focusing on purpose allows us to build Web applications that more closely align with what people want from the Web. Focusing on purpose will require a move to more intelligent client-side applications.*

Technological development in the area of Internet identity over the last several years has left us well prepared for this move to the client. In particular, we argue that identity selectors are a great platform for building these purpose-managing client-site applications. Coupled with a rise in social networking tools that give individuals greater voice in conversations with the organizations that server them, these advances promise a Web that is less focused on location and more focused on purpose. We conclude with six rules for a purpose-centric Web and a call for others to join in helping build it.

Introduction

In 2003, Doc Searls and David Weinberger wrote an essay called World of Ends. The thesis was simple: "the Net is a world of ends. You're at one end, and everybody and everything else are at the other ends." This idea that the ends are what is important online is critical to understanding where the value lies and how to best add value to the 'Net.

From 1993, when the Web was brand-new, to the present we have largely focused our attention on one type of end, or one edge, if you will: the server. Browsers have been seen as a given, something that is and works. To create value online, most people have worked at the server. This has created a pat formula for online success, repeated over and over:

- Get a good address
- Build a killer site with great content
- Advertise to get traffic
- Make the site sticky
- Convert traffic into sales or eyeballs
- Rinse and repeat…

There's nothing wrong with this, of course. Working at the server has created an amazing array of Web sites and services that simply astound me.

But I believe there is significant value to be created at the edge of the network we call the browser. And that for the most part we've ignored it. Browsers have gotten flashier and fancier over the years, but for the most part their job is simple:

1. Go to a URL
2. Get the content
3. Render the content properly
4.

That's not to discount the tremendous and enormously fertile world of browser extensions, but in truth, only Firefox has made browser extensions easy enough to create a significant extension ecosystem. Building extensions for Internet Explorer or Safari is not for the faint of heart and requires real expertise.

Our focus on the server is related to the primary metaphor we use for understanding the Web: *location*. We "go" to Web "sites" using an "address." The first decade of the Web has been characterized as a "land rush."

The problem with ignoring most of the endpoints on the Web is that it leads Web application developers to force fit things that would be better done on the client using a server instead. Portals are one example. Portals try to pull multiple applications and data together into one place to make it more convenient for people to use. Travel portals are a good example.

But portals are rarely successful in really giving people what they want. The answer isn't better personalization. They answer is to move that functionality to the client.

The location metaphor isn't bad; after all, servers *are* places. The problem is that it doesn't go far enough. I believe that we can extend the location metaphor in a way that gives us a new way of thinking about how to solve people's problems.

The Purpose-Centric Web

Most people don’t fire up their browser to go somewhere, rather they want to accomplish something. While going places is part of finishing a task, it’s not enough to just go someplace unless that one place happens to have everything you need. More often than not, online sessions consist of visits to multiple Web sites over time. Consequently, a better metaphor for building Web applications would be purpose.

As an example, consider the purpose of “finding a book to read.” Finding a book is not necessarily the same as going to Amazons or Borders. Those are great sites to browse for books, read reviews, and buy books; but, what if I my preference is to check the book out from my local library when it’s available? Right now, that requires that I visit at least two sites: Amazon and my local library. I connect those experiences together by conducting the same search on each and then collecting the data.

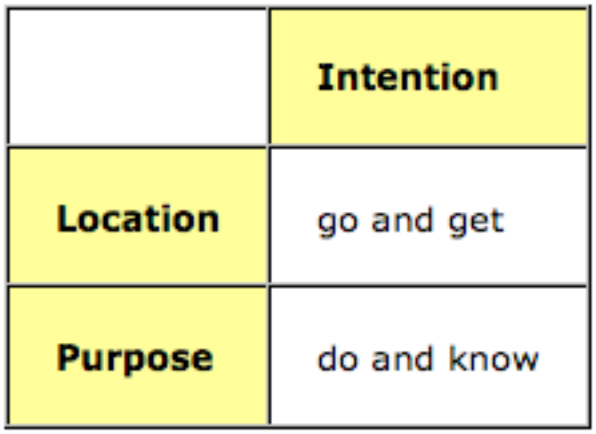
“Finding a book to read” is a relatively simple task compared to other tasks that people do online everyday. A more complex example is “planning a vacation.” People spend weeks and visit dozens of Web sites planning their vacations online. It’s rarely the case that one Web site provides them with everything they need. That is simple counter to the distributed nature of the Web itself.

Let’s return to the task of finding a book and consider how it might be made simpler. The browser can see both Amazon and my library’s Web site. A tool, on my browser, could modify Amazon to inform me when I’m looking at a book that’s available at the library like so:

http://www.youtube.com/watch?v=MMPxLu_foiQ&feature=player_embedded

As this video shows, an intelligent, adaptable browser helps people achieve their purpose rather than simply taking them to a Web site.

A purpose-centric metaphor supports a different intention than a location-based metaphor. The following table, which we’ll expand later, shows this:



	Intention
Location	go and get
Purpose	do and know

In a location-based Web we “go and get” whereas in a purpose-centric web we “do and know.”

Identity on the Web

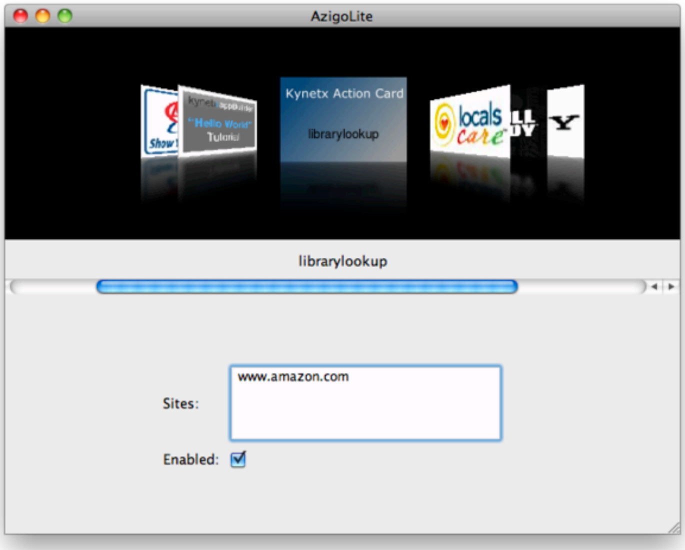
Back in 1993, I was part of an email list that was discussing ecommerce (although it wasn't yet called that). There were two things that people *really wanted*: a way to take credit cards securely and a way to create a shopping cart. The first was solved with the emergence of SSL. The second required cookies.

HTTP is a stateless protocol, meaning that each request is processed independently of any previous requests. That's great for returning pages of text, but makes building things like shopping carts—which are by definition stateful—difficult. Cookies are tokens sent by the server and stored by the browser to be returned to the server with any subsequent requests *to that same Web site*. They were the answer to build shopping carts and other applications that require intra-site state like authentication systems.

Because cookies were good enough for most things people wanted to do on the location-based Web, there wasn't much interest in identity systems that went beyond cookies. But cookies have some significant limitations. Most relevant to this discussion: browsers are designed to only share cookies with the site that sent them. This ensures a level of privacy and security, but makes it impossible to use cookies as the basis for a purpose-centric Web. At best, they could only be used when sites have decide to cooperate beforehand.

These limitations caused people like Kim Cameron at Microsoft to look beyond server-based solutions and decide that a special purpose client was needed. Kim invented an identity system called "information cards" based on a card-metaphor—something very familiar to people—that uses a special client called a "selector."

Here's a screenshot of the AzigoLite selector:



Sites: www.amazon.com

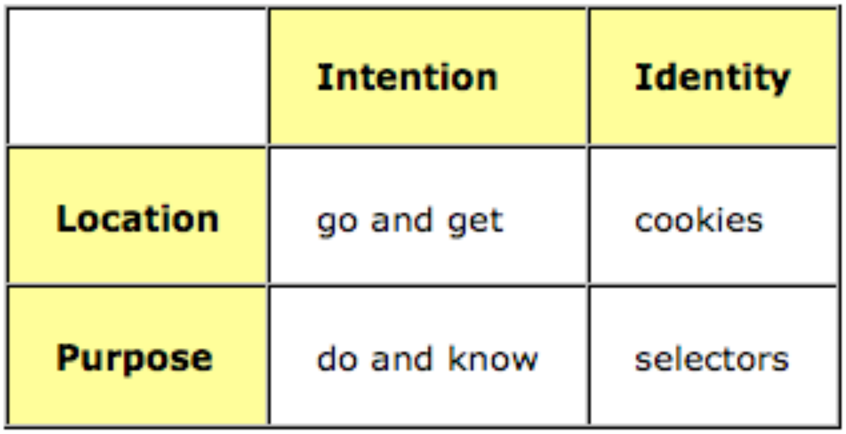
Enabled: ☑

Each of the cards in this selector have an “action” attached to them, making them into client-side Web applications that have the ability to coordinate activities at multiple sites. Of course, because it’s just a card in the selector, if the person doesn’t like what the card is doing, it’s easy enough to delete it or turn it off.

Card selectors provide some significant features for the purpose-centric Web:

- selectors provide real, cryptographically sound identity
- the selector model provides protection for personally identifying information
- selectors provides smart client that can be used to message user in a secure way
- Strong identity model provides foundation for certification and reputation of cards and their associated applications

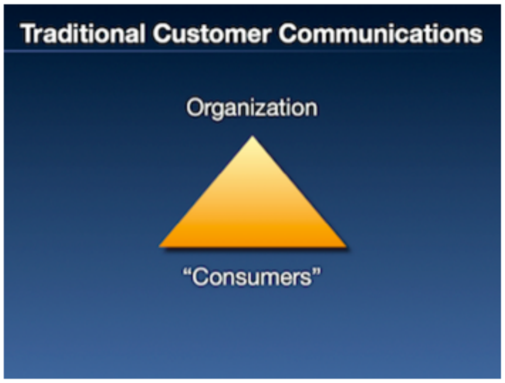
Strong, cross-site identity, like that provided by a card selector, running on a client, enables purpose-centric browsing. We can add this our matrix:



	Intention	**Identity**
Location	go and get	cookies
Purpose	do and know	selectors

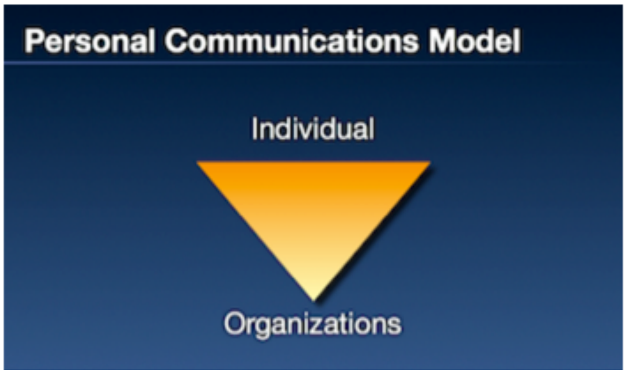
A New Communications Model

Moving to a purpose-centric Web will allow us to change how organizations have come to relate to individuals online. In the traditional customer communications model—supported by advertising and CRM systems—organizations broadcast information to individuals in a top-down manner.



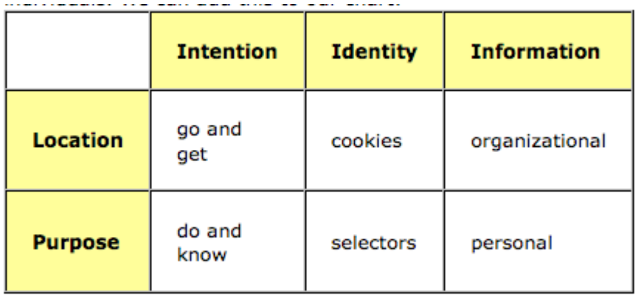
Over the last century, this form of communication has gotten less and less personal while at the same time businesses tried to make it more and more targeted. With the Internet, this has only gotten worse as businesses put ads on Web sites and turned to ever more invasive tactics to increase the click thru rate. The result is ironic: the closer companies get with demographics, the more their customers resent it and retreat.

Companies have to rely on demographics when identity is missing. But as we've seen, new technologies are adding an identity layer to the Web. An identity layer provides an opportunity to flip the traditional demographics-based model on it's head. In the new personal communications model, information flows from the individual to the organization. These flows are owned and initiated by the individual.


Personal Communications Model

Why would people do this? Simple: to increase their choice and the level of service they receive. In fact they already do. When someone posts information about their interactions with companies on Facebook, MySpace, Twitter, or a blog, they are actively engaging that organization and sending information through a personally controlled channel that smart businesses will capitalize on. The rise of Web-site independent identity will only accelerate this trend toward active participation.

This is an important component of the purpose-centric Web because only the individual can tell us their intention or purpose. A purpose-centric Web requires active participation by individuals. We can add this to our chart:



	Intention	**Identity**	**Information**
Location	go and get	cookies	organizational
Purpose	do and know	selectors	personal

Note: See Craig Burton's essay on The Inverted Pyramid for more on this idea.

Rules for a Purpose-Centric Web

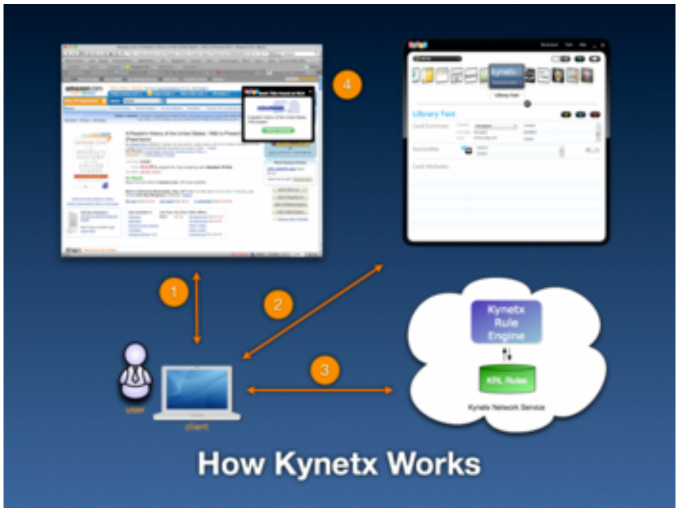
There are a number of important principles, or rules, that we need to remember if we are to capitalize on purpose:

1. **Purpose matters more than location.** To an individual using the Web, giving them a place to go only goes so far in helping the accomplish their goals. We provide significant, additional value when we, instead, help them achieve their purpose. Many Web sites have recognized this, but few have really achieved it because of our focus on servers.
2. **Freedom of choice matters more than controlling the user.** The traditional way companies have approached customers is as “things” to be “owned,” “controlled,” “locked up,” and “targeted.” In the emerging model, individuals have considerable power. Wielding that power will level the playing field. Companies that recognize this power shift and work within it are more likely to build customer loyalty.
3. **Context matters more than content.** Content is dead—or at least not a very good way to differentiate. Just ask the newspapers. But putting content in context, as in the library lookup example I give in a preceding paragraph, makes it more actionable and this more useful and valuable.
4. **Relationships matter more than transactions.** The lifetime value of a customer is obviously much greater than any single transaction—if you can get them to come back. In a world where goods have been commoditized and a cheaper price is only a Google search away, building relationships matters more than ever. I talk to people all the time to shop preferentially at Amazon, even when it’s more expensive, because it’s familiar, convenient, and has their trust.
5. **Loyalty matters more than “time on site.”** Most of the traditional Web site KPIs are structured around the traditional, broadcast-style communications model and heavily influenced by the location metaphor of the Web. Companies spend money on ads with microscopic click-thru rates. They spend money to make their sites “sticky” to entice the click-thrus to increase “time on site.” Finally, we measure conversion that represents a fraction of a fraction of a fraction of the people who originally were shown an offer. Conversely, if you offer people a way to achieve a purpose on the client, you have started to build a relationship that can be nurtured to create real customer loyalty.
6. **Individuals matter more than demograpics.** Knowing that I’m a white, male from Utah who drives a truck is better than nothing. But it’s much better to know that right now, I’m in a hotel in Vegas and really need an iPhone charging cable and that I’m willing to pay for someone to get it to me. Under the right circumstances, individuals will freely share relevant information making demographic data less and less valuable to companies ready to work with customers rather than shout at them and lock them up.

Kynetx and Purpose-Centric Web Applications

Kynetx is an infrastructure provider with the goal of making purpose-centric applications easier to build. Kynetx works at the client-site of the Web thus enabling applications that work across multiple Web sites.

Here’s how the Amazon Library Lookup example we showed earlier is done:



How Kynetx Works

1. The user visits Amazon
2. A browser extension queries the card selector to determine if any of the installed cards are relevant to Amazon
3. If so, a request is sent to the Kynetx Network Service (KNS) execute the Kynetx ruleset associated with that card (given in the card’s metadata)
4. KNS returns custom Javascript for that request which modifies the page DOM and thus rewrites tha page to show the notification

Kynetx bridges the individual silos represented by Amazon and the Minute Man Library to create an integrated experience for the user that more closely aligns with the user’s purpose: find a book to read.

With any new platform, security is a concern. This is especially true on the client. Kynetx recognizes this and is working hard to address it. We don’t have all the answers, but believe that a combination of identity selectors on the client and rules in the cloud provide numerous hooks for building an effective security model that protects users while giving them the advantages of client-side applications.

A Call to Action

The client is on the Web’s forgotten edge—largely ignored by developers. Web sites are locations—useful in accomplishing a goal, but unable to provide a complete experience. But by centering development at the client, developers can build applications that span multiple Web sites and help people with purpose. If information card selectors are to serve as a platform for this purpose-centric Web, there is still a few missing pieces.

Some of the missing piece are things like standards that will allow everyone to play in this purpose-centric Web. Those are coming.

The most notable “missing piece” is that the Microsoft CardSpace selector does not yet support purpose-centric Web applications. If our vision of a purpose-centric Web is to become a reality, selectors must become ubiquitous and users need choice. The Azigo selector can be used as a foundation for controlling purpose-centric client-side applications. Users would be well served if the CardSpace selector were similarly enabled. We call on Microsoft to be part of this effort.

If you’re interested in exploring Kynetx and building your own rules, sign up for a develop account. - http://www.kynetx.com/signup They’re free.

This essay presents the material from the slides from my keynote speech at Digital Identity World given on September 15, 2009 in Las Vegas, NV. The slides from my talk are available online -http://www.windley.com/docs/2009/forgotten_edge.pdf (PDF).

Microformats (4E)

URL: http://iiw.idcommons.net/Microformats

Elgg OpenSource Social Networking Platform: What it is and what we're doing with it (4F)

URL: http://iiw.idcommons.net/Elgg

Convener: Justin Richer
Notes-taker(s): Justin Richer

Tags for the session - technology discussed/ideas considered:

- Social networking,
- opensource,
- openid,
- portable groups

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

MITRE has been doing research with social networking for the past few years using the Elgg platform (http://elgg.org), which is an OpenSource whitebox social networking system. We've used Elgg to build social networks for the intelligence community and MITRE itself. Elgg is highly modular, and is designed from the ground up as a user-focused social networking site, as opposed to the more common CRM with social-like artifacts bolted on. Elgg also has pervasive fine-grained access controls on every artifact in the system.

In the intelligence community, the OneCommunity research prototype is installed on the Intelink network, accessible to US Intelligence Analysts. We developed plugins to allow connection into the existing Intelink Passport identity structure to let users make use of existing credentials. We also developed connections to other social software systems on the Intelink network, such as Intellipedia (a MediaWiki instance). We have worked with analysts to build a recommendation system that is aware of the social media artifacts created by users that can recommend potential working contacts. Our research has shown that people, even in this serious working environment, are interested in social information and "icebreakers" in order to facilitate new conversations.

At MITRE, we used the same software to build out two sites, MITREverse and Handshake. MITREverse is MITRE-only and resides completely inside the firewall. It has acted as a research testbed for our user recommendation and data connection systems. We believed early on that we did not want the social network to own all the data, but to have access to the data available on other tools. We have developed an

OAuth module for Elgg to allow for connection to WordPress and our own microblogging tools. This also has the possibility of allowing multiple Elgg sites to connect to each other to create a federation of independent social networking islands. The possibility of portable groups and portable permissions system seem very great in this area.

Our other site, Handshake, is designed as an outward-facing social network hosted by MITRE to facilitate collaboration with MITRE’s sponsors, academics, and industry people. All MITRE employees have access to Handshake through a custom IdP system, and all external participants are invited by MITRE personnel. This leads to some very interesting problems with identity, such as the need for MITRE to (currently) manage all the accounts for non-MITRE users of the system. This is something we are currently looking to move away from, perhaps by allowing OpenID credentials or other forms of trusted-partner identification.

In parallel, we are looking at deploying an OpenID system for MITRE personnel both inside and outside the firewall to allow MITRE people to self-identify as MITRE people both to our own OpenID-enabled applications and to sites on the larger Internet. We are also researching trusted partner networks and the implications of having portable data across different sites and what that means for access controls and permissions.

