The 7th Internet Identity Workshop 2008b

November 10-12, 2008

BOOK OF PROCEEDINGS

Version 1

Notes Gathered by Heidi Nobantu Saul, Complied by Kaliya Hamlin

Notes in this book can be found online at
http://iiw.idcommons.net/Notes_08b

identity commons
working group

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

Table of Contents for IIW 2008b

INTRODUCTORY LETTERS

From Mary Ruddy – Chair of the Identity Commons Stewards Council

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

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

If you are not already doing so, I invite you to continue the energy sparked by IIW 2008b by joining one of our working groups. You can find a list of them and their descriptions at the end of this document and [http://wiki.idcommons.net/Working_Group_Descriptions online here]

I would like to thank all the stewards

* Chris Allen (IC Evangelism & Marketing)
* Charles Andres (Information Card Foundation)
* Bob Blakley (IdMedia, Photo Group)
* Peter Davis (SAML Commons)
* Pamela Dingle (Pamela Project)
* Nicholas Giovotovsky (Identity Futures)
* Kaliya Hamlin (Internet Identity Workshop)
* Iain Henderson (VRM)
* Jeff Hodges (ID-Legal)
* Fen Labalme (Identity Rights Agreements)
* Dale Olds (OSIS)
* David Recordon (OpenID)
* Drummond Reed (XDI Commons)
* Chris Reynolds (Newbies4Newbies)
* Mary Ruddy (Higgins)
* Denise Tayloe (Kids Online)
* Paul Trevithick (Identity Gang, Identity Schemas)
* Bill Washburn (XDI.org)

For their active participation that makes this community thrive.

Looking forward to seeing you at IIW 8 (2009a)!

=mary.ruddy Chair of the Identity Commons Stewards Council

* Skype: mary.ruddy
* Y!: maryruddy2
* P: 617-290-8591
* E: mary at mersitic.com

'

From Kaliya Hamlin – Co-producer and Facilitator of IIW

This document comes at a real milestone for the IIW community. The Internet Identity Workshop is now three years old and the Identity Gang that it grew out of has been meeting for four years. Many members of the community have been working on aspects of the community vision for many more years before that.

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

We would not be here today without the contributions of some key people and communities.

* The original founders of Identity Commons Owen Davis and Andrew Nelson along with early pioneers working with them including Fen Labalme, Victor Grey, Nicholaj Nyholm, Bill Washburn, Drummond Reed, Joel Getzendaner, Andy Dale, Christopher Allen, Mike Mell, and Eugene Kim.

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

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

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

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

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

The Internet Identity Workshop would not be possible with out the community that gathers or the sponsors that help support our gathering. These were the sponsors for this Internet Identity Workshop and OASIS IDTrust and the Information Card Foundation sponsorship went particularly to support the Documentation Center where the notes were collected.

We wouldn't be here without the contributions of all of our sponsors over the past 3 years.

* AOL
* Novell
* Microsoft
* British Telecom
* Liberty Alliance Project
* Ping Identity
* Plaxo,
* Vidoop
* Google
* Adobe
* Cisco
* OASIS IDtrust
* CommerceNet
* SXIP
* Higgins Project
* Bandit Project
* Rel-ID
* Symplified
* Applied Identity
* Ouno
* Information Card Foundation
* Authentrus
* Planetwork
* ClaimID

Here is a brief explanation of how IIW works and what this book contains.
On Monday we host an introductory afternoon where industry leaders are invited to present about core technologies that relate to user-centric technology. Attendees are also give a one pager packet that contains summaries of all the different projects in the community. The list and most of the one pagers can be found on this page. You will find the copy and some slides excerpted of the presentations at the start of this packet

Tuesday morning we gather all together to create our agenda for the next two days. The methodology we use is called Open Space Technology and any one in attendance can put forward a topic for discussion, an idea they want to present or a question they hope to get answered. They are written on 8.5x11 paper and posted on two paper covered walls. Over the course of two days we have ten one hour sessions. Notes were taken at virtually all of them and this book of proceedings contains those notes.

Each session has a title, a convener, the notes taker and a list of attendees. We list the people who signed the sheet saying the attended the session so if you know them and want to know more about what happened you can ask them. All these notes can also be found on the wiki and each session has its own page there - this is so you can to make changes and add updates. If you need a web reference to blog about some of the things in here please use the URL for the session to link to the material.

At the closing of Wednesday we do an open awards ceremony and the awarders along with the reason for their giving to the awardee is listed at the close of the proceedings.

We encourage blogging in the community - the tag for this event is IIW2008b & IIW. If you have a blog and would like to be included in the community blog Planet Identity http://www.planetidentity.org - just make a request to Pat Patterson.

We also have a by request community mailing list that is google group
http://groups.google.com/group/idworkshop that you are most welcome to join.

Identity Commons is an active community with many groups working on the social, technical and legal aspects of an identity layer of the web. Please read the list of groups that are at the end of the proceedings you would be most welcome to join any that are working on topics of interest to you. If there is a topic that you think it important and would like to see it be part of the community it is also possible to start a new group or have an existing group/entity become an active part of this community too. Myself, Mary Ruddy or any of the Stewards can answer questions you might have.

I look forward to the coming six months, until the next IIW May 18-20, 2009 and the events in between where we will meet and continue to move this industry forward.

Regards,
=Kaliya Hamlin

* Blog: http://www.identitywoman.net * Tiwtter: identitywoman
* IM - Skype: Identitywoman, Y!: earthwaters, AIM: kaliya@mac.com
* Phone: 510 472-9069 e-mail: kaliya@mac.com

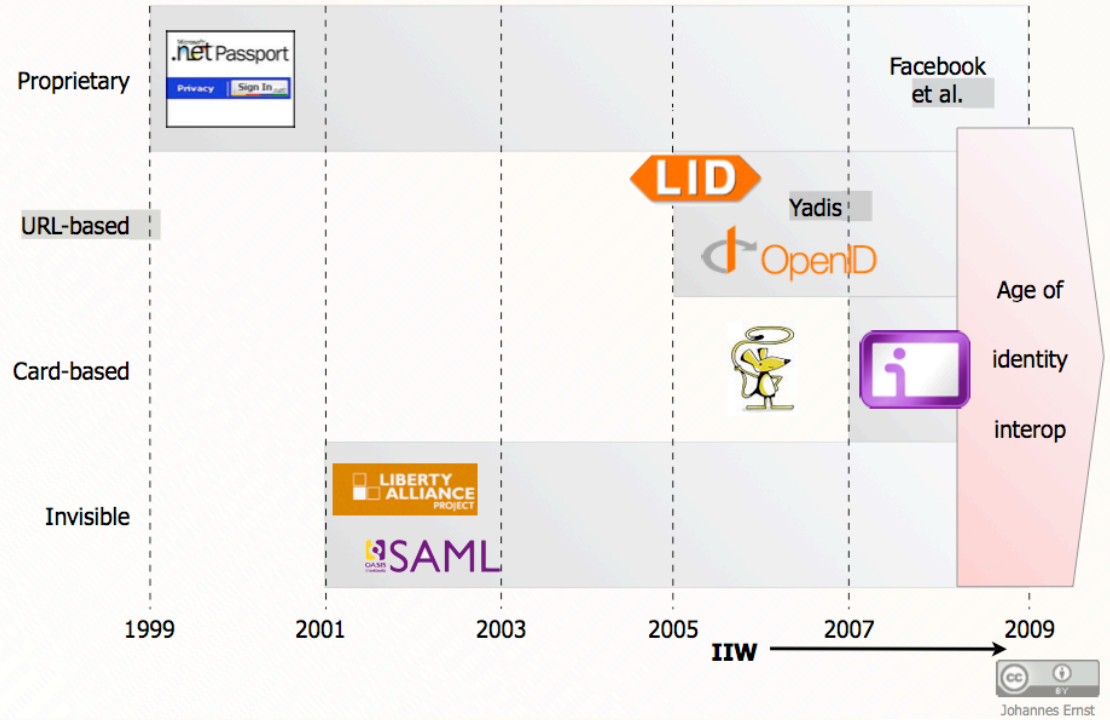
MONDAY – Introductory Talks

Identity Overview – Johannes Ernst

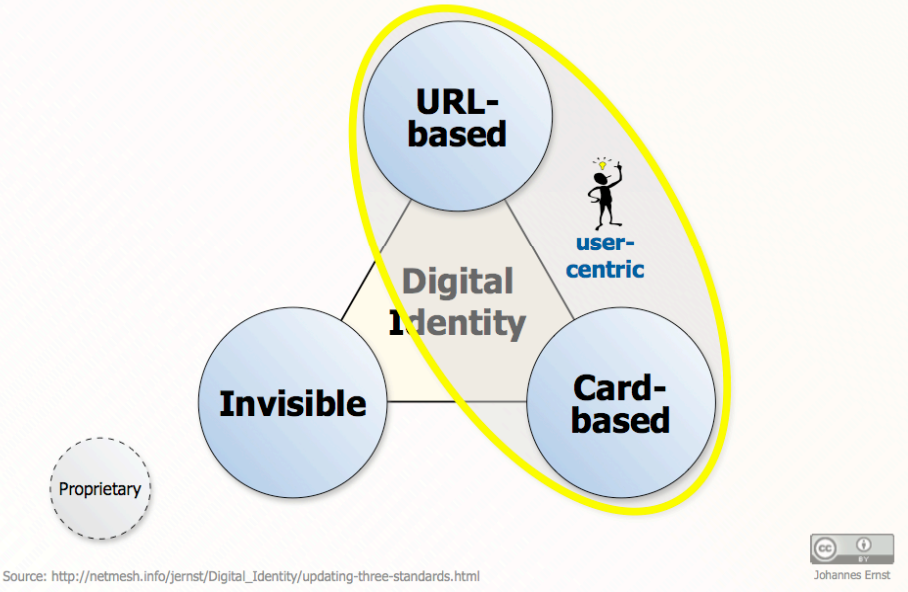
URL http://netmesh.org/slides/IIW2008b/NetMesh-IIW2008b.pdf