Defining Meaningful Claims for Citizen and Enterprise Claims (4G)

URL: http://iiw.idcommons.net/Defining_Meaningful_Claims

Convener: Patricia Wiebe

Tags for the session - technology discussed/ideas considered:

claims, roles, legal, persona

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

Roles:

Employee
Legally Designated Professional
Dad
Husband
Hobbyist
Alumni
Student
Citizen
"is not"
amazon user
gmail user

Claims:
Domain
in bldg D, 4th floor
what division
level of security

Claims about Citizens:

- legal surname
- legal given names (in BC, 3 legal names are possible)
- address - mailing, physical delivery, geo location
- gov't program identifiers, e.g. health #, education #

Claims about enterprise users:

- employment type (employee, contractor)
- position title
- employment role (manager, director)
- organization id
- organization type (gov't, business, corporation, proprietorship)
- professional role/designation

professional body

metadata claims:
identity provider id
level of assurance
verification method

Should we separate authentication layer from claims layer?

openid
LiveID

"Persona": a role a person assumes for a particular context (e.g. acting as a father for some particular purpose, later acting as an employee for another purpose)

Use case: user wants to play a game for a week, they are pseudonymous in the game

Use case: user becomes an avid biker for six months, joins all the forums,

Use case: govt's are already collecting information about users in the form of claims so they can provide appropriate services.

Who do we trust to make claims?
Avid bicyclist: self-asserted
More sensitive claims: only from entities who can verify those claims

Trust is important, but it is not a binary value. There are degrees of trust and assurance.

Trust is not a hierarchy, either. Some claims can only be made by merchant bureaus, other claims can only be made by gov't, other claims are best self-asserted.

Are we conflating the policies around claims with the authentication technologies used?

Yes, for practical reasons claims tend to be made by particular identity providers, so policies and authentication technology get intertwined.

Username/Account is one type of claim, typically verified with a password.

Liberty Project has a concept of identity provider separate from attribute provider.

Use case: one university asserts username and role to another university (probably with Shibboleth). Second university makes an access control decision based on that role. How do we pass those roles around?

Use case: bank allows a user to view their account based on username and password, but wants additional authentication before allowing money to be transferred.

Do we need to add a third "outcome" dimension: (roles or claims) + (action) = outcome

Example: porn site needs to know that user is of legal age in certain jurisdiction

But legal age is not absolute, it varies from jurisdiction to jurisdiction, and for different actions. (For example, legal age for drinking is different from one country to another.)

Assertion: as soon as you talk about assurance and claims, you are also talking about liability.

Concordia discussion group has had long discussions with application owners about what barriers there are to accepting claims from remote parties. This started as a discussion about authentication level of assurance, but moved to attribute level of assurance.

See also: Tao of Attributes

See also: identityschemas.org

See also: previous discussions at various IIWs. Reuse of schemas is *hard*. This creates a tower of babel, with different environments creating competing schemas that all look very similar. US Department of Defense spent months trying to agree on a schema, only got 15 attributes everyone could agree were useful.

Context is another important element in access control:
- authentication (how did they authenticate?)
- claims (what statements about the user are being made?)
- context (what is the current situation? is the user in a secure location? what time is it?)

Another example: physician accessing records from hospital premises has different rights than a physician accessing records from home.

Where does that context come from? Does it become a claim? Or do you do it at the transport layer?

Example: drinking age

If IdP asserts date of birth, there is potential for confusion. Should permission to drink be based on jurisdiction of bar? Or user's jurisdiction?

Maybe IdP should assert permissions claims "old enough to drink" instead?

Maybe IdPs should stick to stating facts they can verify (born on this date) and leave interpretation up to IdP.

Example: doctor

Doctor might be a radiologist, but that doesn't mean they have permission to view all X-Rays. They also need to be your primary care doctor, or be authorized by the primary care doctor?

Permission claim: implies authorization, transferable from someone with authorization to another person.

Attribute claim: statement of fact about an entity

We have a claims translation problem: it is really bad if N IdPs and M RPs all need to translate claims back and forth. It would be bad if you had N * M explosion in the logic required. Alternative is to have a translation service, where translation service translates N different claim formats to a single format, and from that single format to M RP claim formats.

Assertion: only Permissions claims should cross organizational boundaries. Almost nobody agrees with that assertion.

Counter example: passing around physical location/delivery address does not fit into the "permission claim" model, but is a very common use case.

“Claims Fiesta” Roles, Claims, and Personas (4G) 2nd set of notes

URL: http://iiw.idcommons.net/Defining_Meaningful_Claims

Convener: Patricia W of British Columbia, Brian H of Microsoft
Notes-taker(s): Judith Bush

Tags for the session - technology discussed/ideas considered:

Claims – Roles – Personas - Affiliations

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

Whiteboard beginning

ROLES

Legally Designated
professional
Employee
Dad / Husband
Hobbiest
Alumni/student
Citizen

CLAIMS

Domain
In building D
4th floor
division
level of security

Claims
Roles = Identity of Person
Personas

NOT
“affiliations”
Amazon user
Gmail user

Citizen
Legal surname & given names (in British Colombia, three legal names are possible)

Address – mailing
- physical delivery
- -geo location

Gove program identifiers
Health #, education #

ENTERPRISE
Employment type
Position type
Employment role
Organizational id
Org type
Professional roles
Professional body

Auth layer

Why: to provide services

Claims: self asserted and externally (trusted) assertion – levels of assurance

Verification of claims – at auth layer?

Conflation of verification of claims and identity provider

Username & password: is it a minimal claim? Ownership of an identifier.

Whoever authenticates you is not necessarily the right place for the claim to come from. Compare Liberty model: Identity Providers and Claim Providers.

Classic levels of assurance – start with username & passwd.

Do Claims go with Role? Or Claims establish a Role in a system?

The challenge of mapping roles and claims between different systems.

Claim needs level of assurance to support the provider’s need, but not necessarily the identity/authentication.

The RP needs to know what claims it needs to what level of assurance; it’s the job of the authority is to have the correct level of assurance (which incurs liability).

Some self asserted claims may be more valuable than from a trusted agency (addresses are dynamic).

Levels of assurance distinguished from level of trust. One argument of financial liability being measurable. Compare to a Concordia discussion group.

Context is relevant (time of day and right to access to building). Relying parties separate the claim from the context in determining the permissions allowed.

Alan Karp advocates delegation of rights, exchanging permission claims – attribute claims only within a domain.

If the relying party has to recognize claims from different domains (EG: medical agency in BC recognizing professional credential attributes in any province/state.)

Alan Karp insists that the only claims that can be transferred across domains is permissions & delegation.

Resources – but reuse is hard:
* IndentitySchemas.org
* Tao of Attributes

Session 5

OpenID in Scientific Computing + Legacy Apps (5A)

URL: http://iiw.idcommons.net/OpenID_for_Science_Community

Convener: Dhivakaran Muruganantham & Michael Helm
Notes-taker(s): Michael Helm

Tags for the session - technology discussed/ideas considered:

OpenId, authorization, legacy

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

Intro to OpenID – Dhiva's slides
Discussion about Grid computing in a nutshell
X.509 based, but also other tools like ssh & ftp used in distributed computing
Questions about how we register people to get X.509 certs (technology embedded in grids)
How do we authorize jobs?
    Privileges &tc in a database
    Gridmap file the core of how job privileges are managed, ultimately
    Here is a subject name (DN) – here you can recognize it
        Then there is a separate access control system that manages

How do we bring OpenID into grids
Or, why do we wnat to do this?
We could simplify user registration & access experience
Want to minimize other kinds of expenses – heavy crypto authentication operations, browser support issues

Q: Is this a case where ppl want to use browsers but not certs
A: Can be script based and have the same problem!

We have:
We have web portals for distributeed computing
We have browser-based ssj & ftp tools in Java Start
We have a way to bridge between existing X.509 infrastructure & OpenID service (eg our Esnet Openid provider)

We don't have:
OpenID outside web browser context to START WITH
Science community doesn't social networking tech (yet!)
(definitely not in Grid context)

Our complex use case:

- Delegation using proxy certs
- Need scheduling, batch jobs, scripting, reporting, monitoring
- OpenID for services as well as people
- Support for authoriztion

NPE non person entity

How do I support legacy apps
Alan Karp: How do I know I should I honor this request? I need to present an authorization'
CAS was almost right – but the root of trust is wrong

Bob Morgan:
You are trying to have a unified policy space, make the identity processes work across those spaces
When I get a DN, I can map to the user id in accounts database
Perhpas manage keys

HP product provided wrappers & proxies for users for legacy services

Can we simplify the management burden? For the case where
People get shell access w/ ssh or do scriptring w/ X.509?

AK: PI gets contract & gets grant of authorization right
Use the X.509 certs locally instead

Grid is reaching its user scalability problem m users at n hosts
Need to simplify this.

Key insite: user interface inclueding managerment interface can't change much (or slowly)

What are the LBL problems?
They are maybe harder & maybe on a smaller scale
Wedging openid into a problem it doesn't fit into – it's a web convenience protocol

What can we do for legacy apps?
Is there a PAM/ssh we can develop?
Somebody at google has mentioned using XMPP with Google.
Protocols expect user name & password scenarios

Conclusions:
Need to look more at longer range alternatives
Look at PAM and external selectors
OpenID is problematic her

Identity in the Browser and Other Security Topics Related to Active Clients. (5B)

URL: http://iiw.idcommons.net/Identity_in_the_Browser:_Security_and_Protocol_Issues

Convener: Jeff Hodges
Notes-taker(s): Breno de Medeiros

Tags for the session - technology discussed/ideas considered:

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

Items:
-HTTP/S and browser approaches
-New client approaches (active selectors?)
-Automatic validation/ auditing

Server convergence of HTTP policy to client:

Content-Security Policy
Origin header
Cross-Origin resource sharing (W3C/HTML5)
Content-sniffing
Strict transport security (forced HTTPS)

Holder of key in a selector?

Access to keying material in shared
Binding of keyed material to transport (SRP)
Hard to do on sliced hosts …

Consistency for user
OP in popup box: easy to spoof?
Browser toolbar – privileged chrome
address bar must be displayed : what if it isn't?
Popup phishing whitelist/blacklist
If the RP could really know which id to use, the experience would be softer, but would the user understand?

How to best leverage a 2nd authentication setup step?

Role of 3rd Parties in Enabling – Trust Frameworks (5F)

URL: http://iiw.idcommons.net/Role_of_3rd_Parties

Convener: Lena K
Notes-taker(s): Michael Schwartz

Tags for the session - technology discussed/ideas considered:

SAML, Federation, Identity Assurance

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

- Several 3rd party services could emerge to facilitate federation
- Identity Assurance Indicators are needed by RP's to make decisions about how to use information from IDP's
- Role of third party is to make federation easier

What An RP ~~Wants~~ Needs (5G)

URL: http://iiw.idcommons.net/What_an_RP_Needs

Convener: Joseph Smarr
Notes-taker(s): Joseph Smarr

Discussion notes:
SLIDES:

What an RP Wants - *Part II,*

Joseph Smarr

11/02/09

◦

What we said in February

Hybrid OpenID/OAuth is a game-changer

Plaxo/Google integration proved the “Chasm of Death” can be crossed

92% success rate

We need all the major players to become first-class OpenID Providers (OPs)

- More user data (profile/email + contacts)
- User-friendly (not scary) consent UI
- Auto-login on return (checkid_immediate)
- Commitment to do what it takes for both sides to be successful
- What’s happened since(ship early & often)

What’s happened since

What’s happened since e an OpenID RP and joined the OpenID Foundation

OpenID

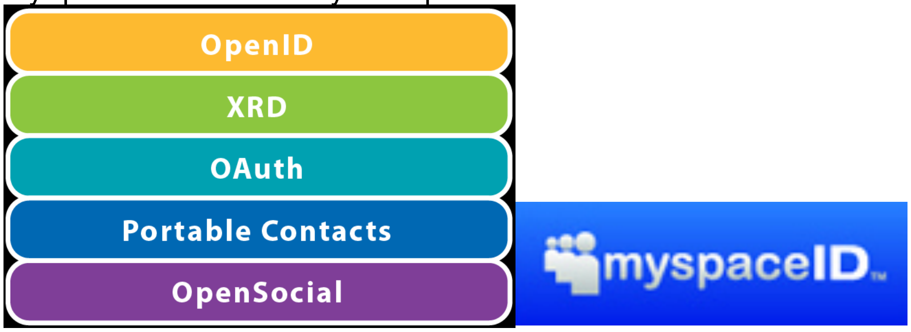
facebook

Plaxo built a deep 2-way integration with Facebook

Plaxo and **Facebook** are now in an open relationship.

(using Facebook Connect)

MySpace rolled out full Hybrid/Open Stack



OpenID

XRD

OAuth

Portable Contacts

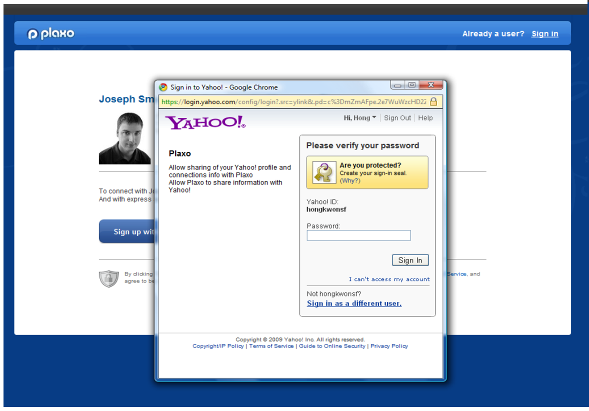
OpenSocial

(though without validated email address)

Microsoft declared they'll do OpenID for real

(though were vague on timing)

Yahoo rolled out Hybrid.



Sign in to Yahoo! - Google Chrome

https://login.yahoo.com/config/login?.src=ylink&.pd=c%3DmZmAFpe.2e7WuWzcHD2

Hi, Hong | Sign Out | Help

Plaxo

Allow sharing of your Yahoo! profile and connections info with Plaxo
Allow Plaxo to share information with Yahoo!

Please verify your password

Are you protected?
Create your sign-in seal.
(Why?)

Yahoo! ID:
hongkwonsf

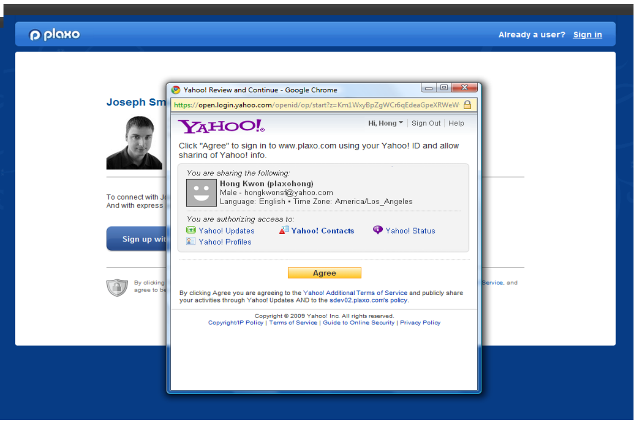
Password:

Sign In

I can't access my account

Not hongkwonsf?
Sign in as a different user.

Copyright © 2009 Yahoo! Inc. All rights reserved.
Copyright/IP Policy | Terms of Service | Guide to Online Security | Privacy Policy



Yahoo! Review and Continue - Google Chrome

https://open.login.yahoo.com/openid/op/start?z=Km1WxyBpZgWCr6qEdeaGpeXRWeW

Hi, Hong | Sign Out | Help

Click "Agree" to sign in to www.plaxo.com using your Yahoo! ID and allow sharing of Yahoo! info.

You are sharing the following:
Hong Kwon (plaxohong)
Male - hongkwonsf@yahoo.com
Language: English • Time Zone: America/Los_Angeles

You are authorizing access to:
Yahoo! Updates | **Yahoo! Contacts** | Yahoo! Status
Yahoo! Profiles

Agree

By clicking Agree you are agreeing to the Yahoo! Additional Terms of Service and publicly share your activities through Yahoo! Updates AND to the sdev02.plaxo.com's policy.

Copyright © 2009 Yahoo! Inc. All rights reserved.
Copyright/IP Policy | Terms of Service | Guide to Online Security | Privacy Policy

What *hasn't* happened since
Still waiting for more great OPs

- Facebook (Hybrid RP)
- Microsoft (Doing OpenID, but OAuth?)
- AOL (OpenID, but not 2.0 or Hybrid)
- Twitter (OAuth, but OpenID?)
- Plaxo (Hybrid RP and PoCo Provider)
- LinkedIn (?) Still waiting

So, where do we stand?

- Significant progress, though more slowly than we might have hoped
- But the fact is, I cannot recommend a new startup bet their business on being an RP
- Why?
- Still a bunch of unsolved issues and un-met needs… for more great OPs

What an RP Wants - nope....
What an RP NEEDS.

- More high-quality OPs
- Desktop / mobile / API best practices
- Solution to the "Nascar problem"
- Confidence that RP users are 1st class
- Virtuous cycle

Desktop / mobile / APIs

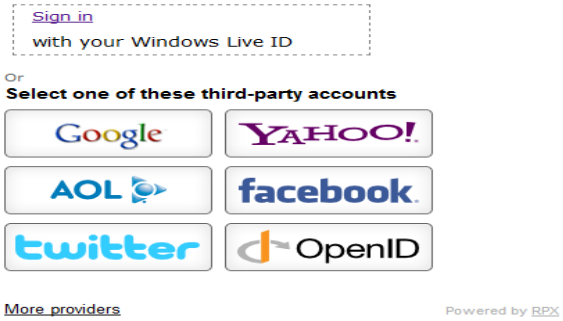
- OpenID login is a web-only solution
- As an RP, how do my users log in to:
  - My rich desktop client
  - My iPhone app
  - My REST API
  - My TV widget
- Option: use OAuth flows as a bridge

  - Pop a browser for OAuth flow
  - Log in using (web-based) OpenID
  - Need some way to tell the client to continue
- Option: direct auth API proxied to OP?
  - Simpler UI, but assumes username/passwod
- Do this for all users, or just RP users?
  - Consistency vs. complicating the base case

Solution to the “Nascar problem”

Solution to the “Nascar problem”

- How many buttons?
  - What about smaller OPs?
- What to do for return users?
  - Visits from other computer?
- E-mail addresses as IDs?
  - What about OPs that aren’t webmail providers

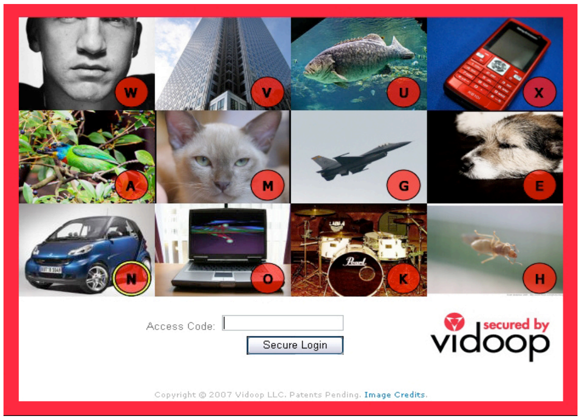

Sign in
with your Windows Live ID

Or
Select one of these third-party accounts

More providers
Powered by RPX

Confidence in RP users

- Part perception issue, part reality
- What happens when an OP dies?
- If users get trained by login buttons, can I ever move/change them?



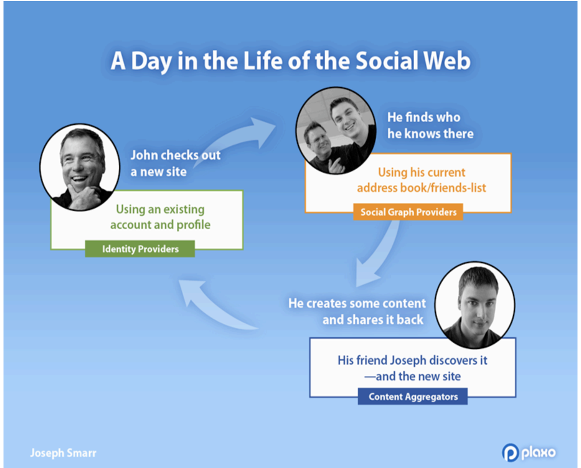
Access Code:

Secure Login

secured by vidoop

Copyright © 2007 Vidoop LLC. Patents Pending. Image Credits.

Virtuous Cycle



A Day in the Life of the Social Web

John checks out a new site

Using an existing account and profile

Identity Providers

He finds who he knows there

Using his current address book/friends-list

Social Graph Providers

He creates some content and shares it back

His friend Joseph discovers it —and the new site

Content Aggregators

Joseph Smarr

plaxo

Conclusion:
We've still got a lot of work to do.