Johannes Ernst NetMesh Inc. http://netmesh.info/jernst
Internet Identity Workshop IIW 2008b

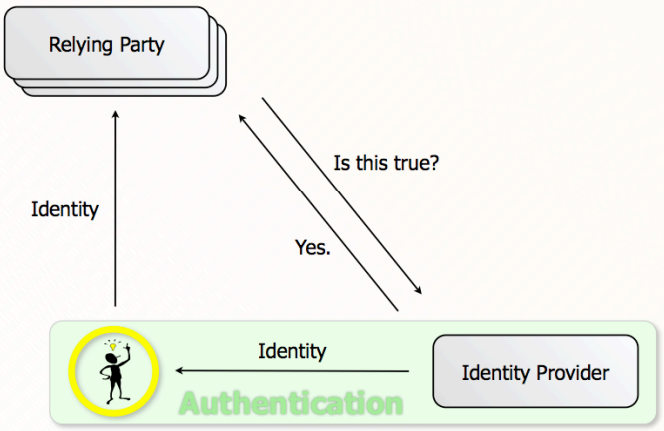
Modern Identity History



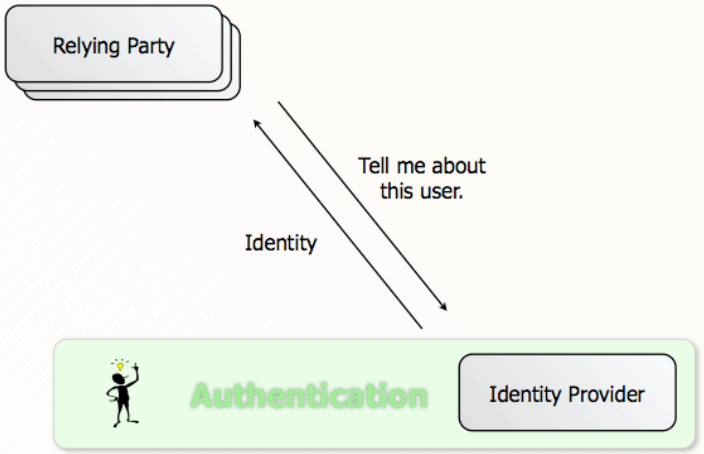
Identity's Three Pillars



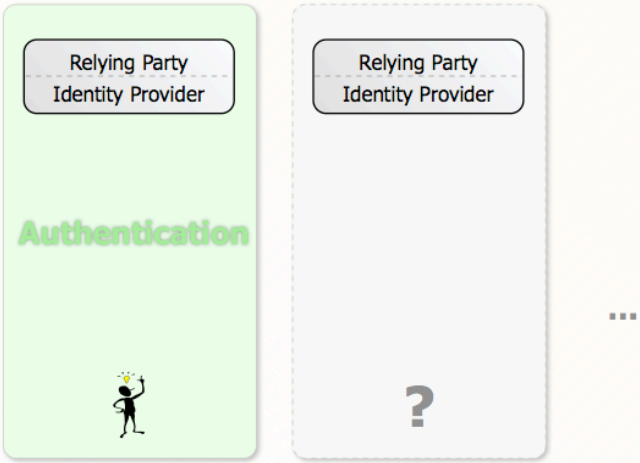
The Basic User-Centric Flow



Comparison: Non-User-Centric Flow



Comparison: Stovepiped Identity



Who is this guy speaking right now?

Please enter your OpenID here:

http://netmesh.info/jernst

- globally unique user name, no name conflicts
- is also a link
- many value-added services a springing up, example:
  - Technorati
  - del.icio.us
  - Identity aggregators like claimid.com
  - Google social graph API

About Myself

- Founder/CEO NetMesh Inc.
- Pioneered URL-based digital identity with LID™
- Board member, OpenID Foundation
- Co-initiator, Open-Source Identity System (OSIS)
- Co-initiated Yadis, the first user-centric identity convergence project
- Advisory board member, Health 2.0 conference
- Contributor to UML; initiator of the Object Management Group's RT-AD effort
- BMW, FZI, MSR, Integrated Systems, Aviatis
- World Economic Forum "Technology Pioneer"
- Doctorate, EE

- Frequent speaker: Digital ID World, European Identity Conference, Comdex, PC Forum, Mix, OSCON, ETel, SDForum, UML World, Emerging Communications, Harvard, World Econonic Forum...

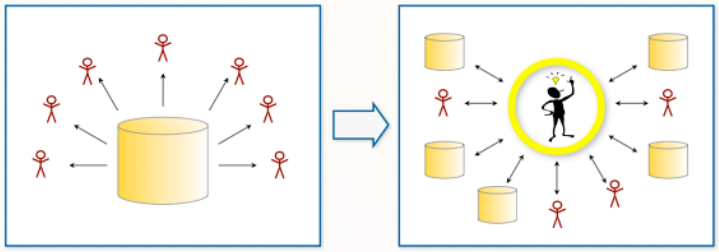
Johannes Ernst

http:/

"My users will keep entering all the information that I ask for."

"They always have, I don't see the need to do anything."

"Users in Charge" (Esther Dyson)



Industrial mass production model

Web 2.0, user-centric model

Kim Cameron's Laws of Identity

1. User Control & Consent

- ...only reveal information identifying a user with the user's consent

2. Minimal Disclosure for a Constrained Use

- ...discloses the least identifying information

3. Fewest/Justifiable Parties

- ...disclosure of identifying information is limited to necessary and justifiable parties.

4. Directed Identity

- ...both "omnidirectional" and "unidirectional" identifiers, thus facilitating discovery while preventing unnecessary release of correlation handles

5. Pluralism of Operators & Technologies

- ...enable the interworking of multiple identity technologies run by multiple identity providers.

6. Human Integration

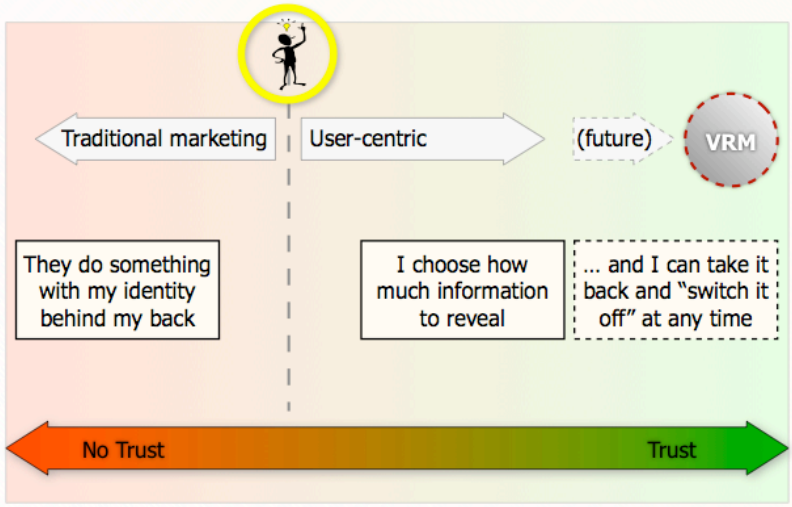
- ...human user to be a component of the distributed system integrated through unambiguous human-machine communication

7. Consistent Experience Across Contexts

- ...simple, consistent experience while enabling separation of contexts through multiple operators and technologies.

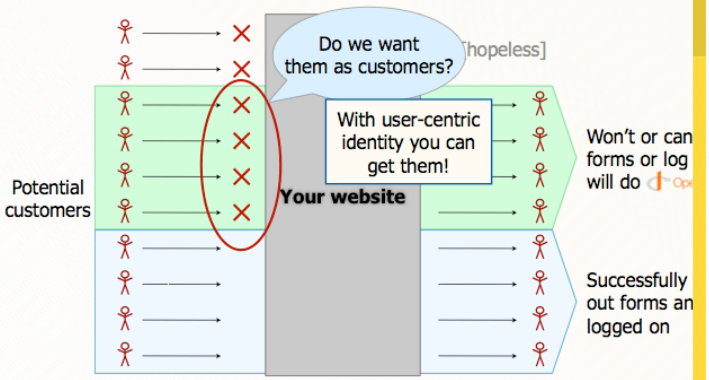
Source: http://www.identityblog.com/stories/2004/12/09/thelaws.html

Customer Trust



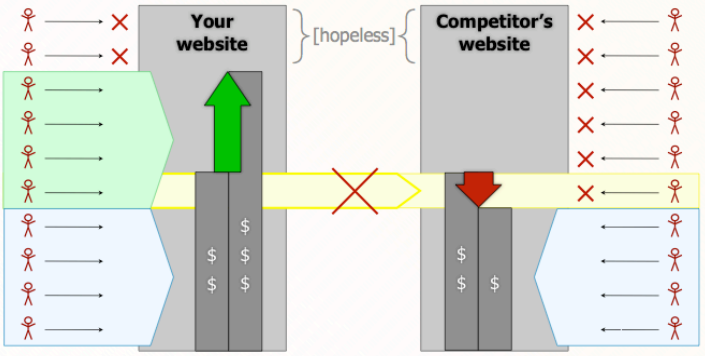
Johannes Ernst

Net Result: More Business



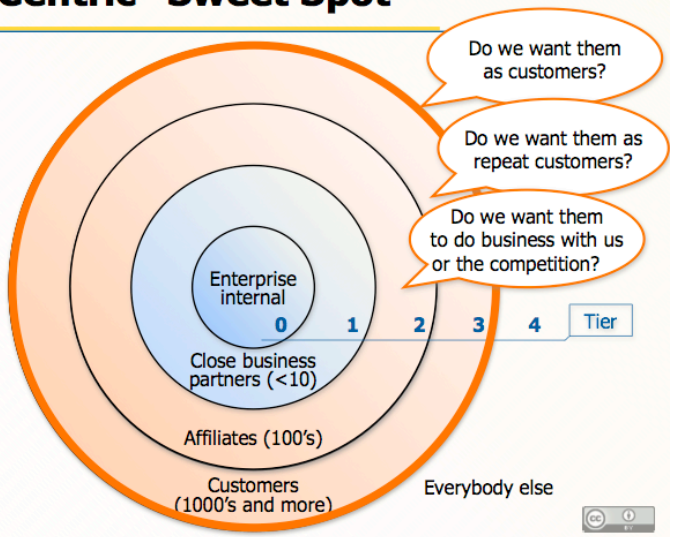
Johannes Ernst

Competitive Effects



Johannes Ernst

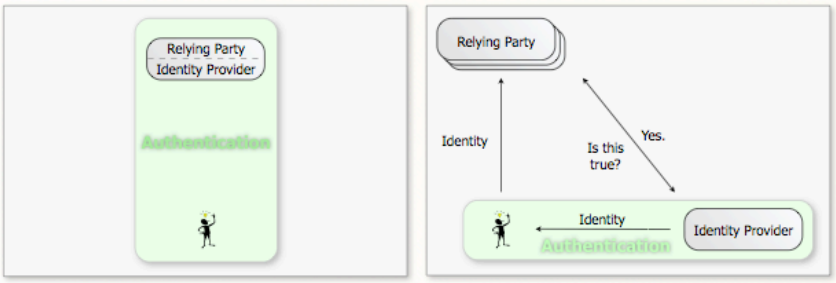
User-Centric "Sweet Spot"



Source: http://netmesh.info/jernst/Digital_Identity/concentric-circles-2008.html

Johannes Ernst

Outsource Authentication



Cost (old-style):

Password management
+ Password reset
+ Anti-phishing
+ Backup tape risk / management

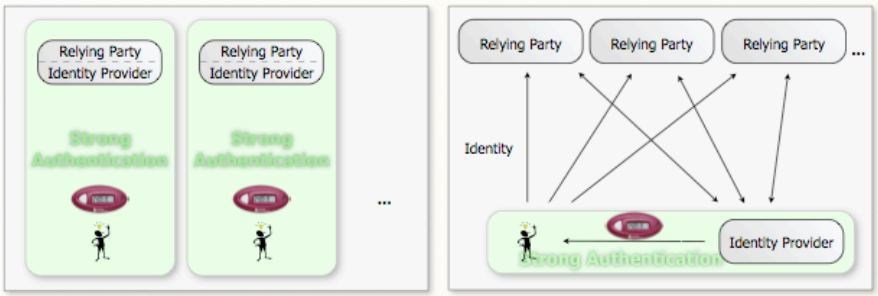
$$$ or €€€

Cost (user-centric):

Key/secret management
+ ~~Password reset~~
+ ~~Anti-phishing~~
+ ~~Backup tape risk / management~~
+ free authentication from major IdP

$$ or €€

Affording Strong Authentication



"Shared token"

- All relying parties benefit from the added security of the same token
- Higher security at lower cost through cost sharing, enabled by internet-scale common protocols
- Much more convenient for the user: one token, not N
- Works the same for other strong auth:
  - voice,
  - biometrics,
  - client certs etc.

Internet Identity Workshop
IIW 2008b

Thank you for your time!

Johannes Ernst
NetMesh Inc.
http://netmesh.info/jernst

OpenID – David Recordon

* Heard of OpenID?
* Have an OpenID?
* Used OpenID?
* Use OpenID?
* OpenID says who and describes where
...to find my services and data

* This week John, Joseph and I shot an episode of TheSocialWeb.tv (Episode 16: "OpenID's Historic Week: Microsoft and Google Go Live") with Eric Sachs from Google's Security Team. Eric's team implemented Google's OpenID Provider and we ended up with a very interesting episode where he talks about some of the background going into why they chose OpenID and challenges they see needing to be solved in the future.
VIDEO http://daveman692.livejournal.com/342212.html

* Magnolia OpenID login with Yahoo!

* BaseCamp allows sign-in with OpenID

* 37 Signals products, Highrise, backpack and Basecamp can all be linked together using OpenID. They have something called the Open Bar that helps you navigate between them.

* Plaxo lets you login with OpenID

* Google Analytics mention of OpenID with key events listed.

* Screen shot of all the logos

* "The next phase of developer adoption will not be measured in the number of OpenIDs or sites that support it, but rather user experience, accessibility, and seamlessness of integration into a wide variety of applications and experiences." —David Recordon (O'Reilly Radar '08)

* Building on the New "Open Stack"

* screen shot of **pinax,** *a platform for rapidly developing websites*

*** OpenID Foundation**
The OpenID Foundation is a membership organization for individuals and organizations that facilitates the development of OpenID technologies, ensures the technology is open, and promotes the technology.
•Non-profit organization with a board composed of individuals from the community and companies
•Mainstream media attention toward OpenID
•New specifications being created (PAPE)
•Range of members from individuals to enterprises

*** OpenID Content Provider Advisory Committee Kickoff Meeting**

HTTP://OPENID.NET/2008/10/01/OPENID-CONTENT-PROVIDER-ADVISORY-COMMITTEE-KICKOFF-MEETING/

A couple of weeks ago the BBC hosted twenty-six people from seventeen organizations including eight OpenID Providers and eight OpenID Relying Parties (sites which accept OpenID logins) in New York City to kick off an OpenID Content Provider Advisory Committee. The goal of the session was to answer specific questions by the Content Provider community (media companies and national affinity groups) as well as to provide feedback to the OpenID Foundation, its member companies, and the wider community on the future direction of OpenID.

* **The First OpenID User Experience Summit**

http://openid.net/2008/10/21/the-first-openid-user-experience-summit/

As OpenID continues to gain momentum, over the past few weeks both Google and Yahoo! have released the results of usability studies they've done around OpenID and digital identity systems in general. Google released their Usability Research on Federated Login looking at how to create user experiences that mainstream users can understand when using one account to login to other websites while Yahoo!'s OpenID Reasearch focused much more on how their own users are able (or not yet able) to understand what OpenID is and how they can use it. While at first glance this might seem troubling, instead it is actually one of the steps in the natural evolution of seeing a technology start to go from intriguing the early adopters to working on crossing the chasm to mainstream usage.

* **OpenID Europe**

PURPOSE: PROMOTE OPENID IN EUROPE ENSURE A EUROPEAN VOICE IN OIDF

Initial focus: Secure Trademarks and domains
Existing National Chapters:
- OpenID France (OIDFR)
- OpenID Portugal (OIDPT)
- OpenID Schweiz (OIDCH) - Switzerland
- OpenID Türkiye (OIDTR) - Turkey

Planned National Chapters:
- OpenID Sverige (OIDSE) - Sweden
- OpenID Polska (OIDPL) - Poland
- OpenID România (OIDRO) – Romania
- OpenID Denmark (OIDDK) – Denmark

* **European Status and Issues**

•Privacy
•Efforts (still) on a national level, but looking forward to exchange of best practices
•Alignment with European E-ID and possibly Kid-ID's
•Multiprotocol solutions (OpenID + SAML)_
•Lower barriers to implement OpenID2 RP (ensure not to loose developer enthusiasm)

* **OpenID in Japan**

• OpenID Foundation Japan Activity
• Now "OpenID" catches the Wave
• Lots of media attentions (30% aware of OpenID)
• 32+ Corporate Members (Financial / Marchant / Telco / etc.)

• Partnership with Liberty Japan SIG
• Trust Extension (TX)
• SSO & Payment Solution for Japan Airline's Partners Program
• Hotel, Car Rental, etc.
• TX Provides Trusted Messaging for Sensitive Information
• The Site Handles over 4000 Transactions ($50-$1000/tr) per month!
• Banks & Telcos considering using it right now
• About to form the new Working Group
• Join the discussion during IIW!

*** OPENID AUTH 2.1**

•Backwards compatible with 2.0
•Specification cleanup and errata from 2.0
•Appendix focused on security
•Updated discovery as XRDS has evolved
•Clarifications around XRI support and best practices
•Possible exploratory work with emails as identifiers and OAuth signature mechanisms

* **Questions?**
http://OpenID.net/
david@sixapart.com

SAML – Paul Madsen

http://docs.google.com/Presentation?id=d57zf97_8892qdkc7ck

* SAML & Liberty ID-WSF
Paul Madsen
IIW 2008b

Federated?
* Federated identity allows a pair of service providers to agree on a way to refer to a single user, even if that user is known to the providers in different guises.
* Often, federated identity is achieved through the linking together of the user's 'accounts' at both providers
* Also
- o no account at service provider
- o linkage based on attributes
- o mechanisms to constrain collusion

What is SAML?
- According to its designers, it is:
  - "an XML-based framework for marshaling security and identity information and exchanging it across domain boundaries"

* Strives to be the "universal solvent" of identity
* Has out-of-the-box profiles for interoperability, but can be extended and profiled further
* Driven primarily by 'serious' scenarios where trust, liability, value, and privacy are at stake
- o B2B, B2C, G2C...

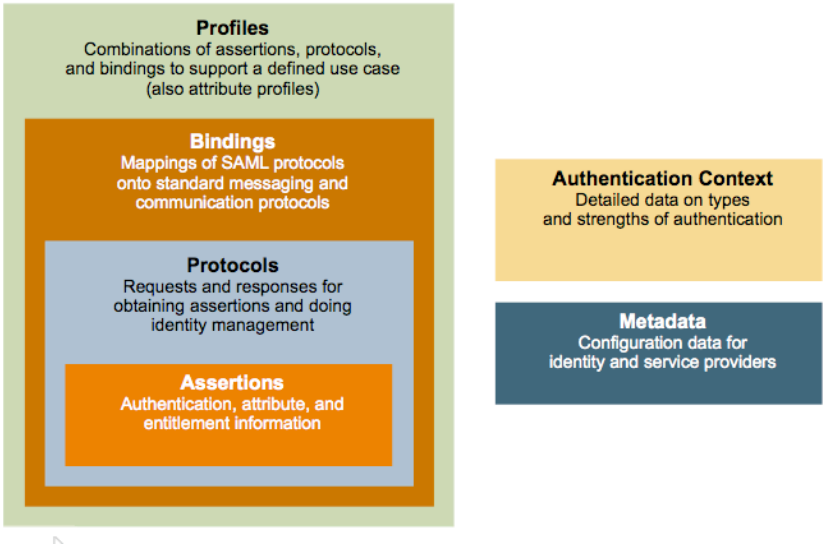
Where is SAML used?