Why I still believe…

The Business Imperative of User Driven Data (5I)

URL: http://iiw.idcommons.net/The_Business_Imperative_of_User-Driven_Data

Convener: @dariusdunlap

Tags for the session - technology discussed/ideas considered:

- User-driven
- User-owned
- User-originated
- Loyalty
- Data
- Business
- User-collected
- Guesswork

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

Why is user-driven, owned, originated better for business?

Answer:

Less guesswork, cost-savings, accuracy, data-entry, security, less adversarial, better business intelligence

Session 6

The Trust Nexus (6A)

URL: http://iiw.idcommons.net/Trust_Nexus

Convener: Mike Duffy
Notes-taker(s): Mike Duffy

Tags for the session - technology discussed/ideas considered:

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

In the very near future digital wallets on cell phones enabled by **NFC technologies** will create a radical transformation in identity management and financial transactions processing. This transformation will provide consumers with secure identities and secure financial transactions.

The basic question is, how can trust be established in the digital age? If you and I have never met and I come to your website or place of business, how can you be confident that I am who I say that I am? **The Trust Nexus answers this basic question regarding the establishment of trust.**

We have designed an identity management system, that will eliminate the possibility of identity theft for all participants, protect consumers and financial institutions from fraudulent transactions and solve many of the systemic problems of the current Public Key Infrastructure system, especially the problems of certificate revocation lists (CRLs) and on-line status checking.

Our solution is **simple, practical and transparent to the consumer**. Consumer acceptance will be rapid and widespread. Our solution protects individual privacy and prevents the establishment of monolithic government control. The essence of our approach is very different from the "Big Brother" approach recently announced by India (http://www.timesonline.co.uk/tol/news/world/asia/article6710764.ece#cid=OTC-RSS&attr=2015164). Rather than creating a centralized directory of private information, we will create a central repository containing a collection of localized decisions which will establish an **Institutional Web of Trust**.

Compared to a decentralized web of trust which creates a web of individuals with, "the expectation that anyone receiving [a list of signatures] will trust at least one or two of the signatures", we will create a system where **trusted institutions legitimize individual identity**. Additionally, the institutional web of trust established by **The Trust Nexus** will have centralized controller processes that rely greatly on self-management and automation resulting in great efficiencies.

The Trust Nexus does not secure identity by, "making personal data harder to steal". Rather, identity is secured by self-managing logical inconsistencies within the system, resolving identity conflicts and preventing fraudulent transactions.

As **Bruce Schneier**, author and security guru, pointed out, "Proposed [identity theft] fixes tend to concentrate on the first issue--making personal data harder to steal--whereas the real problem is the second [preventing fraudulent transactions]. If we're ever going to manage the risks and effects of electronic impersonation [identity theft], we must concentrate on preventing and detecting fraudulent transactions." [Solving Identity Theft; http://www.schneier.com/essay-153.html]

In essence, there are a limited number of institutions worldwide (measured in thousands) that truly matter when it comes to legitimizing identity. Digital wallets on cell phones will enable the efficient association of unique public/private keys to a specific legal identity (legal name and legal address). If there is a non-unique association, an inconsistency arises in the system. If the association is unique and verified by one or more legitimate institutions an individual's identity is secure (as long as the private key which he/she controls is secure).

Our system also provides **the "Holy Grail" for single sign on**. A user's cell phone will be provisioned with information cards containing specified security credentials for different systems and services. Rather than logging into a directory or utilizing a federated identity service, a user will log onto his/her cell phone with a PIN and a voice authentication signature. The user will then select the appropriate information card for the specified system or service (with no need to enter another user name or password). This approach also**solves the "Keys to the Kingdom"** problem where a single sign on to a directory service opens access to all the user's systems and services.

It is a certainty **The Trust Nexus Repository** will be a collection of geographically distinct repositories. It is very likely these repositories will be run in cooperation with governmental agencies.

In the United States, **The Trust Nexus** will solve all of the problems raised by the Real ID Act without any of the problems of privacy and governmental oppression. The Department of Homeland Security has already spent hundreds of millions of dollars trying to solve the problem of reliable identity. We expect to receive significant funding from the Department of Homeland Security.

In the European Union, the user centric nature of **The Trust Nexus** resolves all the privacy concerns specified by ENISA (http://www.enisa.europa.eu/act/it/eid/eid-cards-en). A system that secures identity, maintains privacy and eliminates fraudulent financial transactions will certainly gain support from the European Union.

Considering China, "The number of mobile phone subscribers in China had amounted to 702.7 million by the end of July, more than the combined populations of the U.S. and the Eurozone, according to statistics by the local government." (http://www.tradingmarkets.com/.site/news/Stock%20News/2514497/) For their own reasons, Chinese government officials will enthusiastically adopt a workable identity management system based on cell phones; again, this will be a "natural" development based on technology and social forces.

We expect to become both the de jure and de facto **system of national identity for all nations**. We are confident that whoever controls the infrastructure for secure identity will also control the infrastructure for financial transactions.

Please visit our website (http://www.thetrustnexus.com) for technical details.

Open Identity Trust Frameworks (6B)

URL: http://iiw.idcommons.net/Open_Identity_Trust_Framework

Convener: Don Thibeau and Drummond Reed

Tags for the session - technology discussed/ideas considered:

Open identity, trust frameworks, assurance, policy, US government

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

SEE SLIDES - http://wiki.informationcard.net/files/Presentations/open-identity-trust-fmwks.ppt

Background

There's a work in process, spurred by committee of committees in U.S. Federal Government, who have been focusing in the past year on identity from the perspective of services to the citizen. Began 10 years ago with Al Gore having Government do things in hopes that industry would follow. (Didn't work.) So now it's a political effort of trying to open up government, using social networking tools (many of which helped Obama in his campaign). In March the U.S. Gov't asked Foundations to help in this, the "mother of all use cases."

Purpose

The purpose of this IIW discussion is to answer questions and get feedback on evolving work by OIDF and ICF in this effort.

Government RP Requirements

Open (not just US citizens); explicit (level of assurance (NIST LOA) requirements; Internet scale.

Foundations' Work

Since March the Foundations have worked with U.S. Government to develop government documents spelling out process.

What's next? How best to implement the profiles and trust framework.

[See slides regarding Foundations' principles of openness, key insights, IIW insights in particular.]

User agents could take advantage of a white list operated by the Open Identity Interoperability Framework, which will have a registry capability.

Metadata registry would handle both the Trust Framework (covered by MOA) and the Interoperability Framework.

We are trying to anticipate a global framework.

To be consistent with their missions, the Foundations are aiming to further adoption.

Questions/Comments:

NIST defined LOA; what about LOP – who is to define? U.S. Government's TFAP does have some protection requirements (but who these obligations are for/who can enforce them is another matter). Privacy Impact Assessment (PIA) applies to Government web sites, but how to apply this if trust framework extends to private RPs? The FTC is wanting to protect users' privacy in ways that don't put heavy burden on user.

What is meant by an "explicit trust framework"?

When you say "Internet scale", I see one point right now. Where is the list now? Is this another DNS? Is it centralized?

What is a trust profile? A trust profile is LOA and LOP as defined by policy authorities. Trust framework is the way the whole thing becomes interoperable.

What profiles? SAML, OpenID and InfoCards, but in theory whatever is approved by U.S. Gov't in that trust framework.

Kantara has developed something quite similar.

Who is the envisioned trust framework provider? Both boards have invested in this exchange with government. Now both Foundations are considering, together and separately, whether they should take on this role, and if so, how. Standalone? Joint venture? Outsourced to Kantara? Etc.

Who are the Assessors?

How does liability work?

How does this relate to ISO/ITU work? They are internationalizing NIST work for LOA. Isn't the ITU working on trust framework? That work is very complementary – it makes it easier to have profiles that lots of folks can agree to.

Identity and trust assessments are essentially independent – they need to be viewed as separate processes and separate infrastructures. Authentication useful when plugged into a process. The model is too simple and too concentrated.

Seems to make sense to get in the door by responding to U.S. Gov't requirements. Simple first step to start engaging.

There should be many sessions to drill into the parts of this.

Who's driving the process, and how do people get involved? OIDF and ICF are driving this, contact us or board members if you want to participate. It's moving at Government time, which allows people to participate in shaping it.

Why are the Foundations doing this? Not directly to influence the Government, but aware that what Government does will inevitably affect the private sector.

Wouldn't it make sense for Kantara and the Foundations to cooperate on this? Yes.

Should we take out the word "Trust" – it should be "Open Identity Exchange Framework". [Dick:] No – the certification is to allow trust.

Why would LOA1 require certification? Because the customer says so. But is that a good reason?

[Quite well attended – roughly 45 people, at capacity.]

http://wiki.informationcard.net/wiki/files/Presentations/iiw-open-identity-trust-frwks.ppt

The Hammer Stack - advanced (6C)

URL: http://iiw.idcommons.net/The_Hammer-Stack

Notes-taker(s): John Panzer

Who: Blaine, John Panzer, Breno (just one name, like Cher), Eran Hammer-Lahav, Dirk Balfanz, Will Norris, Eran Sandler, Jared Hanson, Allen Tom, ... et al

Discussion notes:

Problem: Go through open list of issues for the Hammer Stack and decide where to go. Host-meta, Webfinger, L(A)RDD.

Open Issues:

Subject of Host-Meta
EHL: XRD has a Subject element (string). XRD may be subject-less. People getting XRD must know what subject is about. Easiest way is to use a URI for the subject. So anything you can make a valid URI for. 3 proposals:

- Just give it a URI, if you want to use Subject you need to invent some way to use a URI (urn, tag, blah blah)
- Just make it a string, add an attribute that indicates the type of string (URI or ???). Moves war into attribute.
- Just allow a new extension element (in its own namespace) to use instead of Subject if Subject isn't doing it for you.

EHL: Tried hard to find a URI for Host-Meta specifically. Tried host:, dns:, a whole bunch. Only real 2 options are using a "well known URI recipe" e.g., http://host-meta.net/<domainname>. Could use SemWeb hash approach. Could mint a URN in our own namespace. Current thinking is to use "scope" instead of Subject for host-meta (next topic)

Scope of Host-Meta
Define host as ~~tuple: scheme,~~ hostname, ~~port~~. One host-meta needs to support more than one hostname. Proposal: Need to use a unique host-meta document w/unique scope for each RFC3986 domain-or-ip-address.

<hm:Host>example.com</hm:Host>

Q: How to discover public key used for signing? (Undefined by Host-Meta spec... many ways.)
Q: Harder to get wildcard certs ($300 vs. $20), could allow alternate names with Host and HostAlias? (Need a trust discussion.)

RESOLVED: Use single RFC3986 hostname w/syntax as above (namespaced <Host> element).

Host-Meta Template Vocabulary and Syntax
Current draft of URI templates being worked on, will be >1yr before published as RFC, 3-4 months before stable draft. Want to make sure host-meta's approach works with more extensive syntax for URI templates. Defined default template syntax -- can define others dependent on custom rel values. Syntax takes curly bracket {var} with {+var} meaning don't encode reserved characters. (See spec for details.)

Everything works with URIs (not IRIs) so it's been converted from an IRI to a URI using RFC 3987 before this spec kicks in.

List of vars allowed in host-meta templates: "uri", "scheme", "authority", "host", "port", "userinfo", "fragment", "path", "query"
Approaches:

- Just use "uri" alone, and let redirects handle more complicated transformations. PRO: Simple. CON: Means additional redirect to handle common cases that are pretty standard/simple string swizzling.

RECOMMENDED: Just use {uri}, {+uri}

New Approach for L(A)RDD
EHL: Originally, LRDD took building blocks of host-meta etc. to replace YADIS. Started with that, feedback from W3C TAG, others to make it more generic so it'd work for other use cases beyond OpenID. The more generic the less of a normative spec and the more recipe for a protocol. So now site-meta is know well-known, the building blocks are there to build a generic discovery spec. Thinking: LaRDD is about how to get "the LaRDD XRD" for a resource. 3 profiles: ~~(DC) Don't care priority (Are You Feeling Lucky?)~~, (HF) Host-first, then Resource (Link, etc.); (RF) Resource-first, then Host.

(Lunch. Lots of discussion back and forth about HF vs. RF and security/flexibility implications.)

Breno: Parsing HTML makes things slow and more brittle. Just using Link: header cuts out some users from embedding links.
All agree 1 LaRDD priority order is preferable to multiple (willing to compromise on favorite order to achieve this)
Blaine: If we use HostFirst, spec will be ignored.

Summary: Lots of support for resource-first, lots of good points back and forth, security folks support host-first. Interesting proposal (host first, but host-meta has optional "let resource links override if present") which may be a Grand Compromise or not. Clearly needs more discussion on list.

(At least we killed "Don't Care" and "Protocol Dependent" options.)

Rel values: Either have one rel value to discover XRD per protocol, or just one that is for L(a)RDD and then everybody uses that. Everybody is currently assuming a canonical XRD for a resource (OpenID, Webfinger, Salmon, ...).
Point: Can there be more than one signing authority? LaRDD can provide default even if some protocols add more rel values. Should LaRDD provide a default rel value ("describedby") or not?

(Lots of back and forth and levels of indirection. Break to go find a room with a whiteboard.)

Diagram: URI -> <Link>, Link:, or Host-Meta -> XRD URI

Example: URI x in Apps for Your Domain, Google is OP. Let's say use Host-Meta.
Points at XRD for specifically x, which includes links off to OpenID endpoints etc.

Example/Use Case: http://example.com/bob, outsources OP to Google, PoCo endpoint to Plaxo. How?

Concept: example.com/.well-known/host-meta contains pointers wi/rel values pointing at Google and Plaxo (EHL: Wrong architecture!)
EHL: host-meta contains just a pointer to "XRD" per resource.
host-meta contains <Link><Rel>LRDD</Rel><URLTemplate>blah blah {+url}</URLTemplate></Link>, and the template points at an XRD that itself points at Google and Plaxo.

Webfinger result document == XRD for the acct: URI. (That then points at other stuff.)
Webfinger is a special case of LRDD. May want a different profile server for Web?

Common hosting situation: Delegate profile hosting. e.g., btinternet.com points over to Google or Yahoo!. But, don't want Google or Yahoo! to be authoritative for non-acct: URIs for btinternet.com. Let's say acct: URIs are all delegated to Yahoo!.
btinternet.com hosted XRD service that does a 301 redirect over to Yahoo! if acct:, returns XRD content if not. OK DONE.

Question from Blaine that will hopefully clarify things: I get one host-meta document, and XRD, with multiple links with same rel, both fetched and each of those have links to 2 more XRD documents each. Is the XRD for the URI I'm trying to resolve the union of all these? Or something else? (A: No on the first.)

host-meta describes the HOST. uses XRD as a format.
LARDD document describes the RESOURCE. uses XRD as a format also.
Webfinger is a specialization of LARDD that handles acct: URIs ("How You Use LARDD to resolve acct: URIs")

..and the use of URI Templates in an XRD obtained for a RESOURCE is undefined at this time. (Could be defined if desired.)

Breno: We have to be able to tell domain owners to publish a signed XRD file, with templates, _once_ to handle their entire population of users (to say, for example, that the OpenID endpoint can be found over at Yahoo! or Google) -- trying to get them to dynamically sign thousands or millions of user-XRD documents

RESOLVED:

Webfinger - syntax of acct: URI
Webfinger - rel value
Generalized Discovery for URIs
Rel value for xrd-edit URL (a way to discover how to add services? go to web page?)

Identity And Cloud Computing (6D)

URL: http://iiw.idcommons.net/Identity_and_Cloud_Computing

Convener: Anil Saldhana
Notes-taker(s): Anil Saldhana

Tags for the session - technology discussed/ideas considered:

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

- General Concerns around identity Management get compounded in the Cloud.
- There is potential proliferation of Identities.
- Data and artifacts of a company can be tied to identities which is a threat during decommission of identity. It can be lost.
- SLA of Identity As A Service.
- Transfer of Passwords or Password Hashes from Local Data Centers to Cloud environments for migrated applications.
- Users resistance to change with new cloud usage.
- Identity Assurance.

Azigo Higgins – Active Selections & Similar Topics (6E)

URL: http://iiw.idcommons.net/Active_Client_iiw9

Running over 3 sessions.

Convener: Mike Jones
Notes-taker(s): Eric Sachs

Tags for the session - technology discussed/ideas considered:

OpenID, ActiveSelectors, Kantara, SAML, InformationCard, CardSpace

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

First demo: Azigo's browser-extension for OpenID identity selector
- Button on browser toolbar to initiate the identity selector
- www.openidpad.com is sample RP site
- Metatag in RP's site causes the button to be shown in the toolbar
- Uses XRDS file for more information, exposes information about RP's needs similar to InfoCard practices
- Tells selector what AX information to ask for from the IDP
- Selector then sends user to the IDP with a request for that information, and then tells it to send an unsolicited positive assertion back to the RP
- All pages on his RP site include a metatag with a reference to the XRDS file. That allows the selector to activate the toolbar button on every page
- Demo has hardcoded list of possible IDPs, but could obviously be enhanced

Second demo: Adventure Works RP
- http://openidux.dotnetopenauth.net/
- Built with a Javascript client that RP points to with their Login button
- Login button and Visit Members Area button
- Login button shows Nascar UI
- He is okay with a few buttons and OpenID button for long-tail, and tells people to use Google to create a new account if they don't have an account with existing buttons or an OpenID
- All buttons use the popup
- The site remembers the last IDPs you visited, and put those buttons earlier
- The site also does background checkid_immediates to all IDPs who have a button and shows a green checkbox for the ones where the user is logged in
- If the user clicks the OpenID button, then it ajax shows a box below to capture the URL and it supports inames as well. After discovery is done, it ajax shows a login button that lets the user choose which of the multiple IDPs they may have delegated to.
- Provides RP account management options to add multiple OpenIDs assocated with same account

Demo: Google's CDS that does NOT use a browser-extension
- Slides at http://docs.google.com/present/view?skipauth=true&id=ajkhp5hpp3tt_67dvg24phj
- Described at https://sites.google.com/site/oauthgoog/UXFedLogin/central-discovery-service

Kantara slides of their UX initiative
- Described recent group they started to pull together to brainstorm on UX goals without considering the protocol
- Showed example of the challenge NIH has the with the large number of IDPs it trusts in multiple classes such as schools, consumer IDPs, etc.
- Gave example of providing a search box over those IDPs
- Group noted that IDPs want to control how authentication happens, probably should not be in the selector

Part 2: 1:30pm in room E
Dr. Enrie from Apple attempting to summarize goals
Notes at http://iiw.idcommons.net/Active_Client_iiw9#Client_Lifecycle

NOTES PUT on WIKI:

At IIW9 several vendors (starting with Microsoft) demonstrated prototypes for an "active client" that would manage internet identities on behalf of the user. Due to broad interest in such capabilities, several of us are getting together at IIW to work on a common description of such '''Active Identity Clients''' (AICs) http://www.identityblog.com/?p=1070 with the goal of driving unified requirements for the necessary infrastructure.

Agenda
For Tuesday, November 4th at IIW
1. Scope: What will we focus on? [The "Infrastructure to support user experience"]
2. Problem: How much complexity will we tackle *now*?
    1) Which protocols: OpenID as it is today, Minimal changes
    2) Perspective: User-centric, implications for RP and IdP
    3) NAME: Active Identity Client
3. Goal: What do we want to achieve (now or later)
    1) Kinds of information that would be useful
    2) Propose explicit syntax
4. Dataflow: What are the key components, and how do they relate?
5. Issues: What are the problems therein that need to be solved?
6. Proposals: Idas for resolving those problems

Action Items

Markup
object tag or replacement
* Chris Messina (?)