* Telcos, financials, aerospace, Saas...
* Google Apps acts as a SAML SP to its customers
* Shibboleth for higher education
* Governments around world (US, NZ, Denmark, etc) for SSO
* As a key security token formt for
    o Liberty ID-Web Services Framework
    o for WS-Trust/WS-Sec and applications that build on them (e.g. Infocards)
- Microsoft Geneva (NEW)

At SAML's core: assertions

* An assertion is a declaration of fact...
    o ...according to someone
    o You have to determine if you trust them
* SAML assertions contain one or more statements about a subject:
    o Authentication statement: Joe be authenticated with a smartcard PKI certificate at 9:07am today
    o Attribute statement (which can contain multiple attributes): Joe is a manager and has a £5000 spending limit
    o Authorization decision statement (use XACML instead for more than simple needs here)
    o Your own customised statements...

SAML components and how they relate to each other



Single Sign On

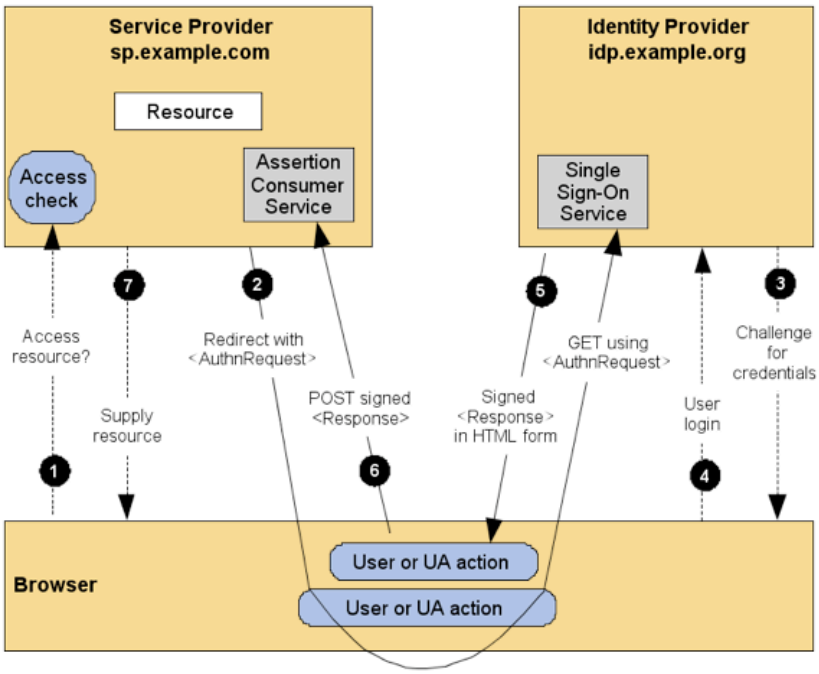
* Single Sign On is perhaps the most typical application of SAML
* Interoperability specified by Web SSO profile specification – constrains assertions and protocols for this use case
* User authenticates at IDP, which then asserts this fact to an SP (or more).
* User then able to access SP resources without additional presentation of any credentials they may have there
* Other attributes may be transferred as well.

SSO permutations

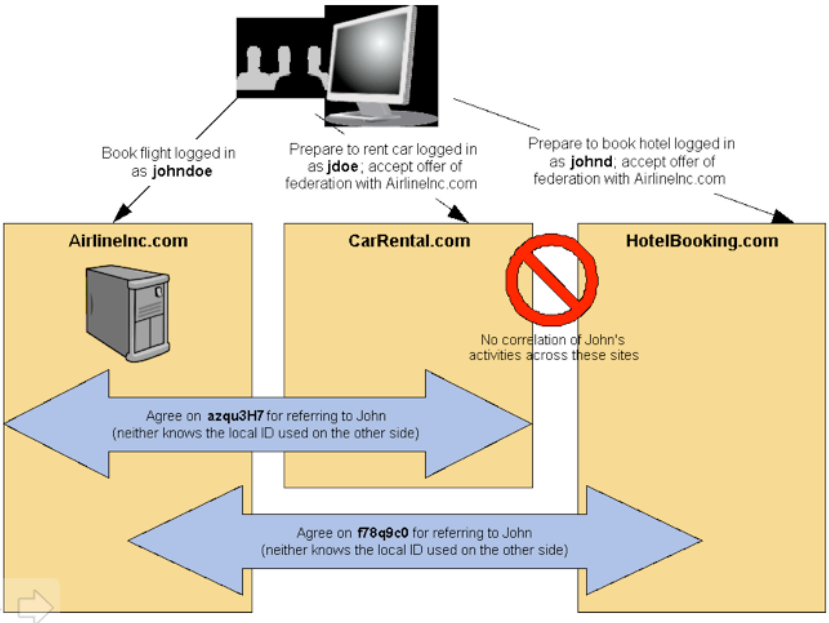
* Does user visit the IDP or the SP first?
    o if user starts at SP, it has to explicitly request info from the IDP
    o The SSO assertion has to be conveyed from IdP to SP regardless, using a response message
* If the SP makes a request, does it push (HTTP POST), allow to be pulled (“artifact”), or use HTTP redirect for the request?

* Does the IDP push (HTTP POST) or allow to be pulled (“artifact”) the response?
* Let's see...carry the two...that's eight options
    o But some are more common than others

SP-initiated/redirect/POST



Pairwise identity federation

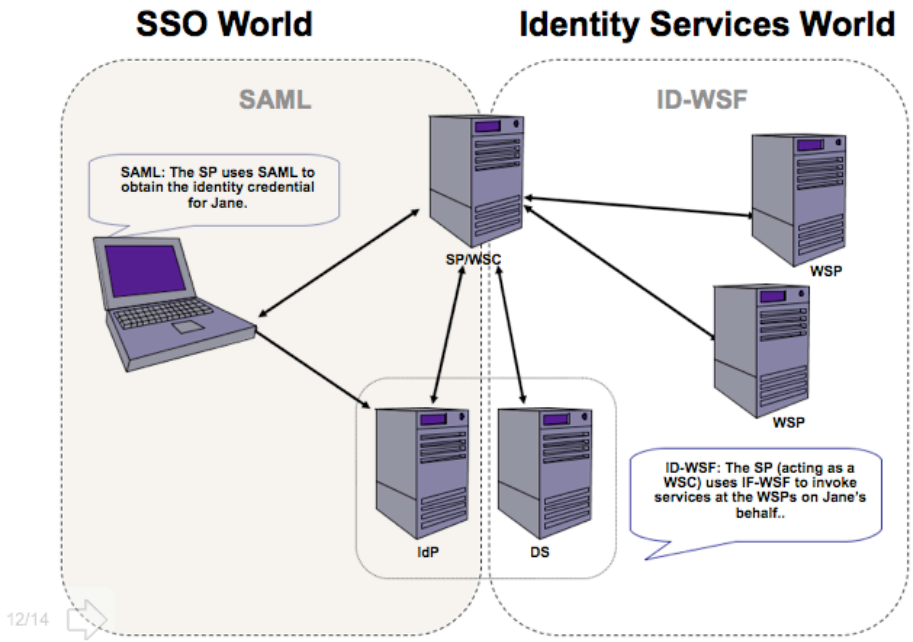


Liberty ID-WSF

* A SOAP-based framework for locating and invoking identity based Web services
* Identity-based Web services:
    ARE ASSOCIATED WITH A PRINCIPAL'S IDENTITY (E.G. MY CALENDAR SERVICE)
    - Typically invoked using a Principal’s Identity
    - ID-WSF
* Permissions-based Attribute Sharing

INVOKING SERVICES UNDER CONTROL OF USER
SERVICE REQUESTOR DOING SO ON BEHALF (EITHER DIRECTLY OR INDIRECTLY) OF USER.

SAML and ID-WSF together



ID-WSF evolution

ID-WSF is being pulled in multiple directions

* Simplicity – WSF Simple removes some of the full functionality in favour of simplicity. Matching conformance profile will lower barrier for vendor implementation
* REST/SOAP – ID-WSF Restful Binding binds functionality to HTTP rather than SOAP. Hopefully more compatible with OpenID &Oauth etc
* WS* - WEB SERVICES HARMONIZATION ACTIVITY EXPLORES HOW WSF CAN BETTER LEVERAGE WS* COMPONENTS (IN ADDITION TO WS-SECURITY & WS-ADDRESSING). LIKELY TO MEAN FORMATION OF NEW OASIS TCS FOR TECHNICAL WORK.

Resources

* SAML specs and outreach info: http://www.oasis-open.org/committees/security
* Liberty deployment guidelines: http://projectliberty.org/resources/guidelines.php
* SAML/Liberty Federation adoption info:
* Paper on Liberty Federation in Enterprise Outsourcing:
  http://www.idealliance.org/proceedings/xml05/abstracts/paper154.html
* Aggregation of many popular identity weblogs: http://www.planetidentity.org
* Some open-source projects involving SAML:
  http://OpenSSO.dev.java.net http://www.OpenSAML.org
  http://www.SourceID.org http://Lasso.Entrouvert.org
  http://ZXID.org

Information Cards – Charles Andres

http://www.informationcard.net/files/Presentations/InformationCards-36.ppt

Information Cards

ON THE INTERNET, NO ONE KNOWS YOU'RE A DOG;

… and that's a problem, because you can't prove you or you

- Businesses don't know who their online customers are
  - They mitigate risk by asking for and storing multiple personal identifying information
  - This adds the risk of a data breach…

…Which increases as the traditional enterprise "walled garden" is poked with holes from outsourced services, international sub-contractors, etc.