Callback Model

RP Discovery/Delegation
cf. i-Frame aliasing

Claim Selection
In the IdP, versus the selector (as in InfoCard)

IdP Metadata
names and logos; in process
* Mike Jones

Validation / Whitelist
* Ernest Prabhakar

Aligning Popup UX with Selector UX
* Allen Tom
* Ariel Gordon
* Paul Trevithek

Participants / Documents

* Aanchal Gupta (@aanchalb), Yahoo
* Andrew Arnott (@aarnott), Microsoft
* Ariel Gordon (@askariel), Microsoft
* Axel Nennker (@AxelNennker)
* Bharath Kumar (@Bharath7923), Amazon
* RL "Bob" Morgan (@rlbob), U Washington
* Chris Messina (@ChrisMessina), OpenID
* Dan Mills (@thunder), Mozilla
* Dirk Balfanz (@Balfanz), Google
* Eric Sachs, Google
* Ernest Prabhakar (@DrErnie), Apple: [http://ihack.us/2009/11/02/chamberlain-a-user-serving-model-for-identity-management/ Chamberlain: A User-Serving Model for Identity Management]
* Gregg Gracheck (@GreggGracheck), Acxiom
* Joseph Boyle (@JosephBoyle)
* John Bachir (@JohnJoseph), Ganxy
* Markus Sabadello, Azigo
* Mike Ozburn, BAH
* Mike Hanson (@michaelrhanson), Mozilla
* Mike Jones (@selfissued), Microsoft: [http://self-issued.info/presentations/An_Experimental_Active_Client_for_OpenID.pdf An Experimental Active Client for OpenID]
* Oren Melzer
* Paul Trevithick, Kantara [http://www.incontextblog.com/wp-content/uploads/2009/11/ULX-at-OpenID-Summit-Nov-2-2009.pdf Kantara Universal Login Experience] (ULX)
* Peter Capca (@pcaperc), IEEE
* Ragavan Srinivasan (@ragavan), Mozilla: [https://wiki.mozilla.org/Labs/Weave/Identity/Account_Manager Labs/Weave/Identity/Account Manager]
* Rajeev Angal, Sun
* Robert Guthrie (@GuthrieRobert)
* Ronak Shah (@RonakS), Apple
* Sam Wren (@TelegramSam), Kyneta
* Sharif Youssef, Acxiom
* Tom Carroll (@TJ_Carroll), Azigo
* Ushasree Kode (@ushakode), Yahoo

Problem Statement

The key tension we want to address is the paradox that identity management is both a) necessary, and yet b) too complicated for typical users. We want to propose an user-centric solution that is meaningful to RPs and IdPs.

We believe the best way to solve this problem by enabling an '''Active Identity Client''', which manages identities on behalf of the user (though obviously we'd love to enable passive clients as well).

The goal of this discussion is NOT to design a specific Client, but to define the minimal infrastructure necessary to optimally "support" that class of client.

Client Description

This proposal should enable a wide range of Clients that:
* Support OpenID and optionally other identity protocols (e.g., InfoCard)
* Run on different OSes (i.e., Windows, Mac, Linux)
* Work with modern smartphones (e.g., iPhone, Android)
* Run in different contexts (browser, cloud, plug-in, desktop, etc.)

Output

The ultimate goal of this discussion is a document that would propose best practices for supporting AICs, including extensions to existing standards (in partnership with the relevant working groups).

Short terms goals may include:
* forming/joining an ongoing mailing list/working group
* encouraging prototype AICs
* building supporting libraries
* identifying areas for future research
* documenting areas of agreement
* putative syntaxes

Client Dataflow

The following are the steps that a typical AIC would likely require:

1. Detection: website Requesting Party (RP) indicates it supports login via OpenID
    1.Requires them to do something - but only one thing, and once
2. Initialization: the AIC launches with knowledge of who the user is
3. Interception: the AIC binds to the websites login so it receives appropriate clicks
4. Activation: the user initiates/accepts the OpenID login process
5. Canonicalization: determining the scope of the login for that RP
6. Discovery: the AIC queries the id attributes requested by the RP
7. Identification: the AIC determines any IdP's pre-selected by the user
8. Decision: the user chooses or enters an IdP
9. Validation: the AIC checks those IdPs against the user's preferences and a security whitelist (blacklist?)
10. Display: viable IdPs are displayed for the user to select (or, optionally, enter their own new one)
11. Authentication: the OpenID (or potentially other) protocol is used to authenticate the user via that IdP
12. Memoization: successful logins are recorded against that website/IdP pair for future reuse

Requirements

To enable that lifecycle, we propose the following supporting infrastructure:

Detection and HTML Markup

While many of us would love Relying Parties to hard-code support for our favored AIC, the reality is that we need a level playing field to encourage both adoption and innovation. This might imply some kind of standard "meta-selector" that would detect the user's preferred (installed?) AIC and auto-launch it on compatible websites.

MS AIC Today (Plaxo)
* RP places explicit object tag in the page with parameters it needs
** protocol tag (i.e., openid): one or space-delimeted
** tokenType (needed by other protocols)
** issuer - suggested providers (space-delimited) [seen if the users has none pre-existing]
*** OpenID identifiers (shortest form)
** issuerExclusive (boolean)
** OpenID parameters inside InfoCard syntax [inline later?]
*** returnTo URL [currently uses browser, be better to do out-of-band]
*** realm [canonical name for always-allow]
*** attributes (required, optional) comma-separated
*** policy_url:
* specifies MIME-type which invokes a handler
** x-informationcard used for prototype as it autoregisters with IE
* explicitly attach JavaScript to login button/anchor
** or embed the object tag inside the form (auto-invoked on submission)
** possible to do with a relTag + JavaScript bindings?
* popup handler when invoked by user
** if click on a specific providers link, should be able to pre-select that provider in selector

Questions

* Does the page invoke the AIC (<object>), or is the AIC always present and scanning the page?
** Alternative is to do just XRDS
** The former is likely to be the most common case, as it allows lower latency
* What is the optimal way for the RP to provide metadata
** Need a simple profile that captures "most" of the cases
* Can we define a new tag that gets rewritten as <object> as necessary
* Is there a back-channel for reverse discovery [may be later, for OpenID-OAuth]

Action Items

* Define the custom tag with specific attributes
* Define a MIME type
* Define fallback behavior (e.g., <object> tag)

Ulimately (as with AJAX) the goal would be to define something suitably generic that it could eventually supported directly by multiple browsers, all of which would interoperate with multiple AICs.

Aside: Alternate Credentials

It would be wonderful if this system could easily be extended -- by others -- to support alternate types of authentication besides OpenID

Relying Party Canonicalization

One of the biggest challenges in reusing logins is determining exactly "whom" we are authenticating against *this* time. To that end, the Relying Party needs to provide the "canonical" name used to identity itself, in order to prevent unnecessary logins on one hand and phishing on the other.

There are several potential ways to accomplish this:
* HTML tags (attribute on Detection, meta tags on the HTML page)
* ".well_known" URIs on that site
* Reverse Discovery on the RP

Hopefully we can agree on a common solution that fits well with existing OpenID workflows

Aside: RP-specified Providers

Should the RP be allowed/encouraged to say which providers they support?

Aside: Additional RP Metadata

In many cases, it could be useful to provide "hints" to the AIC about what "kind" of website this is, to enable heuristics about which of various identities to prefer. For example, many users like to use a separate identity for financial websites. While it is beyond our scope to enumerate all possible such usages, we should prefer solutions that enable the RP to easily provide such metadata.

Identity Provider Metadata

For purposes of display and reuse, the IdP Response should include the following metadata in the XRD(S) response:

* canonical name for the Identity Provider
* icon tag with metadata about sizes (some recommended sizes, intelligent rescaling)
* human-readable name

The canonical name would most naturally be an OpenID Endpoint.
The other iterms in the XRD(S) would be localizable based on the HTTP header

Action Items

* Discussions with Allen Tom from Yahoo! and Luke Shepherd from Facebook
* In-process with OpenID UX committee

Validation Services

For security reasons it is highly desirable to '''not''' let the Relying Party easily specify arbitrary possible IdPs, since it seems likely that eventually there will be IdP "phishers" that mimic well-known sites. On the other hand, it should be possible for users to create their own IdPs (perhaps with feedback about what ones will be accepted).

The optimal model is (for better or worse) is probably one modeled on how root certificates are handled by browsers today (and may in fact leverage that infrastructure). There should be a reasonable set of well-known WhiteList providers that are recognized by default, and authorized users should have the option of explicitly trusting additional sites.

Whether and how AICs represent untrusted IdPs is up to the implementor, though it may be advisable to propose "best practices" thereof.

Questions

* Who is the authority
** OpenID
* How is it published/advertised
**

Implemented a List of Whitelists

* Each AIC has a 'root' list of whitelists (which may refer to other whitelists)
** e.g., Google, Yahoo!, Windows Live, AOL, Orange, MySpace, Facebook

* XRDs can specify which whitelist they belong to
* Users can manually add their own (or remove ones they dislike)

Implemented via Certificates

* Using EV certs as the starting point for whitelists

Rely on AIC to do it their own way

* Use standard anti-phishing or browser blacklists

The Small Business Web: Issues of Building a "Whole Product Solution" (6G)

URL: http://iiw.idcommons.net/The_Small_Business_Web

Convener: Sunir Shah
Notes-taker(s): Sunir Shah

Tags for the session - technology discussed/ideas considered:

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

I described The Small Business Web (http://www.thesmallbusinessweb.com), and our goals of increasing the overall market for SaaS amongst Small Businesses by building a "whole product solution" through integrations. FreshBooks is a founding and leading member of this group.

We then talked about how the current market for small business web apps is undergoing a major push by Very Big Companies to get aligned, all due to App Stores. We discussed how it's in all our best interest to push for Open Web standards as the basis of single sign on, account provisioning, embedded interfaces, licensing, billing, and reporting in order to build the largest economy. Failure to adopt Open Web standards will lead to the monopolization of identity by big vendors who will then take a huge cut of all revenue on the Internet. Put simply, whoever owns the business email address, owns the credit card, and can take a sizable toll unless there is open competition.

We discussed the ideal workflow of applications fitting the user's workflow (through embedding; e.g. OpenSocial, Disqus) rather than users being dragged towards applications (through log ins).

We then discussed the implications for Amazon in terms growing of its affiliate market by making Amazon an IDP through OpenID and extending OneClick (tm)'s reach onto its affiliates' websites.

VRM – 4th Party *Provider* Brain Storm *(6I)*

URL: http://iiw.idcommons.net/4th_Party_Provider_Brainstorm
Video URL:

Convener: Julian Gay
Notes-taker(s): Judy Clark, Julian Gay, Doc Searls

Tags for the session - technology discussed/ideas considered:

- 4th Party
- Agency
- Advocate
- Customer
- Consumer
- Representation

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

4th Party definition = product or service that helps individual intentionally engage with other parties (e.g. Businesses) Has a ethical obligation to act on behalf of the user/ customer (agent or proxy) (Aggregators not necessarily 4th party – no ethical obligation)

Pure 4th party = customer pays

Enterprise benefits in becoming 4th party provider: loyalty increases, long term relationships increases and churn (?) decreases

(written notes transcribed by Heidi)

Session 7

Adoption OpenID Contract Exchange CX Payment (7A)

URL: http://iiw.idcommons.net/OpenID_Contract_Exchange_and_Japan_Update

Convener: Nat Sakimura
Notes-taker(s): =nat

Tags for the session - technology discussed/ideas considered:

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

Shared the progress in Japan. OIDF-J now has 54 member companies. It has become the center of gravity for this kind of work because of the membership composition. People feel that the consensus built here will be de-facto standard profile in Japan and needs to get involved. How it was achieved?

OIDF-J approached three sengmenst in pararel: Consumer, Business&Tech Community, Government.

For Consumer, we kept making news so that magazines and news papers keep producing stories.

For Business & Tech communities, we did monthly seminars, which proved to be extremely popular. Tech event has always been putting emphasis on security, so that “OpenID cannot be secure” kind of argument has disappeared. For Business Seminars, each member companies are revealing their business plans around OpenID and stimulating each other.

In addition, we did over 100 in person customer visit to educate them. Also, we did so many brainstorm sessions with them so that they can come up with new business ideas using OpenID.
For Government, we have been doing educational session in various goverment agencies and committees, that now we are involved in guidelines(*1) creations and pilot studies.

Has kicked off bunch of SIGs, most notably, Payment SIG, which is discussing on creating a standard profile for making payment over OpenID based on Artifact Binding Proposal + AX Req/Res Proposal + Contract Format (mutually digitally signed legal document for non repudiation.)

(*1) Risk Guidelines, Authentication Guidline, E-Signature Guideline, etc.

Info Cards on Phones are Really Cool (7B)

URL: http://iiw.idcommons.net/Identity_and_iPhone

Notes-taker(s): Bo

Discussion notes:

- Phone – Extremely useful and powerful Identifier.
- Certainly level 2 up to level 3 with another identifier.
- Because there network identifier and obtainable privacy is really important

(written notes transcribed by Heidi)

Open ID Session – Management Best Practices (7C)

URL: http://iiw.idcommons.net/OpenID_Session_Management_Best_Practices

Convener: Johannes Ernst
Notes-taker(s): Breno de Medeiros

Tags for the session - technology discussed/ideas considered:

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

- How to switch users at the RP? Need to remember to switch at the OP.
- Signed in to OP only to use RP. Signed-off RP, forget to sign-off at the OP.
- Single sign-off from everything by default may be too aggressive or not fit the desired user experience.
- Client-side indicator of login status (identity selector)
- RP initiated/OP initiated?
- Single sign-off has high complexity.
- PAPE support for approval prompt (as opposed to password entry)?

We typically focus all of our attention on around signing in, but ignore what happens after that. In this session, we discussed user expectations and confusion and ways of remedying session expiration, session revalidation, partial or single log-out etc.

Results are on the OpenID wiki at:

http://wiki.openid.net/Session-Management

Is Assurance Real? (7G)

URL: http://iiw.idcommons.net/Is_Assurance_Real%3F

Convener: Bob Morgan
Notes-taker(s): Michael Schwartz

Tags for the session - technology discussed/ideas considered:

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

Identity Assurance Frameworks:

OMBO4-04
E-Auth - CAF
NIST-800-83
TFPAP
ISAP
Kantara IAF
InCommon IAF

Challenges for universities to achieve level 2:

- Need to evaluate if employees' and students' has been properly validated / verified.

- Possibility that an unknown university service collects creds in the clear. Nothing stops someone from publishing an unencrypted web form that binds against the university LDAPS or Kerberos system.

- Cost: assurance = money. Fundamental problem: IDP bears the cost, but the RP gets the benefit.

Open ID Providers Office Hours (7H)

URL: http://iiw.idcommons.net/OpenID_Provider_Office_Hours

Convener: Yahoo – Google – AOL etc…
Notes-taker(s):

Tags for the session - technology discussed/ideas considered:

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

1. RP's are interested in more AX data – AMEN!
2. Shamelist of OP features on Openid.net
3. Reduce the number of clicks for Open ID flow

Session 8

Salmon Magic Security Pixie Dust (8E)

URL: http://iiw.idcommons.net/Salmon_Pixie_Dust

Convener: John Panzer
Notes-taker(s): Brian

Tags for the session - technology discussed/ideas considered:

salmon, authentication, aggregators, spam, abuse, identity

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

Start by visiting salmon-protocol.org for background:

Problem statement for "identifier correlation problem":

- sources need to identify both aggregators and users for abuse prevention. It should be hard for bot-nets to bring up new aggregators with a good reputation.
- it should be possible for userX@aggregator-one and userX@aggregator-two to show up as the same user (userX, or open id for userX) at the source.

Backing up, new problem statement: how does aggregator authenticate to source?

Option 1: client-side SSL certificates with PKI
Option 2: two-legged OAuth with public key discovery

Example: new aggregator says "Hi, I'm aggregator.com", with certificate from Verisign

Alternate proposal:
new aggregator says "Hi, I'm new here, please give me a fresh id"
source assigns random id
new aggregator begins using random id

Objection #1: tough to build public reputation based on this
Objection #2: difficult to maintain reputation after key compromise

Possible solution for OAuth public key discovery is being discussed in OAuth + PKI discussion tomorrow morning.

What happens if there is a single bad user at the aggregator?
- can the source blacklist the bad user, rather than the aggregator?
- can the source send feedback to the aggregator about the bad user?

Distributed negative reputation:

- if multiple sources publish information about bad actors, then we have a distributed negative reputation system that can improve spam detection everywhere.

Decision: if we don't need to solve the identifier correlation problem, we can avoid salmon signatures entirely.

- aggregators are trusted to assert identifiers within their domain
- we build reputation based on aggregators
- we lose the ability for people downstream to verify the comment back to the aggregator

Scenario:

userX publishes on plaxo
userY adds comment on blogger
blogger pushes comment to plaxo
plaxo adds comment to feed
friendfeed sees comment from userY@blogger

Use case: how can we let a user see a trace of all comments they've made on all aggregators?

e.g john comments from Twitter, and john comments from Blogger. Later he can edit/delete both comments from Reader.

This seems to bring us back to the identity correlation problem.

Proposal: aggregators gets OAuth capability pointing to a "comment server". Comment server then posts on user's behalf to source. Comment server can also edit/delete comments.

Again, this is much easier if we give up the ability to delete comments from Reader. If a comment is made on aggregator X, that comment can only be deleted on aggregator X.

Note this doesn't necessarily hurt usability. If comments point back to their source, then you can just click a link on the comment, get back to aggregator X, and delete the comment from there.

Q: How can aggregators send public global identifiers (e.g e-mail, or OpenID blog URL) rather than local identifiers?
A: aggregators just assert the public global identifier. It's up to sources to trust or distrust aggregators that do that.

If an aggregator continuously posts bad public global identifiers, then they will be blacklisted. In the future, they will do a better job of validating global identifier.

This is similar to how mail relays work. There are services that track bad mail relays and sell that data to others.
We filter 90+% of mail spam. We have gotten good at fighting spam in this way. We can keep doing it.

Strong Authentication for OpenID/InfoCard (8G)

URL: http://iiw.idcommons.net/Strong_AuthN

Convener: Michael Sprague
Notes-taker(s): Michael Sprague

Tags for the session - technology discussed/ideas considered:

Strong Authentication / OpenID / SASS

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

The discussion presented the existence of OP's that provided a higher level of authentication than simple password login. This includes services that use the Trusted Platform Module, SMS challenge, key fob's and others.

The question was posed whether there is value in this… are there business cases for it.

First there was the concern that based on this morning's openid security discussion, adding strong authentication to a protocol with so many holes has significantly diminished value.

Google provided insight on systems using SAML federation between a company's Google apps environment and their (the company's) authentication server. This offers a way for a company to bring their mail environment under corporate authentication. It was noted, however, that when using SAML for federation to external sites, best practice calls for the association cert to be rotated, which rarely happens. OpenID could offer a better approach.

This presented on opportunity for market demand for relying parties by introducing a system that better enables a company to manage their employee relationships to external sites.

Google pointed out that the cost of recovery for compromised accounts represented a significant issue for them as well as others such as AOL, Yahoo and Microsoft. Even with the holes in OpenID, it is considerably better than the status quo. Simple enhancement beyond username/password helps limit the problem.

Google also discussed that a big issue with moving to alternative sign-in methods beyond username password is the legacy of desktop apps that did not anticipate any other identification method. This needs to change first but will take significant time.

Some of the discussion focussed on whether strong authentication should happen at the relying party, rather than the id provider. However the potential cases for this were deemed to be rare.

The group was asked whether there would be value to having a single identity come with different levels of assurance, so that a relying party could only enable sensitive features (bank transfers for example), based on sign-in profile. The concensus was that it's hard enough to get relying parties, that to introduce a level of complexity was not a good idea.

In all though, the whole ecosystem needs to grow and mature for the benefit of strong authentication to kick in... but it's coming.

Schema Mapping – Using the Persona Data Model (8I)

URL: http://iiw.idcommons.net/Schema_Mapping_Using_Personal_Data_Madel
Video URL:

Convener: Paul Trevithick
Notes-taker(s): Joe Andrieu

Tags for the session - technology discussed/ideas considered:
Attributes, claims, schema mapping, semantics, persona

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

Used to think that we could figure out a common schema. But realized that is too hard. Human nature is such that we want the power to mint the names and titles of the terms we use in /our/ systems.

So what Paul has been working on an open source schema for information about human beings: first name, etc... If you make a rich complex schema, it ends up being complex. It's easy to do the dumb things and keep it simple. Hard to do anything that captures the richness of reality without having significant complexity. This schema mixes and matches from tons of places and is intended to capture EVERYTHING, even if no one uses it directly. But you can build schema mapping in & out of this schema for whatever the input and output need to be.
When working on a schema, it is typically done with a specific purpose in mind, which leads to many different schema. So, let's embrace that and have a vehicle for mapping in and out of each of these.

Question: Doesn't that bring up issues about language discovery?
RP wants a claim "X". It asks the IdP. "X" must be golabally unique. If the IdP doesn't have "X", it can try to find a transformation path to product "X" from the data it does have available.
Note that a given transformation could take multiple steps from multiple different transformation rules. And if we have a big, rich central transformation ruleset (Y), then for most transformations, all you need is to be able to map in & map out.
Also, the more granular the base Y, the easier it is to scope in and out... there are more possible transformations the more granular data.

It's faster for me to figure out how to do it on my own rather than to go learn some other ontology. This fuels the cacphony.
(What are the rules? Inference rules?)
Persona?
Not clear what that means? Is it the role a person is in? Perhaps thats just a claim?
Uses some RDF and leverages interesting SPARQL stuff, but in the end, it doesn't need complicated SemWeb tech.

Session 9

OpenID v.next [aka v.Awesome] (9A)

URL: http://iiw.idcommons.net/OpenID_v._Next

Convener: David Recordon, Dick Hardt
Notes-taker: John Panzer

Tags for the session - technology discussed/ideas considered:

openid, identity, OAuth, AX, UX, PAPE, Discovery, Attribute Exchange, Security

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

Agenda:

- OAuth Hybrid
- Attribute Exchange
- User Experience
- PAPE

- Discovery
  - XRI?
  - Email addresses
- User Experience
  - Pop-up
  - Language
  - Active client (non-browser)
- OAuth (see non-browser client above)
- Security

Discussion about agenda:

Want to figure out what we can do in the next ~6months.

Should LOA above level 1 be on agenda? How important is it to get to level 2? Goal is to understand what it would mean to get to level 2 vs. doing other things. If can get to L2,3 without a lot of complexity or losing important attributes of OpenID, then could be worthwhile.

Q: Does anyone know of any actual known attacks against OpenID in the wild? (Yes, someone claims to have broken any number of RPs)

Yesterday, discussed various security threats that we understand (have been used to attack other protocols) and created a list of threats that are significant against OpenID today. Would be nice if we hit most if not all of them when doing v.next. If hit LOA2 in the process that's great, but most usage of OpenID are consumer web apps and we want to make our current users secure. Solutions are things that we know we can do or are not much more of a step from today.

Proposed sub-teams for next year:

- Security
- API / Data
- Usability

DISCOVERY

Email addresses as a form of identifier. Query: What about other types of identifiers? Can we make anything that resolves to an OpenID be usable? See Webfinger mailing list. Rough consensus that we want to look at email like identifiers, some discussion around usability etc.

Dick tries to take a poll: Do we want to narrow down universe of identifiers or widen? Discussion about usability of having different RPs accepting different types of identifiers. (Need to build persistent, reassignable identifier into discovery.) Ultimately want we want, when a user goes to a site, their OpenID will work no matter what. (=drummond: XRI 3 will be in the form of a URL.) Breno: We don't know yet enough about discovery. Resolved: We don't know enough to make that decision.

=drummond: Set goal of understanding implications if we do or don't address problem. Everyone agrees we need to understand the problem this year (not everyone agrees we need to solve it).

User Experience: Yes we agree we need to improve it. (International requirements may drive UX as well - jurisdiction, etc. is important, Yahoo! has an additional parameter in addition to language to determine jurisdiction.) UX to be merged into v.next (which also means finalizing the UX extension.)

Active Client: Should we support them? 1. Outside a browser; 2. OpenID enabled browsers -- client code that is OpenID aware. Advertising that OpenID is available (XRD discovery)? Is there consensus to give a recommendation to browser vendors on how to integrate with OpenID.

OAuth and OAuth like things: Should we add support for rich clients to authenticate -> API for rich client to call. (Note: Really hard for OAuth desktop app to figure out what happened in the browser.) (Yes.)

JSmarr: Speaking of making rich clients operate with OpenID: 'Direct' auth? (Heresy! Burn the witch!)

Attributes: Proposal from Mike that there's a standard set of attributes and a standard way of communicating them. (Should they be URLs? Or shorter?) Consensus that we need to have attributes that are widely available and with consistent semantics and syntax. (RESOLVED.)

Single Signout: No consensus that we have to do this in next 6 months.

(Call this v.6months?)

Question: Backwards Compatibility? (Or transition period? How much software is in standard libraries that can be revv'd vs. custom deployments?) 2 questions: Can implementations make their own decisions about compatibility modes, are are they forced to be backwards compatible? Can they re-use the same endpoints (do the protocols collide)? Note: If we use the Hammer Stack for discovery, then the "new" discovery will follow a different path in any case.

JSmarr: Discovery of active sessions on OP; is there some way to do this (UX/ Discovery)

Mobile Support/Alternative Devices: Want to make sure protocol works well in mobile environment (mobile web browsers?) Esp. dealing with long, long URLs. (2K limit, etc.) Request and return URLs both problematic. Devices that don't have browsers (will there be any of those in 2011?)

Security: Top 3 attacks we want to mitigate? (See above, was separate session on that.)

Votes: "Who is going to work on what" (as opposed to "what should be worked on"):

Votes (official ones to be provided by David & Dick):

Discovery: 10
UX: 10
OAuth hybrid/Rich clients: 8
Security: 8
Attributes: 9
Mobile: 8

Information Sharing (Kantara Work Group) (9E)

URL: http://iiw.idcommons.net/Information_Sharing

Convener: Joe Andrieu
Notes-taker(s): Joe Andrieu

Tags for the session - technology discussed/ideas considered:

Information Sharing, Kantara, VRM, permissions, user-driven data, user control

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

AGENDA/OUTLINE

1) Information Sharing
  a) Work coming out of the Project VRM Standards Committee
  b) User Driven & Volunteered Personal Information
2) Kantara Initiative
  a) Customer-Supplier Engagement Model
    i) Building on Iain's 10 steps in the customer relationship
    ii) http://kantarainitiative.org/confluence/display/infosharing/Scenario+-+Buying+a+Car
  b) Information Sharing Agreement
    i) Standard Agreement for the use of information shared by the individual
    ii) Current work (and its introduction)
    iii) Bi-weekly call to continue that work (internally)
    iv) Once we have a stable version, reach out to other groups
      (1) legal review
      (2) start with internal Kantara briefings & conversation
      (3) open to external groups on a discrete basis
      (4) publish work group report
      (5) open to public commentary
      (6) finalize draft
      (7) legal review
      (8) present for Kantara publication
  c) Consumer Research
    i) Consumer Barriers to VRM adoption
    ii) Literature Review
      (1) Underway
      (2) Half funded by Kantara, Half by ISOC
    iii) Proposal for ~$200,000-$350,000 conjoint analysis study
  d) White Paper

Notes from meeting

- Kantara helping to establish framework for VRM
    - Trust
    - Identity
- Discussed auto industry vrm scenario
- Discussed frameworks, related projects (CMI)
- Recognized significant paradigm shifts for customers and enterprises

- Data flow exists between search & targetting
- How do I manage the incoming data?
- Old school
    - Awareness, attitudes, usage pattern
    - create awareness:
    - change attitudes
    - generate usage
- new school:
    - needs
    - search
    - retention

- watson & brohman/
- Data completeness (ACM has a recent article. 2001 is first article)
- CMI (customer managed interactions)

- gaps within companies, between companies & industry, between customers & companies

- six or seven papers in this field

- should it all just be free
- but information has asset value

- Right Side Up

Data Traceability in the Cloud (9F)

URL: http://iiw.idcommons.net/Data_Traceability_in_the_cloud

Convener: Steve Holcombe, Pardalis, Inc.
Notes-taker(s): Scott David of K&L, Gates

Tags for the session - technology discussed/ideas considered:

Supply chain, Fragmented, Complex, Federated, Products, Trust, "4th Party", mandate, industry, government, health, safety, liability, traceability

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

Case study examination of USDA's declaration of mandating animal identification to livestock supply chains following the 2003 mad cow case, early implementation of a market driven (i.e., profit driven) data identity and traceability system by Pardalis, Inc. for small calf producers, and the subsequent collapse of the marketplace because of USDA's failure in 2006 to introduce their sought-for mandate.

Lack of products and services provided to fragmented beginnings of supply chains due to lack of data (e.g., no "life insurance" for diseased livestock of small farmers because not enough data upon which to do risk analysis); liability concerns as a driver regarding genetically modified crops and/or allergens; and lost opportunities for selling ag products overseas due to lack of authenticated data traceability.

Correlation of cattle and ag commodities to other product supply chains (lead painted toys, melanine laden food), and leveraging the 'identity' movement into commercial supply chains.

Misc.: Further discussed the common need for trusted entities along complex supply chains; possible use of info cards (including conditional access to encrypted, individual data elements); and activity streams.

Pseudonyms Sock Puppets – spectrum of ID Entity (9L)

URL: http://iiw.idcommons.net/Spectrum_of_Identity

Convener: Rick Smith/Kailya
Notes-taker(s): Rick Smith, Jeff Vander Clute

Tags for the session - technology discussed/ideas considered:

Sock puppets, anonyminity, pseudonymity, verified identity, socially verified identity, reputation, social versus technical mechanisms, boundaries, privacy, expunging records, under age

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

Kaliya proposes a range of four types of identities

A. Anonymity –
B. Pseudyminity – Gamers, visitors to govt sites that aren't performing actions on personal legal things
    a. Single site pseudonymity
    b. "Linked" pseudonymity – using a persona in multiple locations
C. Socially verified – Facebook, twitter
D. Verified – tied to one person

US govt is looking at OpenID and such because there are sites that do NOT want to explicitly identify their users, but wants to provide a customized experience, which in turn relies on an authenticated identity.

"Limited liability persona" – spin off personas that are linked back to you but don't really pass liability back to you.

Two separate worlds of identity – I buy something on craigslist, I want to see flickr photos, but I don't need to see the birth certificate.

"There are lots of people who push for assurance in identity want to push for the "verified" range of identity, and that somehow that makes it all work right. But problems persis

Some people say that ideal identity is tied heavily to the physical person.

Credit card companies used to care about identity. Today they really don't care that much. Credit card companies find that it's not worthwhile to focus on it. Instead they only care about transaction integrity.

Sites are one of the boundaries people create – each site provides a boundary within which people create identities. These may or may not relate to identities on other sites.

Google is a terrific platform for traffic analysis – people would ego-surf and find peoples' blogs who talk about them, rag about them, and produce unexpected and undesired results.

Identity as aggregated reputation - your personal events get posted on the Internet, some disappear and others stay on line forever.

A problem today is that we have no process to expunge information about people before they were of legal age. Your youthful indiscretions may follow you and you might not have a way to recover.

France does not have Yahoo groups. Two laws: hosting child porn is illegal, and if the word 'private' appears in a site, then the host company is legally forbidden from looking at the group's contents. The two interact in a bad way: the sites can't host ANY groups because there's no way for them to police possibly illegal groups. Ditto for Nazi things.

There isn't really a "Real" identity, it's lots of things. It's a set of transactions and doings that have the same origin in agency. "On your behalf"

"How do I know that I'm chatting with Joe?" There's no real way to know. At most you might be able to know that you're chatting with Joe's agent.

You have this bundle of things that are your agents (user identities) and bundle of transactions with others, which becomes your reputation.

Yahoo Identities are the toilet paper of the Internet – you use it once and then throw it away.

People and social structures tend to protect their kids effectively. It's almost impossible to implement these things technically. Yahoo was trying to establish mechanisms for kids to interact with the site with parents' permission. The parents' actions tended to produce the right result and the mechanized solutions tended to get complicated and counterproductive.

More Notes from spectrum of identity session

Subjective: The importance of having multiple personas.

Laws of Identity - should be required reading
Limited Liability Personal

Kaliya's proposed spectrum, for the purposes of stimulating a dialogue:
1. Anonymity - used once

2. Pseudonymity - association is opaque (gamer world, handle reality); gov't LOA 1. We don't want to know who you are and we're not going to let you tell us. Types:
  - directed pseudonymity, only works on 1 site, directed OpenId, can't use same pseudonym on multiple sites
  - linked pseudonymity, portable to multiple websites, regular OpenId
3. Socially verified - Facebook (real), Twitter (persona)
4. Verified
5. Verified anonymity: e.g. +18 but NPI

IIW long ago stopped debating the philosophical concept of identity and instead chose to focus on Internet identifiers and how they relate to people.

No one wants an identity, but wants what an identity enables.

Like the Heisenberg Uncertainty Principle: The more precisely you know an identity, the less that person is willing to do, so the system loses important forms of value / interactions. Balancing level of identity on the proposed spectrum against desired forms of interaction.

Twitter is a much easier context to understand because everything's public (unless you protect your tweets) except for DMs.

Tests to determine limits of identity, e.g. Does it continue after you die?

Two different worldviews:
1. Verify using social means, get the vibe (e.g. Flickr photos)
2. Verify using birth certificates

Boo to "Identity assurance". All forms of identification can be gamed when large transactions are in play. So credit companies care about transaction validity not the person.

Shifting boundaries in public-private conversations... not reflected by the technology.

Sites are boundaries that people create.
"The politician and the chess player." "Bill Gates on Quake."
Separation today formed by separate sites, but most people don't realize that pseudonyms are public.
Problem: Not having visibility of the boundaries.

The brain is built to forget things over time. But the Internet is a permanent archive.

Internet identity as aggregated reputation. The history of all you've done online defines your identity.

We don't even have a discussion going about how to expunge. Crimes committed by minors can be expunged from the record, but not online.

Current evil: Graph analysis that collapses identities, which get sold to marketers.

In France there is no Yahoo Groups because of 2 laws: 1) hosting child porn is illegal (of course) and 2) if private appears on the site anywhere by definition the company is not allowed to look at the content for any purpose. Bad interaction between the two laws. Can't monitor for child porn for the purposes of removal.

Cliff: Flaw is to think about identity as a thing. You have lots of identities. The flaw in the frame is that id is not an entity but a set of transactions, actions, and doings that have the same origin in agency (you or your agents that work for you on your behalf). => identity as history. Also things people say *about* you.

Identity = capabilities + history. Don't just focus on the capability bundles.

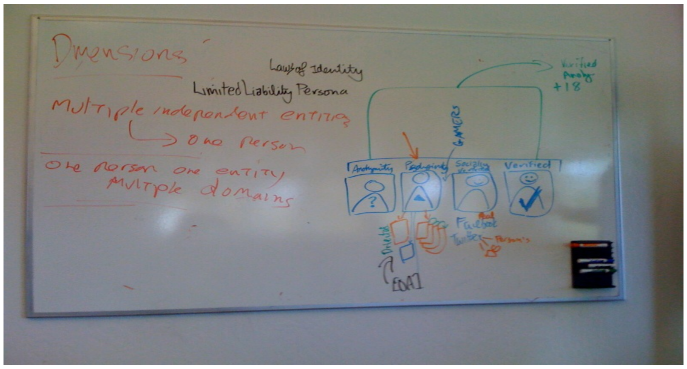
The problem with Yahoo ids: Logins, email addresses, and display name are all the same. You should be able to log in with a Google id. Don't deplete the Yahoo name space when only a unique id is needed. 99% of Yahoo ids don't receive (legitimate) email. Display names but not unique ids on the site.

Back to identity vs. identifier. Sometimes I want to use capabilities without providing an identity.

Proposal: Change the spectrum to classify types of activities?

At Yahoo, we found you got more protection with less verification. We want to hide the email address and IM name, but lawyers were opposed. The verified Yahoo id has too much capability attached to it. The better thing for the kid is the social identifier, but not the verified legal identifier. (We fixed the insanity.)

Rules will never substitute for parents protecting their children.



Session 10

WRAP – Simple OAUTH (10A)

URL: http://iiw.idcommons.net/WRAP

Convener: Dick H. – Brian E. – Allen T.

Discussion notes:

OAuth-WRAP Google Group:
http://groups.google.com/group/oauth-wrap-wg

All WRAP docs are here:

http://groups.google.com/group/oauth-wrap-wg/files

And the most recent version is WRAP-0.9.7.2

From Paramecium to People – Bioinformatics, Identity and Law (10C)

URL: http://iiw.idcommons.net/From_Paramecium_to_People
Video URL:

Convener: Scott David
Notes-taker(s):

Tags for the session - technology discussed/ideas considered:

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

From Paramecium to People: Bioinformatics, Identity and Law

Scott L. David

What is identity?

- Contextual
- Internal vs. External Identity
  - External Identity
    - “This is my stuff”
    - “I did (X)”
      - Data is the “trail of crumbs”
      - Reliability, availability and analysis of data are big issues
    - “I am capable of doing (Y)”
      - Authority
      - Ability
      - Interest
  - Internal Identity
    - Big question
    - Possibly an illusion

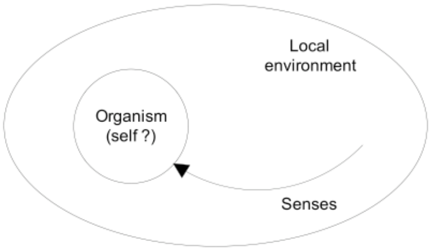
What is identity? -

- Ignore “theft” for this discussion
- Approach to analyzing identity
  - Identify each element of identity
  - Examine the effect of technology on each element
  - Review cumulative effects and emergent elements

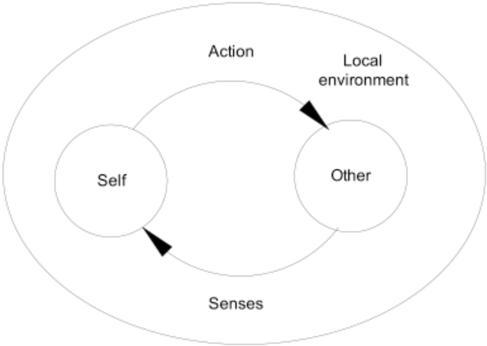
- Repeat

- Key Point:
  - The feedback loops that give rise to identity will be affected by technology which will fundamentally alter both the concept and the “experience” of identity

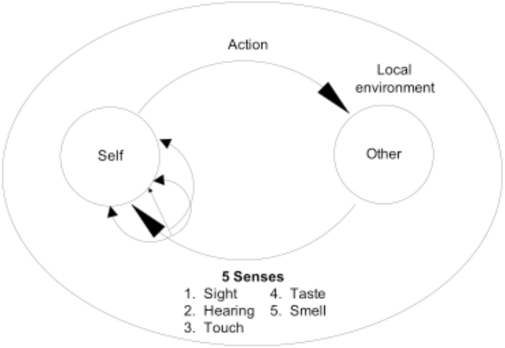
1. An organism and its senses



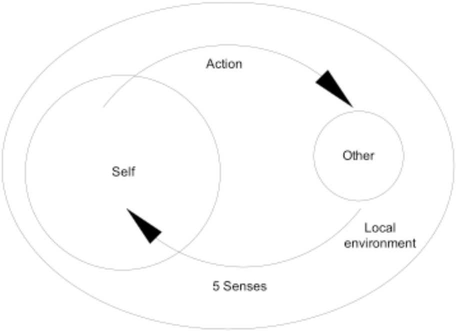
2. Identity emerges from a feedback loop



3. Feedback input is the five senses

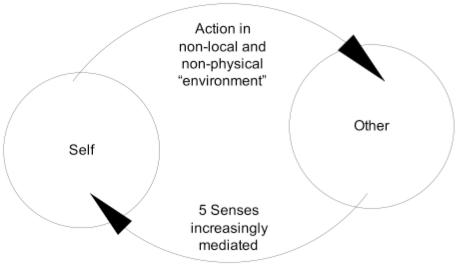


4. Identity is “expanded” by cultural components



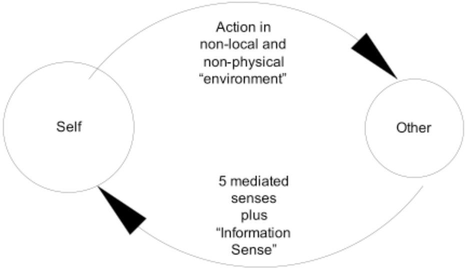
5. Tech affects feedback input and output

- Tech expands range of action and mediates senses

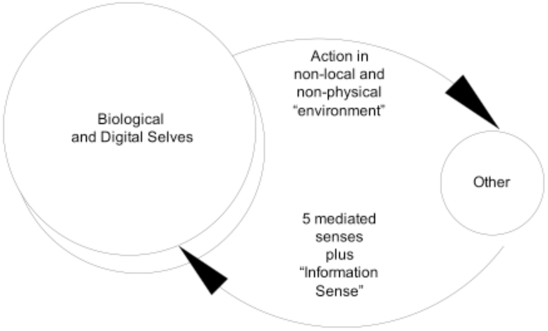

Action in non-local and non-physical “environment”
Self
Other
5 Senses increasingly mediated

6. Tech adds a new sensory channel

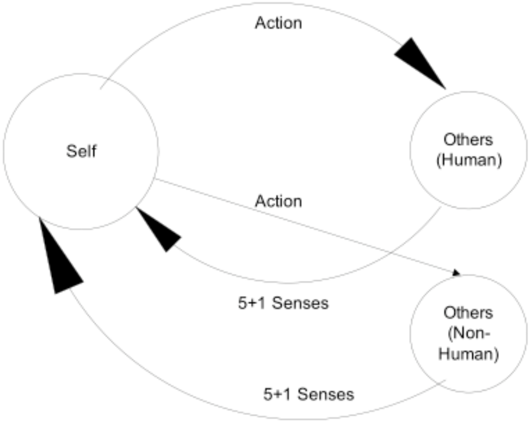
- Different quality and quantity of sensory input


Action in non-local and non-physical “environment”
Self
Other
5 mediated senses plus “Information Sense”