Usernames, passwords are out of control

Every site with value or valuable transactions requires a username/password.

- Username is often an email address
- Password is most often:
  - Always the same
  - Too complex to recall
  - Not used often enough to recall
- Email addresses proliferate spam probability
  - Users fight back with junk filters (which can block desired email) and still more email addresses
- Users allow their browsers to remember their passwords…
  …but these can be easily stolen.
  Others call up a spreadsheet that lists them all. But how well does that work?
- Frustrated customers ask: is all this really necessary?
- WWILF?
- It took so long to get here, I forgot what I going to buy.

We have made the Internet safe for Criminals

- Phishing Attacks
- Without a consistent user ceremony, users don't know what to expect.
- Phishers take advantage of this naïve confusion.

How do Businesses stay up to date?

- Users information changes
- Only the user knows what changed
- The user has to proliferate a changed address to hundreds of providers.
- How many notifications do you have to make everytime you move?
- How do you know you got them all?

How did this happen?

Back in the 20th Century…
In the computer lab, identity was not a big issue. Separate accounts with a name and password were enough.

But the network had begun

When the network were all known computer labs, it wasn't a problem…

- No financial transactions
- Trusted vetted community

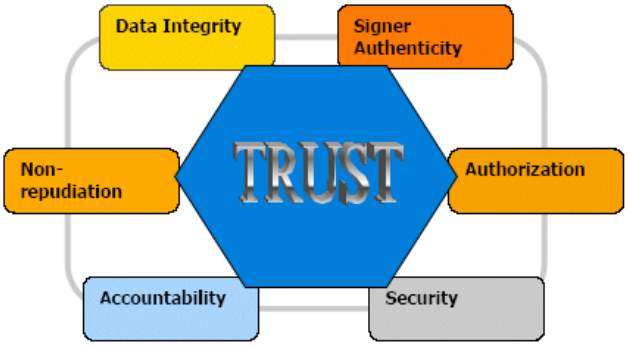
Shopping on the Internet wasn't imagined

ONLINE SHOPPING SURVEY: CONVENIENT BUT INSECURE

…let alone deliberate attacks…

Trust is essential to doing business

- Without data protection, there is no accountability
- Without accountability, there is no trust
- Without trust, there is no:
  - Commerce
  - Personal Welfare
  - Society
  - Financial system
  - Freedom
  - Peace
  - Order



If Businesses can't trust, they ask for more data

- No one can believe the claims you make.
- Your personal data continues to replicate out of your control
- There are no trusted verifiers, so businesses have to do it themselves.
- Businesses ask for more data every year as the criminals get smarter, data proliferates, as part of the risk aversion.
  - CC#:
    Exp Date:
    Secret Code:
    Billing Address:
- Yet fraud continues to increase, which costs all of us.
- And yet, more and more personal information is stored by businesses….

…until…

Data Breach: Everyone's Issue

Dear Mr. Andres:

"Your Investment Bank and **Trust** Company regrets to inform you that a contractor we hired lost your Social Security Number while traveling to Chennai, India. We regret any inconvenience this may cause you…."

- TJX Breach estimated to cost $2.7Billion
- Hannaford Data Breach
- UK Government admits losing personal data on 16 million Britons

Password Management is Everyone's Issue

- Same password everywhere?
- Different one everywhere?
- 8 characters minimum? Alphanumeric?
- How often do you change them? Are forced to by your IT policies?
- Where do you keep your passwords?
  - In your PDA?
  - In a spreadsheet?
- What if you travel?
- What if your laptop is stolen? Or has an HDD crash?
- How much time do you spend dealing with security and access issues?
- Multiply that by several billion…

Problems to solve

Users

- Make it easier
- Make it safer, more secure

- Minimize passwords -- reduce to one (or less)
- Allow anyone to have multiple personas (keep professional and personal life separate) (Religion, politics, private matters)
- Control the copies of and access to your personal identifying information

Businesses

- Lower Fraud rates
- Make Phishing much harder
- Lower data breach opportunities
- Get more timely data from customers (address changes, etc.)

Lower costs for password resets, customer complaints,

- A simple method that follows a predictable known method
- Familiar to us
- Compatible -- Works with existing sign-on systems
- Is flexible for both low and high security situations
- Is not controlled by one company
- Is not centralized by the government
- Is flexible to meet today's and tomorrow's business needs
- Less personal data proliferation

Everyone seems to have your data, except you

But how?

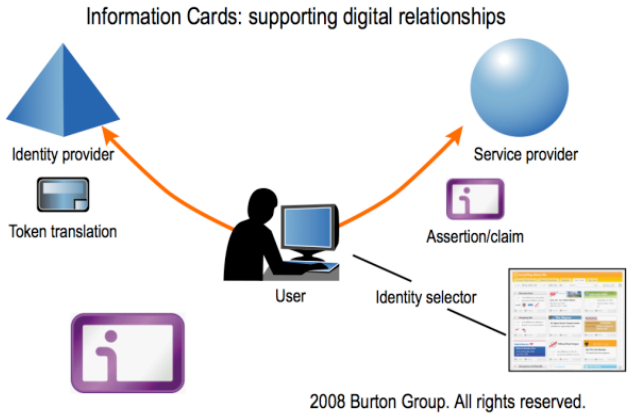
We all need:

Information Cards: The digital equal to your real world experience

- A Familiar Metaphor: Wallet and Cards
  - Psst!: (There is no wallet, there are no actual cards)
  - And There is no personal data on the cards

But to a user, they act like a wallet and cards only better

Wield the claims others make about you



Information Card Basics

- Cards have claims (name, address, etc.) associated with them
- Claims may be high or low value
  - Low Value: username
  - Middle Value: member ID, I'm over 21
  - High Value: Financial Transaction information
- Cards may be either (or both)
  - Self-asserted Claims
  - Managed Claims from an Identity Provider
- Card Selector (aka digital wallet) can be intelligent
  - Only show the cards with claims that match a website's Requirements
    - Retail Website = Service Provider = Relying Party
  - Phishing warnings
  - Handle multiple personas: Shopping You, Travel You, Hobby You, Professional You

CLICK IN

- There when you need them; invisible when you don't.
- 1x setup (need to associate card with website account (relying party))
- No username or passwords to remember
- No forms to fill out -- just present the card or cards

One or more cards hold all the data you now type and type and type in again and again

Trusted Verifiable Claims

- I claim to be: joe-sixpack423 and UPS, Bank of America, and the NY RMV will vouch for me. Today. Right now.

- Who lives at: an address that UPS knows where to deliver to (according to UPS)
- Who pays: his bills and is good for this transaction (according to Bank of America)
- Who is over 21: (according to the NY Registry of Motor Vehicles)
- Now please sell me that bottle of Neuf du Pape at the price we agreed, B of A will transfer the money, and UPS will pick it up - send to Account #12-4872733
- You don't need any more information about me.
- However, if you would like more information, I would be willing to give you marketing data useful for future business in return for a discount. I am open to a mutually beneficial business-to-business relationship.

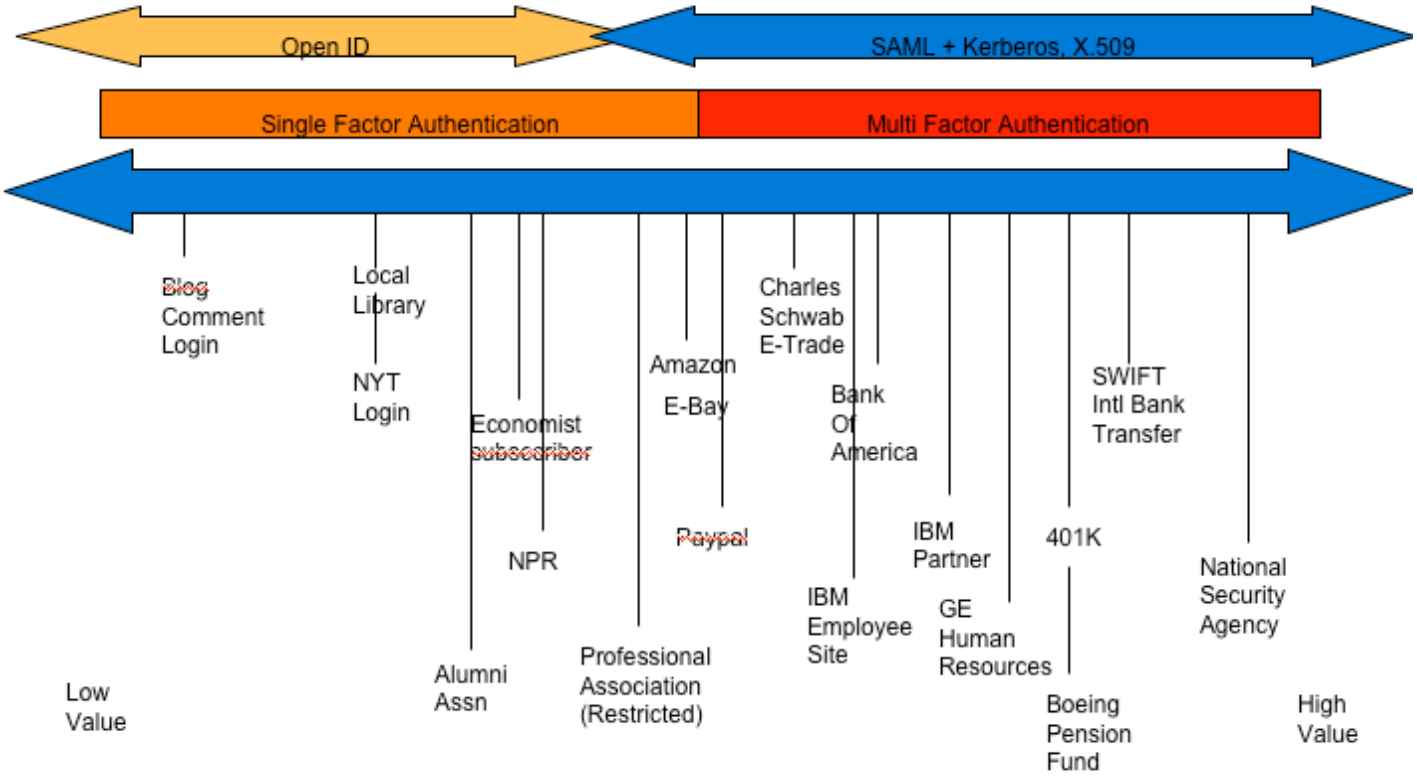
The new Digital Relationship Model

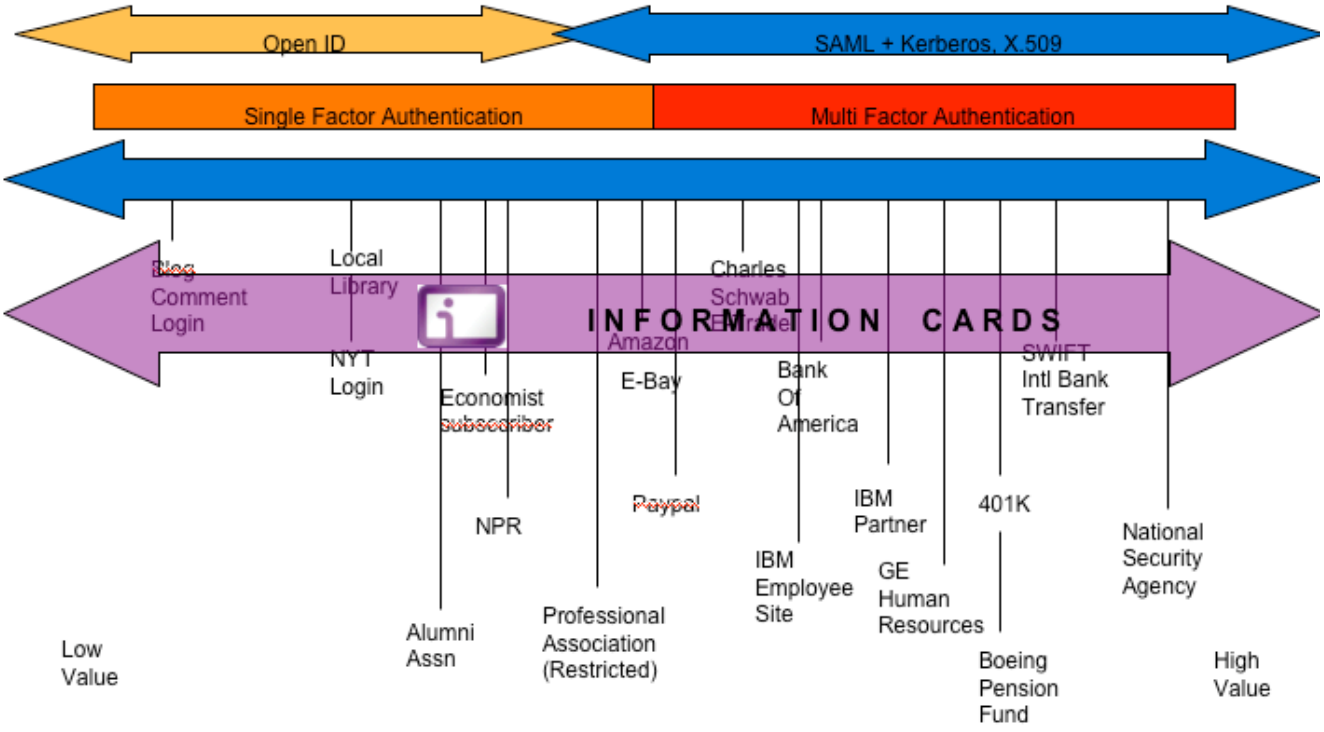
- Mutually beneficial relationships between parties:
- Business to business
- Buyer and seller
- User and Service Provider

User initiates transaction

- Each User has their own personal data storage system
- User controls what claims to reveal to a relying party
- Persistent Connection as long as both parties agree
- Not dependent on e-mail addresses
- Less personal data proliferated
- Less fraud risk
- Less data exposed to data breach risk
- Opt-in Relationship opportunities for trusted parties
- Better and more consistent customer connections

Dynamic Range of Security Requirements





Card Selector = Wallet

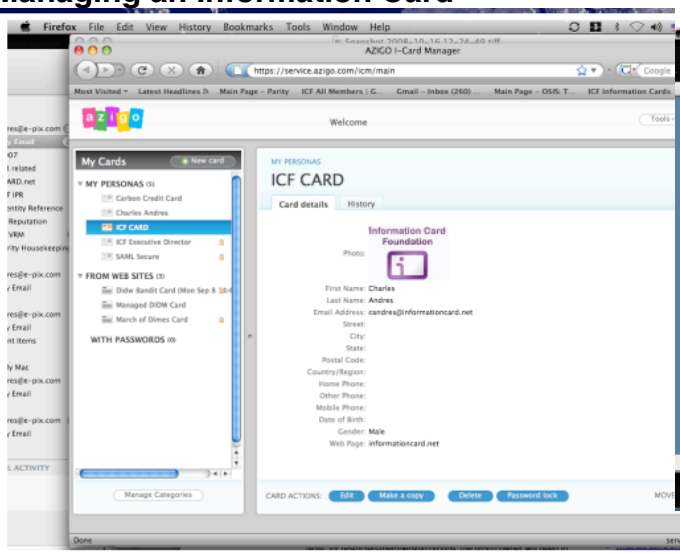
- Card Selector access -- may be protected by:
  - one password or
  - 2 factor (auth device + password)
- Cards may be protected by:PIN

2 factor (+ auth device or Sitekey)

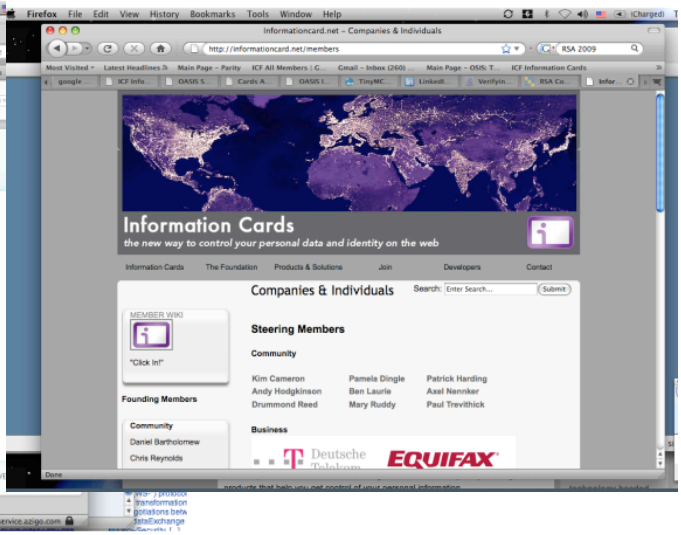
Managing an Information Card
Securing a single card
Card Selector = Wallet

- Card Selector access -- may be protected by:
  - one password or
  - 2 factor (auth device + password)
- Cards may be protected by:PIN
  - 2 factor (+ auth device or Sitekey)