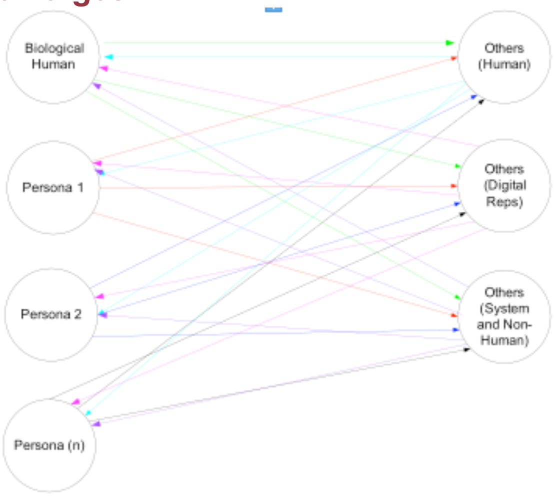
7. Tech adds new self – Humans as “1s and 0s” (even if rendered in graphical, VRI)


Biological and Digital Selves
Action in non-local and non-physical “environment”
Other
5 mediated senses plus “Information Sense”

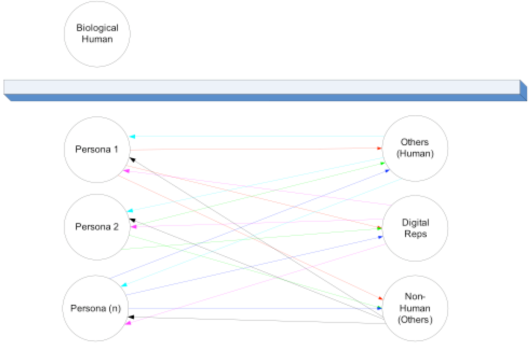
8. Tech adds new “others”



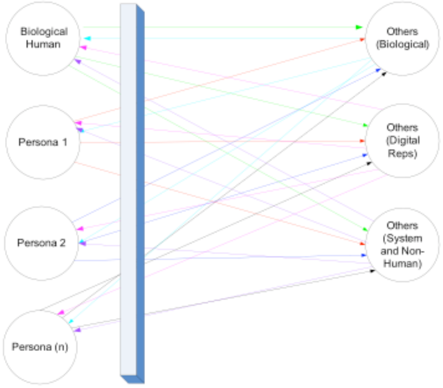
9. Tech results in feedback loop “system” of multiple “selves” and multiple “others” from which identity emerges



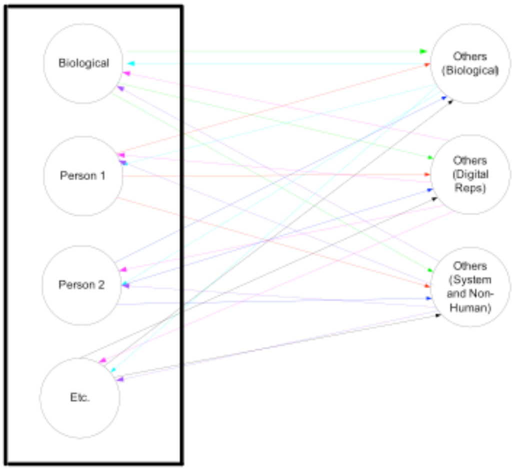
10. Increasing autonomy of your digital reps



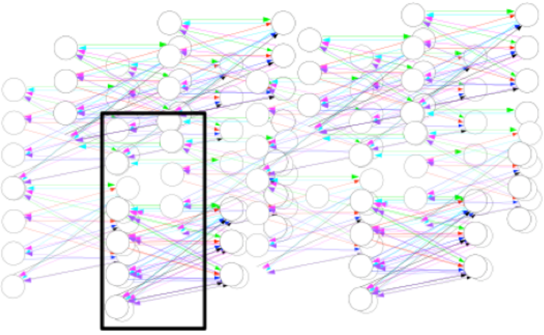
11. Disintegration and re-integration of identity through tech tools and legal rules



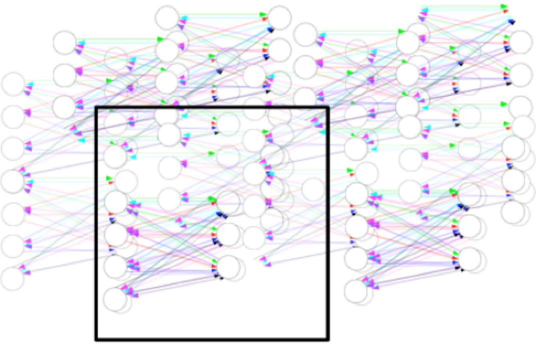
12. Non-biological, semi-permeable membrane (made from “tools and rules”) defines the “system you”



13. System “you” is immersed in the sea of system relationships (and is a component of the system).



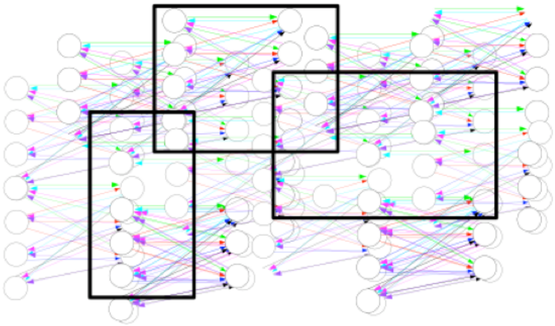
14. How far does the “tools and rules” membrane extend? Where does your identity end and the system begin?



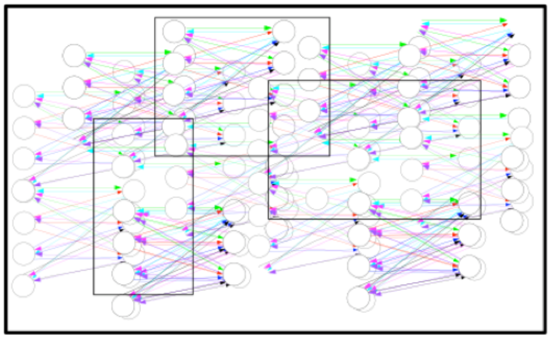
15. Why do you ask?

- If identity arises from feedback loops that are contextual, the answer to how far identity extends is also contextual.
- The “context” is the environment, which is no longer merely physical, but is increasingly made up of other human and non-human relationships (with increasing levels of abstraction) which together comprise the system.

16. Mapping multiple identities in a context



17. If the “tools and rules” membrane is placed around the whole system, what do we call that new thing? Does it have an identity?



The Future of Identity

- Continued expansion of effect of technology on 4 feedback components
- Increased ability to “tune” actions and senses to refine feedback loop as “needed”
  - “Machine assisted synasthesia”
  - Tuning of sensory channels

The Future of Identity

- Disintegration of self into various “Personas” followed by integration of multiple selves into larger system
- Autonomous development of elements of identity
  - Ratification of autonomous actions taken by persona
- Data relating to identity will take on new forms
  - VRI driven identity manifestations
  - Synthetic DNA in medicine and reproductive technologies
- New system (and identity) management tools will arise, many of which will be autonomous

The Future of Identity

- Let’s continue the discussion
-
- scott.david@klgates.com
- Twitter: ScottLDavid
- Second Life: Higgs Wopat
-
- Thank you

Portable Context Online (10E)

URL: http://iiw.idcommons.net/Portable_Contexts

Convener: Joe Andrieu, Switch Book, http://switchbook.com/
Notes-taker(s): Virginie de Bel-air, Orange Labs

Tags for the session - technology discussed/ideas considered:

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

How can a user keeps track and manage context to share with the sites he/she is visiting

Context: ambient, active (active implicit or explicit)

How could it look like?
Could be a cross-site cookie with semantics that I can control
Portable data store

A. Use-cases:

- search (different level if intent from browsing to be ready to transact)
- status update
- customer support

B. Content -> what should be in the portable context document?

Active:

1. Implicit: actions/ attention
2. Explicit: interim work product
    1. discovery (image, html)
    2. excel data set
    3. flash file

PII by reference
Ambient by reference
The environment (time, at work, weather....)
Permissions

C. Format/ Protocols
RDF document
Subject Pre Object

I.e: user queried travel trip
Departs city LA
Arriv City HNL

Ontology:
W3C work:
Delivery context
Describing human activities

D. How to share?
Discovery: Web sites could have link on their websites that could be discoverable where one can plug the portable context
Sites need to have server ability to understand what is being sent
Conditions: only data that can be sent is an ontology that is understood by the “data store” and that can be presented in a meaningful manner to the user and that the user can edit

E. What type of tool?
Switchbook has a IE plugin
Yahoo Search Monkey (collects searches in digital scrap book)
Browser can do that
Should be editable

How Should ID Support In The Browser Look? (10F)

URL: http://iiw.idcommons.net/How_Should_Identity_Support_in_the_browser_look_like%3F

Convener: Johannes Ernst

Tags for the session - technology discussed/ideas considered:
Active client, passive client, webfinger, UX

Discussion notes:

- Whatever solution we come up with, must work in *every* browser. So if an active client is involved, there must be a passive client solution that is very similar.
- Can we get the user login experience to nothing at all? Where the browser "knows" your membership at each web site and implicitly logs you in. Alternatively, we might define a per-site discovery mechanism by which the user agent can suggest to the user to "upgrade" their experience from "Yahoo" to "My Yahoo", which if the user selects would log in the user (as automatically as possible given the discovered authentication mechanism).
- E-commerce sites want to entice the user to buy before asking the user to log in.
- We don't think we can achieve pure uniformity of login experience across RPs and protocols. But perhaps we can achieve uniform *initiation* of the login ceremony, so that users can recognize how to begin to login, and so that active clients can automate it reliably.
- Uniform-looking username/password prompts across sites encourages users to use the *same* username and password across sites, which is *not* desirable.
- A user logging into a site for the first time may choose from several options:

1. Don't log in at all
2. Log in with a temporary, disposable identifier.
3. Log in with a permanent identifier that does *not* correlate with other sites.
4. Log in with a permanent identifier that *does* correlate with other sites.

- Upon returning to a site, a user may choose any of the above options, or an additional one:

1. Log in with an alternate (permanent) identifier to begin a new persona at a site.

- If we can get the login experience to be *completely* automatic, then logout must also be *completely* automatic (no persistent authentication cookies). Closing the browser must log the user out of all web sites implicitly.
- Mozilla: Less than 2% of users using a password manager in a browser use a master password.
- Classifications of our audience:

1. Single-computer user
2. Internet café
3. PC+Xbox+cell phone

- Dimensions:

1. Can roam (another device) / cannot roam (only one device)
2. Federated (non-local) / non-federation (local)

My Ideal Identity Flow (10I)

URL: http://iiw.idcommons.net/My_Ideal_Identity_Flow

Convener: Eran Sandler
Notes-taker(s): Eran Sandler

Tags for the session - technology discussed/ideas considered:

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

<u>Assumptions:</u>

- The notion of Personas (even if its just one) is available in all OpenID providers (if there is just one, its just you)
- OpenID providers has a standard, yet to be developed, protocol/API which gives:
  - List of personas (if available)
  - Switch current persona
- OpenID consumers (sites) will support an the Discovery XRD spec to detect:
  - OpenID end-point
  - Signout end-point (for when I want to switch a persona and make sure I'm signed out from a site with the current persona)

<u>Eventual Result:</u>
Have an integrated always knowing identity toolbar that can auto sign me in to sites I've previously used with the OpenID provider. The provider will also associate a specific persona with the site I'm logging into so that when I switch personas, it will automagically log me out of the current site with the current persona and allow me (if I want to) to register with a different persona.

<u>Scenario(s):</u>

- Open browser and log into the defined OpenID provider
- Go to a site
- Identity Toolbar will detect if there is an OpenID end-point (through XRD discovery)
  - If there is an OpenID end point toolbar will query the OpenID provider if I've previously signed up to the that site with the current active persona
    - If I did, based on a preset it will either ask me if I want to sign-in or automagically sign me in by initiating an OpenID login with the openid end-point previously discovered
- When I switch a persona, the toolbar will request the site to sign-out

- When I access a sign-up page, the toolbar will detect that this is the sign-up end-point and will perform an OpenID login which, since this is the first time, will act as a registration flow and will try to automatically register me with the details of the current active persona.
- It would be great to have a "guest" mode, in which when I give my computer to someone to browse it will disable the auto sign-in/up features so that the person currently using my computer won't gain access.

It's a bit messed but that's basically the point I've originally assembled on some paper and transferred here for the summary of IIW :-)

The efforts of the XRD discovery will make this toolbar/features closer to reality. Now we just need to close the OpenID provider’s standard API/protocol and to have sites support the sign-out end-point :-)

Session 11

Identity in the Browser (11B)

URL: http://iiw.idcommons.net/Identity_in_the_Browser

Notes-taker(s): *Dr. Ernie*

Discussion notes:

http://ihack.us/2009/11/10/active-identity-clients-aics-for-openid/

Tags: identity, javascript, openid

"“Enough is enough! I have had it with these #@%!*$ AICs and their #@%!*$ panes” — Samuel H.S. “Hammer Stack” Jackson (with apologies to Neville Flynn)"

Introduction
The OpenID community is still wrestling with how to deliver a first-time login experience that is acceptable to mainstream users. Research indicates we need something less open-ended than typing into a blank URL field, but neither is it desirable to push users to choose from a few (or worse, many) pre-selected identity provider logos.

One approach for solving this problem is called (for lack of a better term) the Active Identity Client, or AIC (similar to what I previously called a Chamberlain). An AIC boostraps the identity selection process at a new website (aka Relying Party, or RP) by storing some amount of identity information on the user’s home computer. The AIC uses that identity to access a persistent record of the user’s interaction with multiple sites and identity providers (IdPs) to negotiate and streamline future such interactions. This (in theory) allows the user, rather than the RP, to prioritize which providers to use.

A number of such AICs were demonstrated at last week’s Internet Identity Workshop. Rather than attempting to standardize on a single AIC, a group of us discussed developing a common infrastructure that might enable a broad spectrum of AICs to innovate and compete. Specifically, we attempted to identity conventions, best practices, and extensions to existing standards that would support both “native” and “in-browser” AICs.

This article is my idiosyncratic attempt to synthesize what we discussed into a coherent vision for Active Identity Clients. It may not fully reflect the opinions of any given participant, and certainly does not represent the views of our respective employers. Rather, it is a subjective snapshot of a still-evolving problem space, and is intended to provide a concrete starting point for further discussion, critique, and clarification.

Usage
The one problem OpenID can’t solve is knowing what to tell a first-time user, since by definition the website doesn’t yet know who the user is. An Active Identity Client is able to streamline the process of establishing trust because it always knows who the user is, and can thus negotiate with the website on the user’s behalf to ensure only relevant choices are presented. For example, it can:

1. Track and manage the user’s preferred identities
2. Automatically sign on to known and trusted sites with the appropriate ID
3. Suggest which existing ID to use when visiting a new OpenID site
4. Safely enable user to acquire a new ID for a given site, when necessary
5. Ensure a user’s custom ID is as readily usable as a ‘well-known’ ID
6. Record where and when a user used various IDs

Scope
In order to make forward progress during IIW, we explicitly agreed to focus on a very narrow set of requirements:
1. OpenID, versus all other protocols (e.g., InfoCard and SAML)
2. Required infrastructure, versus the overall AIC user experience

Those other issues are far from unimportant, but we wanted to first come up with a concrete solution that addressed this specific problem, after which we can and should see whether it could be easily generalized for broader use.

However, we did expand the definition of AIC to include both native (e.g., via plug-in, toolbar, external manager, or direct browser support) and JavaScript (e.g, cloud-based) implementations. There was heated discussion about which of those models is more secure and/or viable, which is why we want to enable both and let the market decide. Note however that ensuring this flexibility may require some creativity in how this gets implemented and rolled out.

Markup
This first piece of infrastructure needed to support AICs is some simple markup a web designer can add to their website to indicate support for OpenID and AICs. We consider — and rejected — a proposal to simply include the information as a META tag in the header, as that would potentially require the AIC to scan every page to determine whether to active/be activated. Instead, we agreed to develop a custom tag that could either be interpreted directly by the browser, accessed by JavaScript, or converted to an <object> to launch a plugin when activated.

The rationale for a custom tag (as opposed to, say, a microformat) is to allow the website (i.e., Relying Party) to explicitly and unambiguously provide important metadata, such as:

# Canonical name/template for the Relying Party (“realm”)
# Lists of suggested and/or required Identity Providers
# URL to return to after authentication
# Link to privacy policy
# Tags describing type of website (to facilitate user policies)
# Plus perhaps “protocol” and “tokenType” to allow use of tag by other protocols

I believe it is important to provide appropriate defaults (either global or AIC-specific) for all of these, so that it is as simple as possible for web developers to ‘tag’ their websites as supporting OpenID AICs. For example, one possible implementation is to have a “login” tag that wraps the various URLs used for manual login, which would not need any attributes if the developer was happy with the default values. In theory it might even be possible for browsers to “sniff” OpenID support even in the absence of an explicit tag, but that may or may not be advisable.

Status
The ultimate goal would be to have this tag become part of HTML 5 or a similar standard. Chris Messina of the OpenID Foundation has agreed to take this action item, to propose an implementation and shepherd it through the appropriate approval process.

Provider Branding
The second extension required is a way for OpenID Identity Providers (IdPs) to provide human-oriented descriptions of themselves to facilitate user decisions. Currently, various websites and client software hard-code their own list of names and logos for different providers. Instead, we recommend that as part of its XRDS file each IdP also specify their:

* logo, in, e.g. 16×16, 48×48, 128×128, 256×256 sizes
* human-readable name

Note that were appropriate there should be a localized version of this content based on the language specified in the HTTP headers.

Status
Mike Jones of Microsoft has already been discussing this extension with the OpenID User Experience working group, and formal proposal is in the process of being approved.

Security and Spoofing
One of the main reasons for Provider Branding is to enable a friendly listing of Providers specified by the RP in the login tag. Unfortunately, this means that Branding could be used to redirect users to a phishing site. While in one sense this is no different than the website presenting that directly, the fact that a putatively trustworthy AIC is displaying what may be misleading information is a cause for concern.

The best that can be done is for the AIC to explicitly mark Providers as untrusted (vs. trusted) until they have been explicitly verified by the user. But to avoid bombarding the user with false negatives, AIC’s should pre-populate with a list of well-known Providers (“whitelist”), or perhaps well-known Phishers (“blacklist”).

There was considerable interest in having such lists be published and/or managed by a neutral party, such as the OpenID Foundation. However, there was no clear consensus on what the policy should be for inclusion in that list, given that different regions may have different “well-known” providers and some providers (e.g., Google) may want to authorize millions of subdomains.

Status
Under the circumstances, I believe it is premature (and may well be unnecessary) to standardize this aspect of the user experience. Instead, it is incumbent upon each AIC developer to:

* Choose a reasonable set of pre-approved Providers
* Require SSL certificates for any trusted Providers

* Allow the user to easily specify their own trusted Provider
* Automatically honor Extended Validation Certificates
* That should provide a reasonable balance of convenience and security for the short term, and provide useful experience to inform future standardization efforts.

JavaScript Support

One area we only touched on briefly at IIW but may prove crucial to adoption is the development of a standard JavaScript library to act as a meta-selector. Since it will take a long time (if ever) before browsers fully support a login tag, participating sites will probably need to include a JavaScript library that:

* Detects which AICs are installed/available
* Determine which AIC the user prefers/has configured
* Can rewrite the login tag to launch a plug-in
* Can delegate to an in-browser AIC
* The logical home for this would be an OpenID popup library, which would also act as “fallback” if no AIC was available. In fact, the additional metadata specified here should enhance the user experience of the popup, by allowing it to dynamically customize the list of buttons based on the Providers recommended by the website.

Status

This is the most important but least well-defined of the areas under investigation. Ariel Gordon of Microsoft agreed to work with Allen Tom and Paul Trevithick on how best to integrate it with the frameworks they work on.

Conclusion

OpenID has enormous potential for making browsing the web both safer and more convenient, but that potential will not be realized under “ordinary” users feel comfortable using it. I believe that if we can successfully tackle these few remaining issues then JavaScript, browser, and platform developers will be able to experiment with and deliver vastly improved user experiences. This in turn should encourage even more websites to act as Relying Parties, and finally make single sign-on a reality on the public Internet.