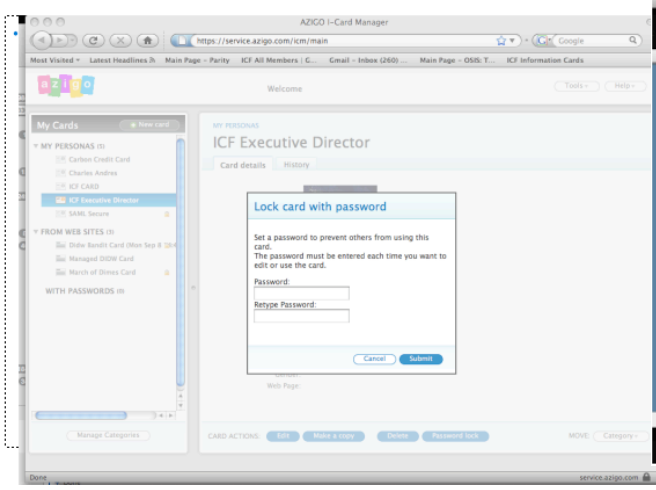
1 Managing an Information Card



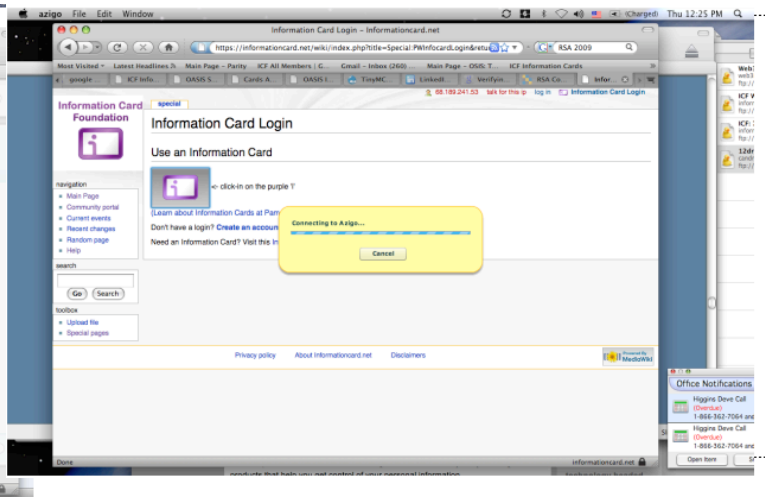
4 Clickin not Login



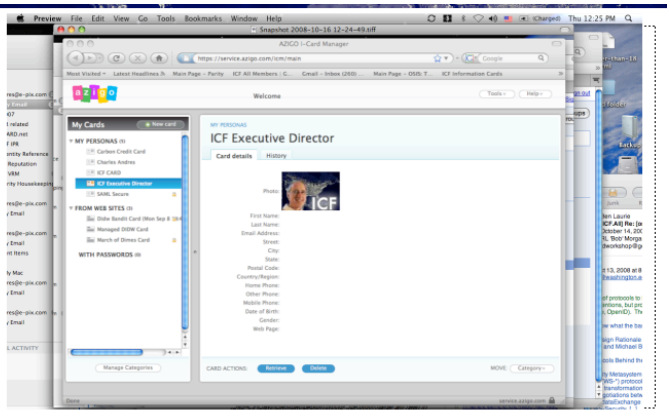
2 Securing a single card



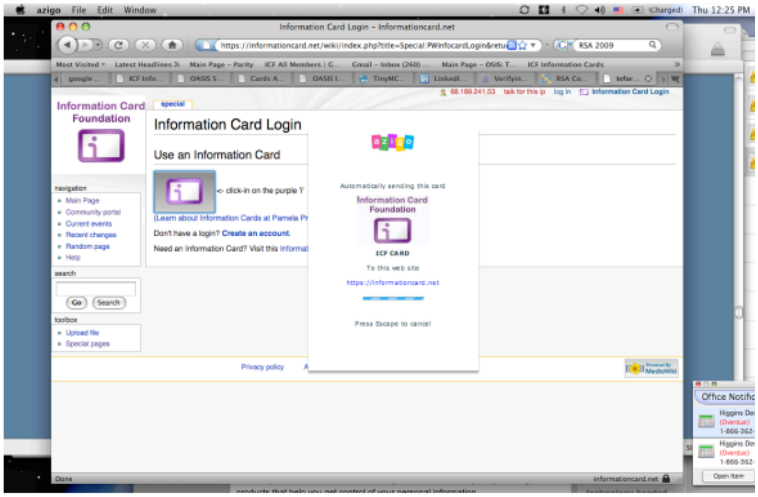
5 Calling up a Selector from the Cloud…



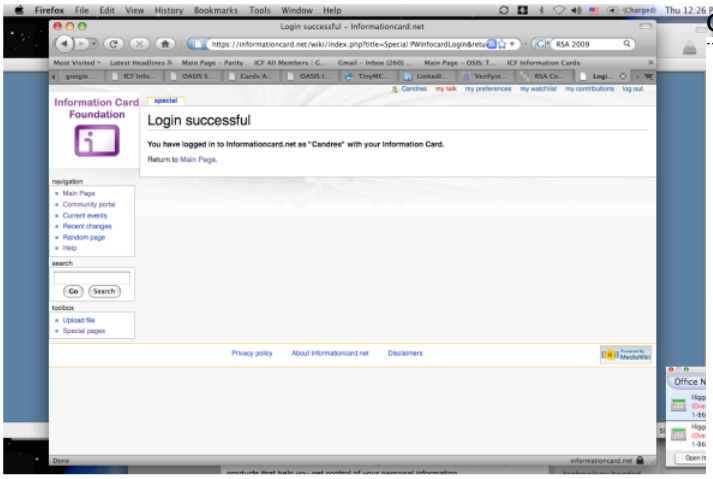
3 This one is now PIN protected



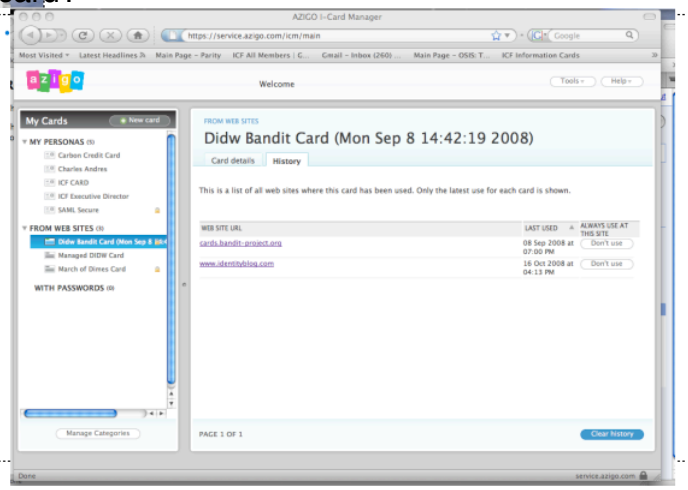
6 Always use this card at this site…



7 Look, Ma! No Passwords



8 Where have I used this card?



Information Cards: "Click in" not login

- **Trusted Verified Claims on the Internet** will change everything
- **Information Cards** allows anyone to wield the claims others make about them.
- Simple metaphor of a *'digital wallet'* and cards simplifies authorization.
- **Better risk assessment, lower fraud, less data breach exposure**
- Tripartite system (user, website, identity provider)
- **Information Card Foundation**: Google, Microsoft, Paypal, Equifax, 40 others.
- Better user experience: Endless digital baptism of username/password/form filling will end.
- Phishing, Pharming become much more difficult.
- Applicable to retail users, employees, citizens, patients, investors, members of any organization
- Digital Relationships will be more persistent but severable; encourages better B2B, B2C, C2B relationships.
  more at http://www.**informationcard.net**

Information Card Foundation

Mission

- Advance the use of the Information Card metaphor as a key component of an open, interoperable, royalty-free, user-centric identity layer spanning both the enterprise and the Internet.

Methods

- Promote interoperability via recommendations, technical interop events, and working group reports for Information Card technology, policy, and user experience.
- Provide guidance and support for projects advancing Information Card infrastructure on the widest possible range of platforms, including freely available open source implementations.
- Encourage the development of policy frameworks, identity rights agreements, auditing mechanisms, and other means of ensuring that Information Cards meet social and legal requirements.
- Engage in promotional and marketing activities to encourage the adoption of Information Cards.
- Create and maintain an open community portal that:
  - Provides easy access to tools and resources about Information Cards.
  - Supports a community of designers, architects, and developers working on Information Card-based projects, protocols, and applications.
  - Promotes Information Cards to users, sites, communities, governments, and any other interested audience.

Current ICF Objectives

- Common agreement on claim types schemas
- Consistent user ceremony (website best practices)
- Create an ecosystem that is not dominated by one or 2 powerful players
- Make it easy for websites to use i-cards
- Certify Identity providers and best practices
- Promote Interoperability

Encourage information card services

Interoperability

2007-2008:

- 4 Interop Events
- Burton SFO June 2007
- Burton Barcelona Oct 2007

- 57 Companies and Projects
  - Information Cards
  - Open ID
  - SAML
  - Open SSO

The Tipping Point

One or more of the following occurs:

- USPS follows UPS issuing Information Card with address
- A large bank issues Information Cards for login
- Credit Card systems link to Information Cards
- A large on-line retail chain issues Information Cards as Loyalty Cards+
- A medical insurance program issues Information Cards to its members
- A pension fund issues Information Cards to its members

Savvy Internet Users all have the following Information Cards:

- Of age
- Address
- Blogging Card
- Credit Card with self-asserted claims

Member Card to clickin to alumni site, 401K, etc.

We all need Information Cards

- http://www.informationcard.net

Charles Andres,Executive Director
Information Card Foundation
Candres@informationcard.net

How will i-cards evolve?

At first, low value transactions

- most self-asserted for ease of use, connected with some new identity providers
- I am of age
- I am authorized to complete this transaction
- Form filling for popular sites

Next, relationships begin to emerge between business and customer-- easy clickin (no passwords)

- Authorization that user is a member (town library, AAA, prof org)-- little used sites -- alumni assn, retirement plan, etc.

I.e. Alumni Assn becomes an Identity Provider, issues I-cards to minimize password hassle.

2020

- 21st Century Clickin Replaces 20th Century Computer Lab Login
- Phishing, Pharming are much more difficult
- Personal data is only stored when and where necessary
- Trust is back in fashion
- Linked Contracts lower cost of doing business
- Data breaches are largely a thing of the past
- Internet is more safe, secure, and private
  - On-line retail reaches its potential
  - Phone and wallet merge

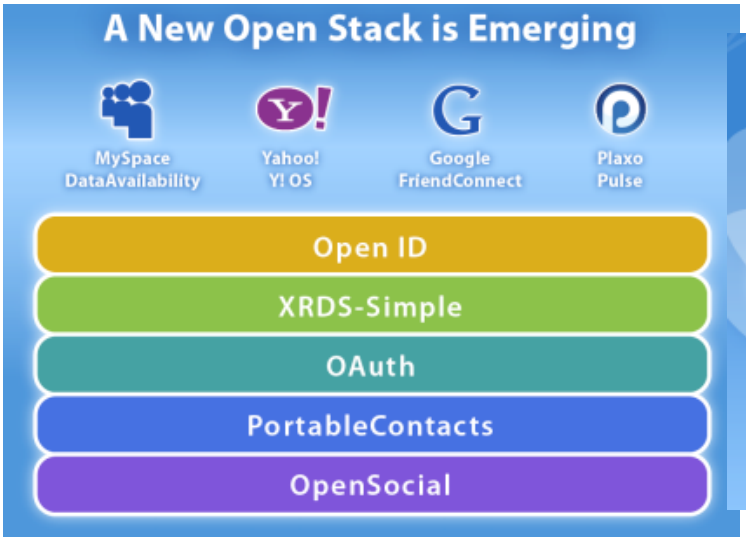
The Open Stack – Joseph Smarr

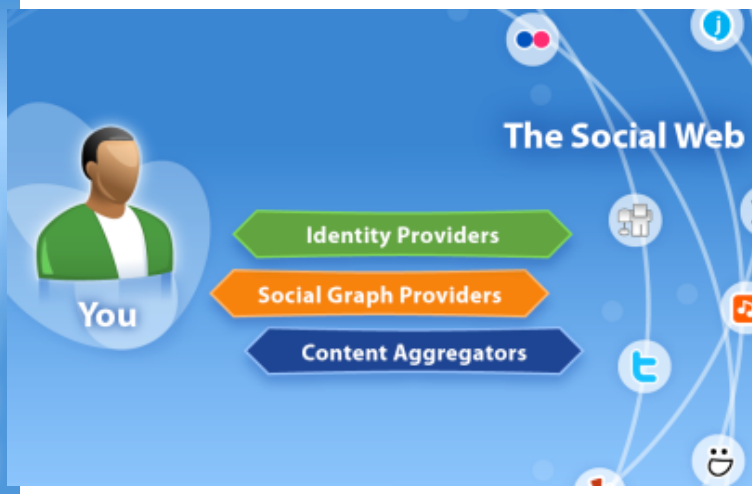
You can find his presentation here
http://bit.ly/OpenStack
http://josephsmarr.com/2008/11/10/a-new-open-stack-greater-than-the-sum-of-its-parts-internet-identity-workshop-2008b/