'''Appendix: Related Technologies'''

* [http://hueniverse.com/2009/08/introducing-webfinger/ Introducing WebFinger]
* [http://www.abstractioneer.org/2009/04/personal-web-discovery.html Personal Web Discovery]

SAML and OAUTH a la Hybrid (11C)

URL: http://iiw.idcommons.net/SAML_and_OAuth

Convener: Paul Madsen

Discussion notes:

http://bit.ly/2kFVtr

Goals

- Explore (useful) combinations of SAML & Oauth
- Builds on 2008 proposal from Ping ID for combining SAML SSO & Oauth authz sequence
- Learn from OpenD Oauth Hybrid extension

SAML & OAuth

- OAuth does not stipulate how the user authenticates to either the SP or Consumer
- SAML SSO can provide the authentication
- If so, question is whether/how the SAML messages by which SSO happens can facilitate the fundamental Oauth sequence of
  1)Obtaining User authorization (consent) of a request token
  2)Getting the authorized request token from the SP to

Consumer
* OpenID community calls this scenario 'hybrid', SAML/Liberty a
'boostrap'

Oauth Request params

- The OpenID Oauth hybrid model does away with the initial server-to-server call by which the Oauth Consumer gets an unauthorized request token
- Consequently, instead of carrying an unauthorized request token and asking for its
- approval, the OpenID request carries an implicit 'return an approved request token' request
- Request includes Consumer_Key, maybe not Consumer_Secret, callback_url....

SAML extensibility

• SAML provides flexible extensibility model by which protcol messages (e.g the <AuthnRequest> and <Response>) can be extended with XML elements from other namespaces

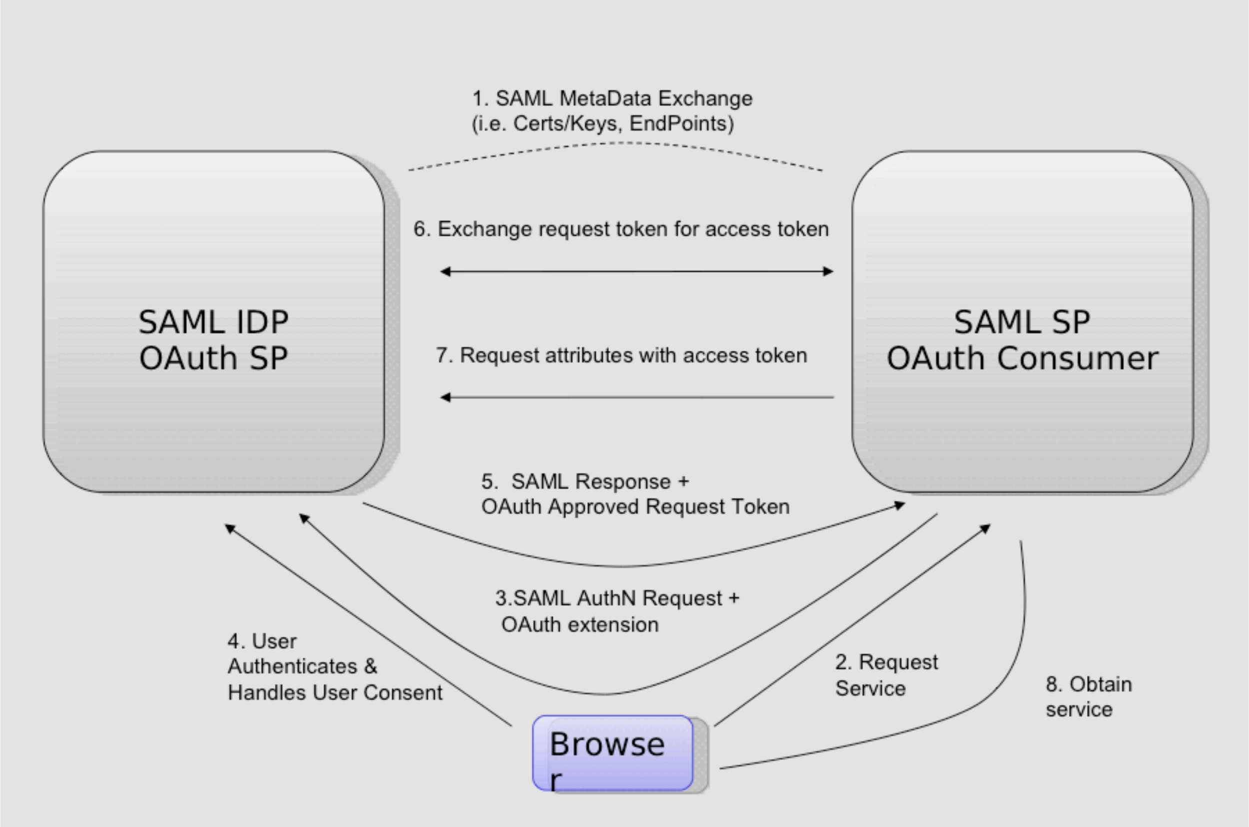
• SAML defines some core attributes but new ones can be spun up as necessary

• Depending on SAML/OAuth roles played by actors, we'll need one or both of extension point

#1 SAML Idp == Oauth SP

- In the simplest case, the SAML IdP == Oauth

- SP & SAML SP == Oauth Consumer As in the OpenID Oauth Hybrid extension
- Challenge is to get the User & Oauth request params from Oauth Con to the Oauth SP, and get the authz request token back
- Use SAML AuthnRequest to carry the Oauth request params from Oauth Con to Oauth SP
- Use SAML <Response> and <Attribute> within to carry the authz request token back



#1 Extension Needs

- Define Oauth extension to SAML AuthnRequest to carry Oauth params from SAML SP(OAuth Con) to SAML IdP(OAuth SP)
- Define SAML Attribute to carry the approved request token from SAML IDP(OAuth SP) to SAML SP(OAuth Con)

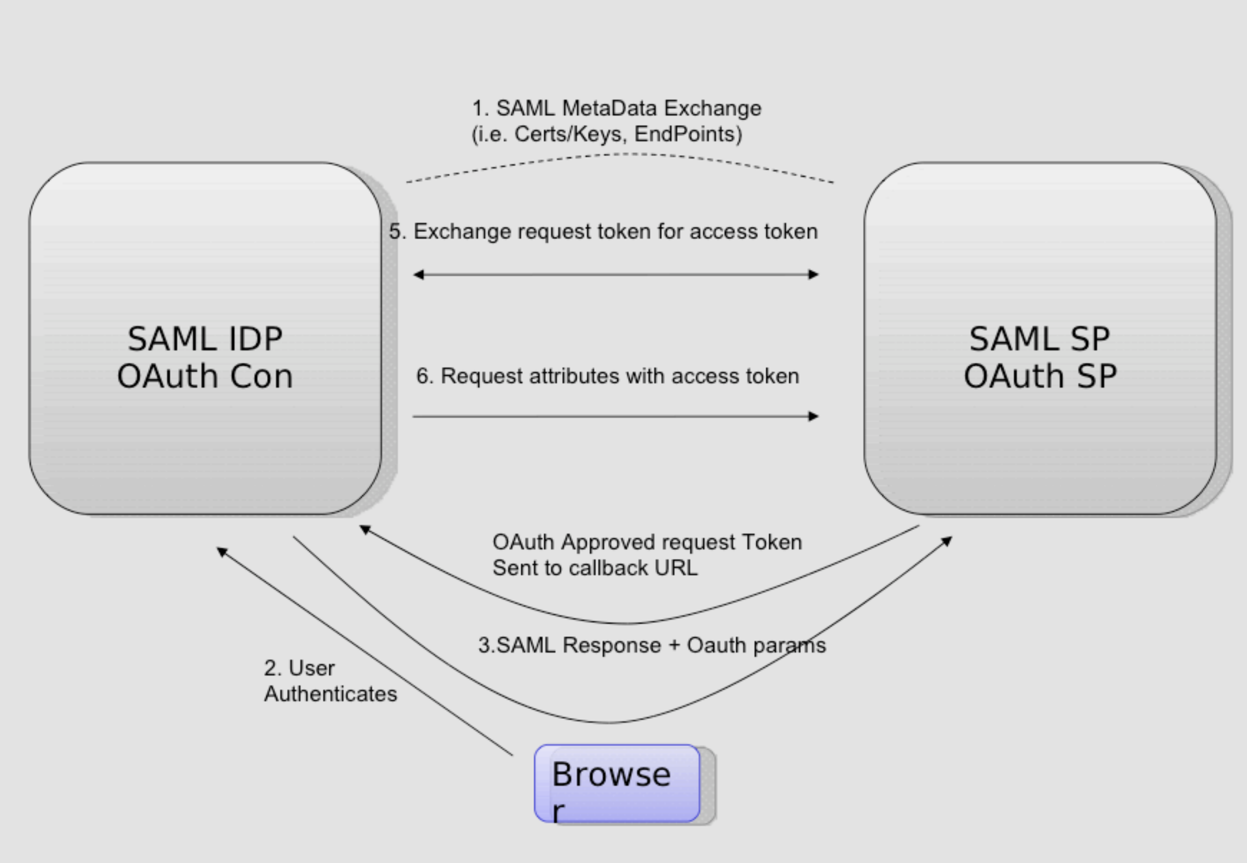
2) SAML Idp == Oauth Con

- And SAML SP == Oauth SP
- Implies separation of roles between authentication and attribute storage/sharing
- User authenticates at SAML IdP, but must give consent/authorizations at Oauth SP

- Challenge is get Oauth request params from SAML IdP to SAML SP/OAuth SP in order to obtain Oauth consent (and eventually get an authorized request token returned)

– Use unsolicited SAML <Response> and <Attribute> within to carry Oauth request params

– Rely on Oauth msg to get the authz request token from Oauth SP to OAuth Consumer


1. SAML MetaData Exchange
(i.e. Certs/Keys, EndPoints)
5. Exchange request token for access token
SAML IDP
OAuth Con
6. Request attributes with access token
SAML SP
OAuth SP
OAuth Approved request Token
Sent to callback URL
3.SAML Response + Oauth params
2. User
Authenticates
Browse
r

#2 Extension Needs

- Define SAML Attribute to carry Oauth request params from SAML IDP (Oauth Con) to SAML SP (Oauth SP)

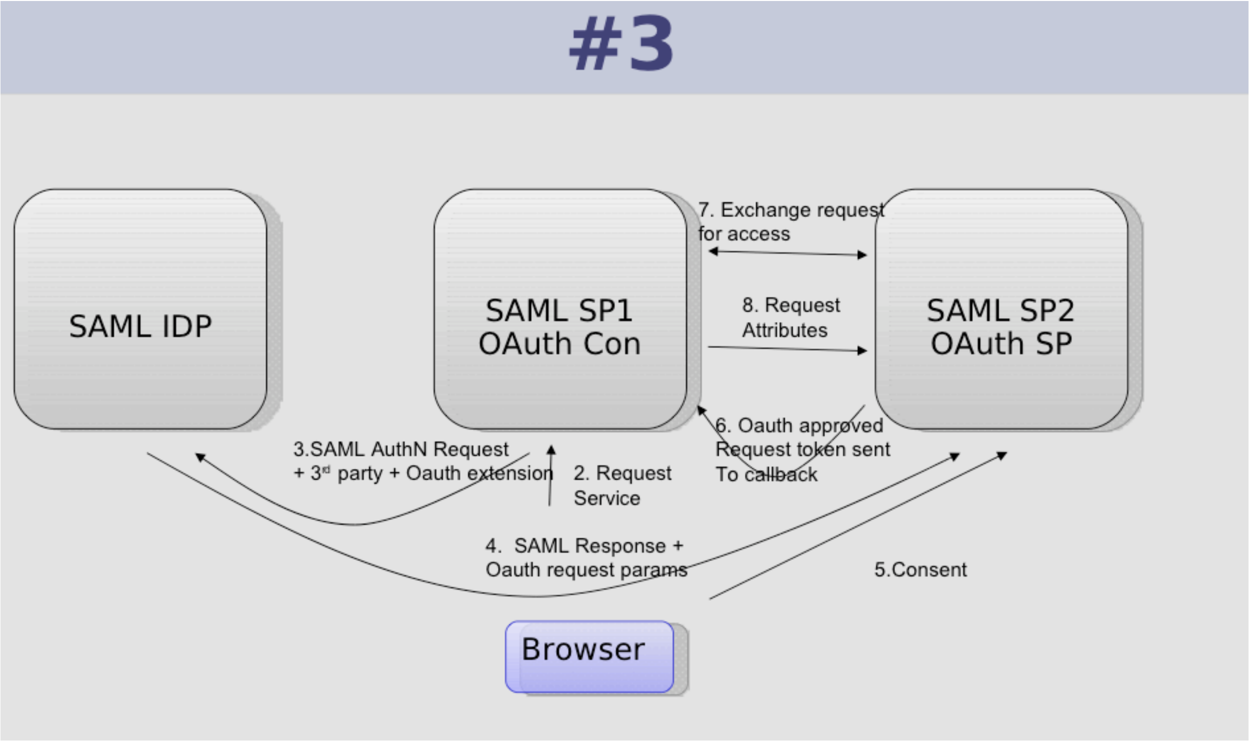
3) SAML SP1==OAuth SP & SAML SP2==OAuth Con

- Most general case, SAML IdP not involved in attribute sharing
- User authenticates at SAML IdP, SSOs to two distinct SAML SPs (an Oauth SP & an Oauth Consumer respectively)
- Challenge is to get the User & Oauth request params from the first SAML SP to the second in order to obtain consent, and the authorized request token back

– Use SAML 3rd party requestor extension to get

- Oauth request parsms from Oauth Consumer to Oauth SP

– Rely on Oauth msg to get the authz request token from Oauth SP to OAuth Consumer



#3

SAML IDP

SAML SP1
OAuth Con

SAML SP2
OAuth SP

Browser

7. Exchange request for access

8. Request Attributes

6. Oauth approved Request token sent To callback

3.SAML AuthN Request + 3rd party + Oauth extension

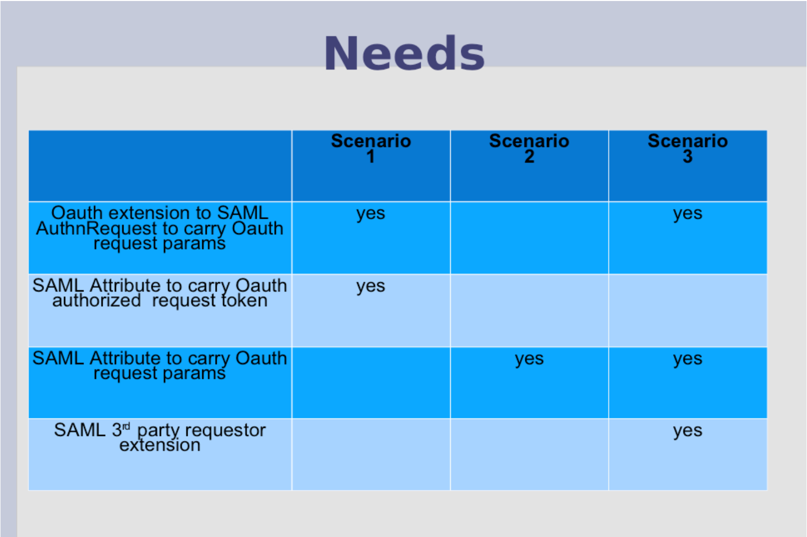
2. Request Service

4. SAML Response + Oauth request params

5.Consent

#3 Extension Needs

- Leverage the SAML 3rd party Requestor extension to indicate IDP should send SAML response to Oauth SP2
- Define Oauth extension to SAML AuthnRequest to carry Oauth request params from SAML SP1 to SAML IdP
- Define SAML Attribute to carry Oauth request params in a Response from SAML IDP to SAML SP2



Needs

	Scenario 1	Scenario 2	Scenario 3
Oauth extension to SAML AuthnRequest to carry Oauth request params	yes		yes
SAML Attribute to carry Oauth authorized request token	yes		
SAML Attribute to carry Oauth request params		yes	yes
SAML 3rd party requestor extension			yes

Open ID Trust Frameworks/Open ID & Info Cards (11E)

URL: http://iiw.idcommons.net/Open_Identity_Trust_Frameworks

Convener: Don Thibeau and Drummond Reed
Notes-taker(s): Mary Rundle

Tags for the session - technology discussed/ideas considered:

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

See slides http://wiki.informationcard.net/files/Presentations/open-identity-trust-fmwks.ppt

Purpose

The purpose of this IIW discussion is to answer questions and get feedback on evolving work by OIDF and ICF in this effort.

Terms of Reference

Terms of reference have changed as a result of IIW discussions.

Foundations' Work

Promoting the adoption of Open Identity protocols, including OpenID and Info Cards.

The diagram includes the user/user agent in the middle. OpenID vNext will have support for active clients.

The registry function is not a broker.

Operate at Internet scale. So identity scheme profiles should have URIs, so you are able to do a fairly simple look-up. Lightweight and generally useful.

An IdP or RP could have multiple registrations according to different schemes.

To make it a trust framework, you factor in the policy requirements (e.g., LOA). [Has LOP fallen out?] Assessors check if a party meets the requirements of the trust framework.

Questions/Comments:

Have you shared it with any of the audit firms? Not yet. A goal is to allow self-certification and on.
What constitutes a qualified assessor/auditor? It's open. Our role is to audit the auditors.
Regarding terminology, the two terms assessor and auditor are being used interchangeably, as Kantara uses one, the U.S. Government uses the other, etc.

Will the user see a branded version of the registration? That might be a focus area.

What do you mean by “trust” in this context? The words “Trust Framework” are not our choice, but rather what is used by the U.S. Gov’t. Open Identity Trust Registry could instead be called Open Identity Policy List. The term policy can include trust; it’s more general. Open Identity Reference Model?

Can we change the term “identity scheme profiles”?

Is it meant to work in a purely commercial setting? Yes.

Can’t we use terminology that industry prefers? For the purpose of engaging with Government, this terminology is most practical.

Why draft a white paper for industry? Industry needs a YouTube video or two-page specs document, and then a white paper can explain it to Government.

Why not keep it simple and go for self-certification, esp as Government use case now is LOA1? Spell out a model now that allows going up in LOA. If you only do tech interop, you are not addressing policy needs.

Is there more than one certification agreement per profile?

Is there intention to impose criteria on IdPs by this? If so, it’s policy/regulation by the backdoor.

Is this too ambitious? Commercial players may have their own interests, e.g., not public policy but their own policies. Our goal is adoption, so yes, the model is meant to factor them in.

The philosophy reflected here feels more like PCI Level 3 (credit card industry). Uptake was very rapid there.

Are the mechanisms flexible enough for other entities to have other profiles? Yes, for example in health care.

ICAM has conflated interests of claims provider and service provider in the profiles.

Next steps:

Catalogue issues, draft white paper (telling terms and players). A white paper allows subsequent distillation in YouTube, etc.

More Notes

The key takeaways at a very high level were:

1) The IIW community reaffirmed that there is a real need and many real use cases for an trust framework model for open identity, and that a model that can accommodate multiple trust frameworks in one

infrastructure is a good direction.

2) The semantics around the terms for this model are extremely important - we spent half our time just explaining and refining (based on community feedback) the terms uses to describe the model.

3) The community strongly agreed that the model needs to address Levels of Protection (LOP) as well as Levels of Assurance (LOA) for identity information.

4) There was strong feedback and consensus that the model should support BOTH technical AND policy certifications and BOTH self-certification and third-party certification. So this matrix of all four combinations must be supported by the overall model, even if specific trust frameworks (such as the US ICAM trust framework) requires a subset of these options.

Lastly, we invited all community members who are interested to get involved, and invited them to contact either of us directly.

Sorry, I don't remember the room or session number. But here is the discussion group with our meeting notes!

http://groups.google.com/group/oauth-key-discovery/topics

Cheers,
Brian

Lessons Learned From Email (11G)

URL: http://iiw.idcommons.net/Lessons_Learned_Past_Efforts

Convener: Jim Fenton & Craig Spiezle
Notes-taker(s): Ellen Siegel

Tags for the session - technology discussed/ideas considered:

How can we apply lessons learned in standardization/adoption of email authentication and Extended Value Certificates to current efforts in the identity space?

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

Email Authentication

- Chicken and egg... no one wants to invest before the technology is active in the industry
- multiple technologies... which one to implement?
- Even within a given technology, specs were still evolving, some had protected intellectual property or proprietary specs... some concerns about motivations of key players involved in spec development
- disconnect between technical specs and business stakeholders... what's the business case?
- Role of policy layered on top of authentication specs.. technology, use case, etc
- conflict of interest: anti-spam vendors, certification services
- sometimes over focus on fringe cases... can derail standardization efforts
- lack of analysis tools slowed adoption... lack of confidence that implementations have gotten it right
- some rough tools have been pretty widely available (test reflectors for DKIM, similar tools for sender ID / SPF... but hasn't really been enough
- maybe less incentive for e.g. esps to get their customers on board... left it up to individual companies (this has for the most part changed now... most esps support email authentication at least as an option for their customers
- also issues with incenting hosters to support necessary DNS configuration (this is still somewhat an issue today, especially for smaller businesses who use 3rd party DNS/web hosting services... some key hosters are starting to make it easier for their customers to configure email authentication, although probably still too complicated for really small businesses
- openID may have an advantage because it's a community effort and not driven by one (or a small number) of companies with potentially private agendas

- open id may still have some of the long tail for small businesses, because the setup requires network configuration knowledge... currently that tail is mostly not using authentication on their web sites, but that may change

Key issue: how to motivate adoption: what is the business case for key stakeholders

Another example: Extended Validation certs (EV Certs)- needed to address the fact that certificates were losing value because it was relatively easy to procure a deceptive certificate and confuse consumers.

Went after key stakeholders to encourage early adoption, and provide concrete examples for follow-on adopters; early adopters could also use their adoption to self-promote added business value for their customers

also got browser support for recognizing ev certs and making validation visible to users (green/yellow/red bars in URL text box)

value proposition was higher level of consumer trust for participating sites (not enitrely clear how to measure this)

driven by smaller, focused group with clear goals

succeeded in much shorter time frame than email authentication

like with many of these efforts, need to do this within the constraints of existing technical infrastructure

needed to create/standardize new requirements for the additional validation for cert requister (organization applying for certificate)

DNS issues:

- is there support for publishing txt records (required to store auth info)
- is there support for '_' in domain names (required for dkim key publishing)

Question: how can we get identity efforts from today's state to something closer to the EV cert experience

- early focus on compelling business case and value proposition (ideally for both business and for end user)
- identifying key set of visible initial stakeholders to adopt and promote technology/ standard
- make sure to have sufficient focus on user experience (both for deploying organizations and for end users)

Email auth experience focused more on technology side and on fringe cases, and less on business case, value proposition, end user experience

Domain reputation:

- domains may have more than one reputation (e.g. email reputation vs. is the site fraudulent)... but many discussions seem to confuse the two
- what is identity? e.g. there are email auth domeains that aggregate under a brand (e.g. newsletter.brand.com), and others that aggregate under a 3rd party (e.g. brand.3rdparty.com)

How can we support multiple identites (specific limited representation for particular sites/applications) but also have an easy way for **me** to locate and manage all of these? One answer is that the “collector” is the IDP, but it's unlikely that at least in the near term that a person will have a single unique IDP (but at least there will be fewer IDPs than personae).

Lunch Day 3

Why Facebook Doesn't Implement OAuth Today

URL: http://iiw.idcommons.net/Why_Facebook_doesn%27t_implement_OAuth_today

Convener: Luke Shepard, David Recordon
Notes Taker: Luke Shepard

In this session, we (Luke Shepard and David Recordon from Facebook) talked about some of the technical reasons why Facebook hasn't implemented OAuth.

High level:

- We generally respond to our customers. Some of them request open standards, but more important is that our API is fast and simple.
- OAuth is more complex and less performant than our own native authentication mechanism
- We (Facebook) really want to use OAuth but I can't justify deploying and maintaining a new system that will be slower and create more maintenance headaches for our customers
- OAuth WRAP looks like it will solve most or all of these problems

Performance concerns

- It takes only two HTTP requests to get a user session in Javascript and start making API calls. With vanilla OAuth, it takes four HTTP requests - two on the server, and two on the client.
- URL length is a big deal. We try to keep ours terse. The full-URI-based approach of many open standards leads to ridiculously long URLs that have perf impacts.
- We do some tricks to support client side caching and JS api calls, whereas existing protocols mostly assume server-side setups.

See the attached PDF for the diagram showing the difference between the two flows.

Response

There was active participation from Allen Tom, Joseph Smarr, Brian Eaton, Eric Sachs, and a few others.

- Several people asked why we don't just support OAuth as an alternative - at least it would be open, right? My response was that if we use an open protocol, we would like to eventually use it exclusively. It is draining and expensive to support multiple authentication mechanisms, so why would we roll something out that wasn't a step in the direction we want to go?
- Agreement from big companies. At Google and Yahoo, which have had OAuth endpoints for some time, they both report that their proprietary protocols (AuthSub and BBAuth) are still dominant. Why?
- You can only roll out a standard that isn't in your strong business interest for so long. If internal proponents push for a company to launch something that isn't well adopted, then they lose credibility for the next attempt.
- Why not OpenID/OAuth hybrid? Main concern is URL length and complexity of unifying two protocols in a library.
- Standards are sometimes too quick to close security holes that proprietary protocols deem acceptable. For instance, Facebook passes the session back directly in the response, and

even stores it in cookies, which means that a poorly-written endpoint could leak it to images or iframes that are included in the page. OAuth protects against this flaw, but BBAuth does not. So general question is if security risks are acceptable in proprietary protocols, then shouldn't they be possible in the standard?

- Library support is often touted as a reason to adopt OAuth, but there was general agreement that library quality is overall pretty poor. I think many agreed that if we make the actual protocol much simpler, then we will get a lot more general library support.

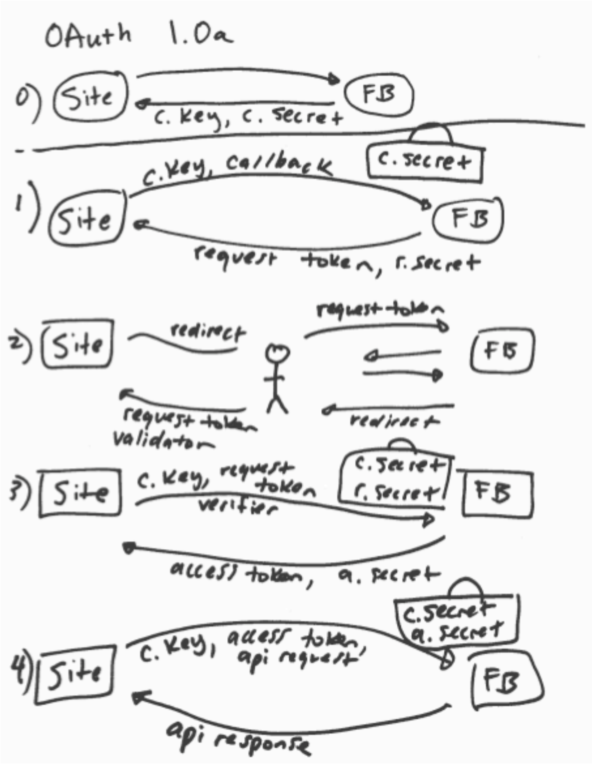
Future

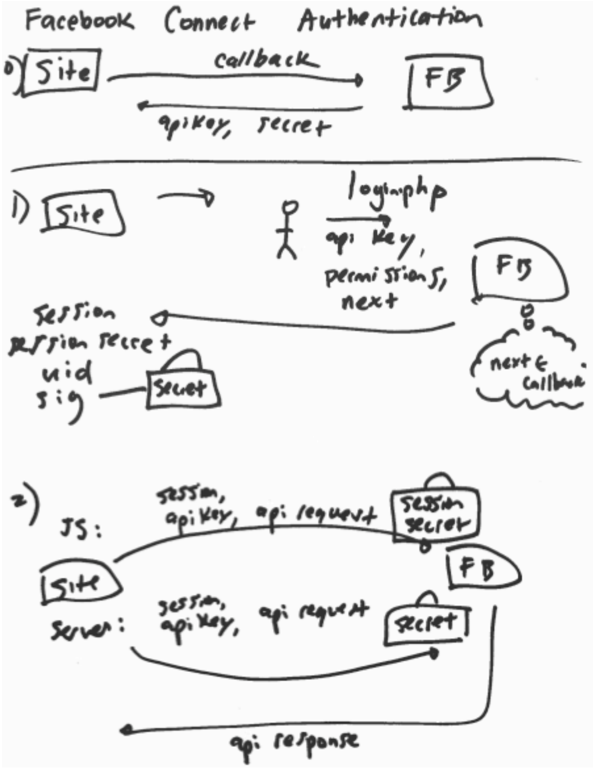
Brian Eaton showed that OAuth WRAP addresses many of these concerns- fewer HTTP requests, simpler libraries, easier to understand. It also supports multiple profiles.

A bunch of OAuth WRAP folks are planning to meet Tuesday Dec 7 at Facebook HQ to more specifically hammer out an OAuth WRAP profile optimized for JavaScript authentication. It's great to see forward momentum come out of this meeting.

Links

- Whiteboard image from the talk: http://iiw.idcommons.net/images/c/c2/Oauth_fbconnect_comparison.pdf
- OAuth WRAP: http://wiki.oauth.net/OAuth%20WRAP
- Facebook Connect auth implementation: http://github.com/facebook/connect-js/blob/master/src/core/auth.js#L211





Getting Data into XRD

URL: http://iiw.idcommons.net/Getting_data_into_XRD

Convener: Will Noris

XRD Provisioning (XRDP)

XRD provides a common document format for describing a resource and the relations it has with other resources. This document defines XRDP, a protocol facilitating delegated management of entries in an XRD document.

For example, when an individual creates an account at a photo hosting service, the service can provision a link into the individual's XRD describing the new relation. When a service provider changes its protocol endpoint, it can update the entries in its users' XRD documents to reflect the new value. A user could use a desktop application with a rich user interface to configure their XRD preferences, and have that provisioned to their XRD provider.

XRDP Service Endpoint

The XRDP service endpoint for an XRD is identified by a Link with the following Rel value:

- http://docs.oasis-open.org/xri/xrdp/v1.0/

The endpoint MUST be an http or https URL.

It is recommended that the URI for the Link is the URI for the XRD document itself. (REST-ful)

!! If the URI is anything other than the URI for the XRD document, then we are violating the HTTP spec with respect to the PUT method, and violating the intended use of DELETE.

The XRDP service endpoint URL MUST NOT contain any of the following URL parameters: "rel", "media-type", "uri", "uritemplate".

The XRDP service link differs from most XRD links in that the relation is between the XRD document itself and the XRDP endpoint, and not between the resource described by the XRD and the XRDP endpoint.

Identifying Links

Some XRDP operations are performed on a specific Link element within an XRD document. Link elements are uniquely identified within an XRD by the combination of the Rel, MediaType, and URI or URITemplate (whichever is present) child elements of the Link.

((This is based on the assumption that it doesn't make sense to have two Link entries with the same Rel+MediaType+URI tuple. Alternately, Links could be identified by an xml:id attribute. For the create and update operations, it doesn't make too much of a difference either way. But for the delete operation, something like an xml:id would make it much cleaner.))

Operations

Operations are performed by sending HTTP request to the XRDP endpoint for the XRD. Requests SHOULD be authenticated, but the exact means of doing so are beyond the scope of this document. (OAuth is recommended?)

XRDP servers are responsible for enforcing appropriate authorization rules, such as preventing a service from updating or deleting a <Link> they did not initially create.

Create and Update Link Entry

Create and update operations are made by sending an HTTP POST request to the XRDP endpoint for the XRD. The body of the request MUST be of type "application/xrd+xml" and include the single <Link> element that is being created or updated. If a Link already exists in the XRD document with the same identifier tuple, it is replaced by the Link in the request.

XRDP servers SHOULD only allow a Link entry to be updated by the same XRDP client that originally created the entry.

Delete Link Entry

A Link entry is deleted by sending an HTTP DELETE request to the XRDP endpoint for the XRD. The link to delete is identified by including the appropriate URL parameters in the delete request:

- rel = the Rel value of the Link to delete
- media-type = the MediaType value of the Link to delete
- uri = the URI value of the Link to delete
- uritemplate = the URITemplate of the Link to delete

All URL parameter values MUST be appropriately encoded. Parameters MAY be omitted if the Link to be deleted does not contain values for those parameters.

Update the XRD

The entire XRD document may be replaced by sending an HTTP PUT request to the XRDP endpoint for the XRD. The body of the request MUST be of type "application/xrd+xml" and include the new XRD document.

- Must the subject of the new XRD match the old?
- What about signing the new document?

Related Work (section added by Markus 11/06/2009)

@fullXRI experimental OAuth endpoint:

- An experimental OAuth endpoint for modifying i-names' XRDs is documented here: http://oauth.fullxri.com
- Two experimental consumers of the above OAuth endpoint are implemented here: http://www.busystatus.com, http://www.buzymazterz.com.
- This OAuth endpoint only supports one very basic editing operation ("add service").
- One key thing to note is that all data about the editing operation is already passed in the OAuth "Get Request Token" step. The final "Access Protected Resources" step then does not contain any parameters except the standard OAuth ones.

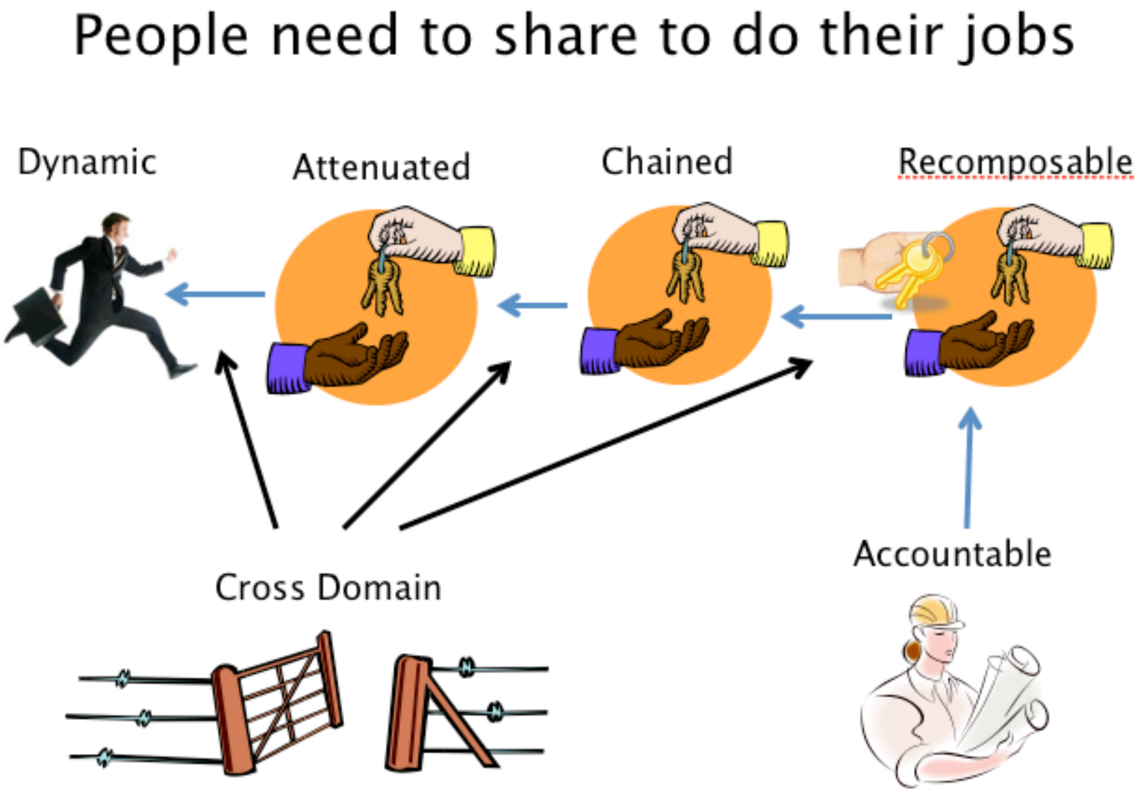
I-Brokers and the GRS

- When managing your i-name at an i-broker such as 1id.com or fullxri.com, those i-brokers make changes to your i-name by using the EPP protocol to talk to Neustar's central registry (GRS). This protocol is essentially also an XRD editing API (plus other things).
- In that API, <Service>s (<Link>s) have IDs. Those IDs are not exposed to the outside world, but can be used by an i-broker to delete <Service>s (<Link>s). The API has no methods for updating/replacing <Service>s (<Link>s), only for adding and deleting.

Session 12

Rich Sharing on the Web (12E)

URL: http://iiw.idcommons.net/Rich_Sharing_on_the_Web
Convener: Allen Karp



People need to share to do their jobs

Dynamic

Attenuated

Chained

Recomposable

Cross Domain

Accountable

XRI Resolution Using XRD 1.0 (12F)

URL: http://iiw.idcommons.net/XRI_Resolution_using_XRD_1.0

Convener: Drummond Reed
Notes-taker(s): Drummond Reed

Tags for the session - technology discussed/ideas considered:

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

About a dozen of us went over the protocol flow for XRI Resolution 3.0 – the new version of XRI resolution that will be based on the XRD 1.0 discovery/descriptor document format from the XRI TC.

The flow is very similar to XRI Resolution 2.0 (which used the previous XRDS format) except that it is significantly simpler with XRD. The key takeaways were:

1) From the standpoint of standard XRD libraries, such as we anticipate OpenID v.next will use, resolution of an XRI will look just like XRD discovery on a URI. All of the resolution steps will be hidden from the library because they will happen on the server side.

2) Even a true local XRI resolver should be able to use the standard XRD format, including the basic URI template defined in the Host-Meta spec (see Eran Hammer-Lahav's blog at http://hueniverse.com/ for links to all of these specs).

The next step is for an editing team at the XRI TC (most likely Drummond Reed and John Bradley) to produce a Working Draft 01 spec.

Where Should Identity Live (and how to control it)? (12G)

URL: http://iiw.idcommons.net/Where_should_Identity_Live

Convener: Andrew Arnott

Note-taker(s): Hannes Tschofenig

Tags:
Identity, IdP, service provider, token, assurance

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

Definitions

Entity - A person or device that should be discernable from another.
Identity - the minimal data necessary to discern between entities in a given context.

Terminology taken from ISO/IEC JTC 1/SC 27 N7751:

entity: something that has a separate and distinct existence

identity: total list of attribute values of an entity that allows this entity to be distinguished from other entities within a context and to be recognized in that specific context

some term needed for "context".

What identity is NOT

- Membership: identity is not controlled by an organization, and cannot be revoked by an organization. Membership or authorization may be revoked by a controlling party, but that is not identity.
- Authorization or (necessarily) access control: although an organization may control access to a resource, they do that by assigning or revoking privileges to an identity, and not by revoking privileges to assert that identity.

Ideals in Identity

- Roamability of the client: (most) users MUST be able to log into (most) services from any geographic place and from any device. An entity's possession is not always a requirement.
- *Portability of the IdP: The identity asserting service or device MUST be able to transfer that capability of assertion to another service or device. Or **Limited delegation of authority.***
- Rights of assertion: (some) users are willing to empower a trusted third party to assert their identity without aid of another party or device. Some services require multi-factor authentication. Some users will prefer to spread out rights of

assertion, such that an IdP and a physical user token are required at the client in order to assert an identity at an RP. Perhaps users will fully empower one IdP, while only partially empowering another.

- Multiple identities (persona): (some) users want or need to maintain multiple identities for individual services in order to avoid correlation or separate tasks.
- Correlation of identities: some users want to correlate their identity across services. Some services want or need to correlate the identities of their users. Some users do *not* want services to be able to correlate their identity across services. Some sites MUST NOT be able to correlate their users' identities across services.
- Phishing protection: identity SHOULD NOT be phishable. It's not that we mitigate against profitable phishing -- we make it impossible by using non-phishable credentials wherever possible. (non-correlatible)
- Verifiable assertions: An identity assertion can be verified by a service without a need to trust the IdP that sent the assertion (the IdP may not be the signing entity), and possibly without a network connection. Checking various identity revocation lists, if supported by a particular service, would require at least periodic updating of a cached list or a network connection.
- Non-collision of identities: an identity must be globally unique.
- Revokable only by entity: an identity, once created, can only be destroyed (or rather, the ability to assert that identity can only be destroyed), by the owning entity. The creator of an identity may also create a power of revocation that may be assigned to the entity, allowing the entity to terminate a compromised identity.
- Temporary revocation: Some entities may lose control of their identities (lost cell phone) but later recover it.
- Non-transferrable: Roles are transferrable -- not identity. Identities MUST NOT be reassignable to others, especially by accident. (exception: perhaps an organization does not want to expose that a change in the person filling some role has taken place).
- Non-enumerable: if a physical token maintains a user's identities and the services the user is a member of, physical access to that token should not enable someone to enumerate the services the user has come in contact with.
- Non-repudiation: (some) services may need to be able to prove that an identity was asserted to it. (some) users may need to prove that they visited some service.
- Level of assurance: Some services demand a certain level of assurance that an asserted identity is indeed originating from the owning entity.

Practical Details

- Identity may have metadata (attributes) associated with it (i.e. membership, roles, authorization, signed claims). Services may store metadata about an identity within the service, or may publish metadata to a shared service for which access control may be set, perhaps with user consent.
- These public identity-metadata correlation services may provide a service to search for identities with metadata that matches some criteria, thus allowing people to easily find identities based on traits known about a known entity.

- Some services do not need identity at all, but only claims (membership, roles, or other metadata) signed by a trusted identity in order to provide services to other entities.

Risks

- Denial of service: An evil entity that gains temporary control of an identity may obtain a revocation for that identity, which the evil entity may issue at a later date, after the identity's rightful entity regains control of that identity.
- Denial of service: A disruption of a service's means to verify new identities.