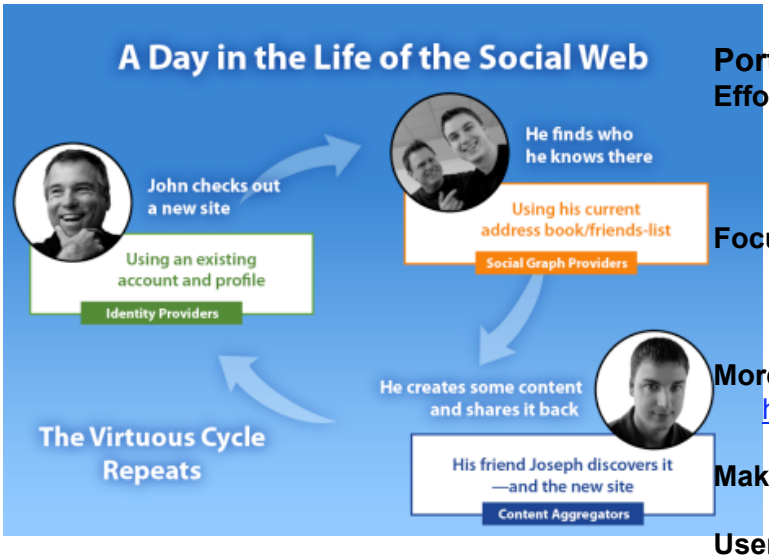
You can find a video of him giving his talk here.
http://www.vimeo.com/2230008

Commentary from his Blog on the talk:
I was asked to give one of the opening overview talks at the Internet Identity Workshop about how the "Open Stack" is getting mainstream sites interested in supporting OpenID, OAuth, and Portable Contacts, because the combined value these technologies offer together is greater than the sum of their parts. Having learned so much myself at previous IIWs, it was both an honor and a unique challenge to address this crowd and do them justice–the audience is a mix of super-savvy veterans and new people just getting interested in the space, and I wanted to please everybody. So I put together a new talk with a new core message: the Open Stack is greater than the sum of its parts, and together these building blocks are delivering enough value to make the proposition a win-win-win for developers, users, and site owners to adopt and embrace.

The talk was well received, and it led to a lively discussion afterwards in the break and at dinner. I can't wait to see what sessions people will call over the next two days to discuss these issues in more depth. It was certainly a joy to be able to demo running code on Yahoo, Google, and MySpace as part of my talk–this is no longer a theoretical exercise when it comes to talking about putting these standards to work! I was even able to show off a newly developed Android app that uses OAuth and Portable Contacts to allow import into your cell phone from an arbitrary address book. I just found about the app this morning–now that's the Open Stack in action!







Portable Contacts: The missing piece

Effort underway to standardize:

- contact schema
- discovery / auth
- common operations

Focused on ease & speed of adoption

- Active involvement from large & small players

More info & current draft spec:
http://portablecontacts.net

Making people data portable: it really works!

User signs in with an OpenID

- Site fetches OpenID URL → looks for X-XRDS-Location
- Site parses XRDS-Simple doc to discover available APIs

Site tries to access contacts API → gets a 401

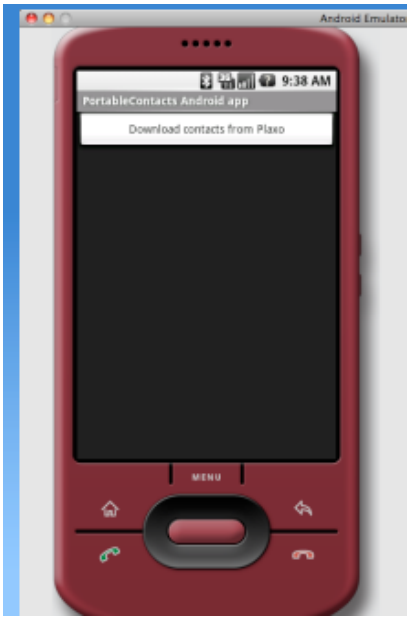
- WWW-Authenticate response header specifies OAuth
- OAuth Discovery (via XRDS) provides OAuth endpoints

Site sends user though OAuth flow to grant access

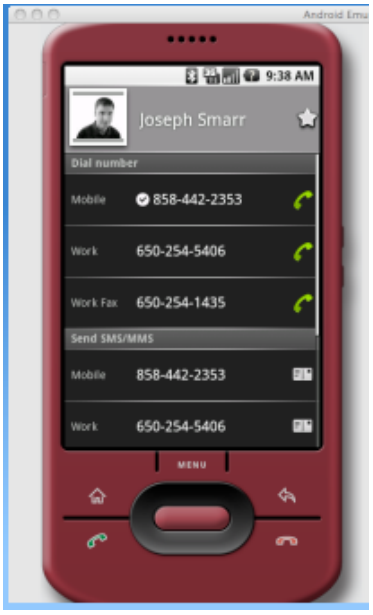
- User returns to site with authorized access token
- Site can now access users' contacts data via API + token


PortableContacts test client
Auth type: OAuth
API base URL: http://modules.partuza.nl/social/rest/people
OAuth
Access token: cee5c4f6-dbf4-cfe4-9bfc-f1ffddf3fcf9
Access secret: 20aaa89f4eef32f7100644ea708de3b1
Consumer key: e3ebe4fc-d2df-c9d3-82cb-edd8ebdce2f2
Consumer secret: 6b79faebccbcea427c5732abb27f9e13
Portable Contacts
path: /@me/@all
filterBy: (none)
filterOp: contains
filterValue:
Start over | Generate a link
Contacts
Barry
Bruno
Chris
Android Emulator (5554)
6:20 PM
Sign In
E-mail: plaxo@seansullivan.com
Password:
Remember me
Sign in
Other ways to sign in:
Sign in with OpenID
Sign in with Yahoo! ID
Sign in with a Google Account
clickpass enter
MENU
http://code.google.com/p/inoco/

6:20 PM
www.plaxo.com: Plaxo
plaxo
My Profile
Access Request
Grant access
Deny access
MENU


9:38 AM
PortableContacts Android app
Download contacts from Plaxo
MENU


9:38 AM
Dialer
Call log
Contacts
Favorites
John McCrea
Mobile 650.218.4502
Joseph Smarr
Mobile 858-442-2353
MENU


9:38 AM
Joseph Smarr
Dial number
Mobile 858-442-2353
Work 650-254-5406
Work Fax 650-254-1435
Send SMS/MMS
Mobile 858-442-2353
Work 650-254-5406
MENU

So, in conclusion…
There is now a clear vision and everyone shares it

Vendor Relationship Management – Doc Searls

Doc gave a talk about the state of the VRM project – what it is and where it is going.

How will we get to the BIG BANG of Identity? - Everyone

We divided the community up between oldies and newbies and then broke in to small groups that were evenly mixed. We had 12 groups and they discussed what it would take to get to the big bang of Identity for 40 min. Each group reported out its answer both verbally and on post-it notes.

Here is what was written on the post-it notes.

* PORTABILITY OF IDENTITY
* Portable (mobile) identity information
* Compelling apps/business cases
* Developer protocols like open social
* Trust framework for OpenID Providers
* Where are the Relying Parties

* objectives from biz dev " We want to own the users."
  * problems of trust
    - o can we have global reputation?
    - o Fear of data breach more compelling/reputation risk
  * Relying Parties requests for IdP
    - o Digg Captchas
    - o HealthVault - security audit.

Interoperability
  * Protocol - between specifications
  * Implementation
  * deployability

IDENTITY CREATION/TERMINATION
INTEROPERABILITY

Interoperability
  * Trusted IPs - Critical must
  * Aggregator of Claims
  * Trust Technology
    - o Reputation
    - o Secure
    - o Strong Auth
  * Verified Claims
    - o RP's fore Life Essentials - critical mass
  * Privacy - user controls

Eliminate the need fore "global" identifier - to be used by people.

A solution looking for a problem

  * We start by getting straight what the "big bang" is.
  * When we figure out what form the "big bang" takes.
  * Don't have to solve all problems to have a big bang.

* Education of end users
* Usability (must do something they value)
* usability big bang - 1 ID gets you in composite identity

* Techies stop talking about tech and talk about user experience
* Excellent User Experience
* Simple user experience decoupled from plumbing (protocols, bits and bites)

* Ability to enforce trust in plumbing (including open standards)
* TRUST FRAMEWORK

* SOLUTIONS & ADAPTATION FOR ABSTRACTION USERNAME/PASSWORD

* No Big Bang until the users feel/experience it as Big Bang
* Making ID relevent to common people
* Replicate Pre-neolithic Human Interactions in the virtual space
* When Users Care
* Trust & Tools so SP will always alow other SP to authenticate customers
* User has 1 way of authenticating on any site and managing her ID anywhere
* Value of digital ID allows you to make more money, friends or social capital, then people will adopt it
* Figure out how to manage risk & provider value beyond single-sign-on
* When individuals care to own who they are outline & interact with others authentically
* (Aids to increasing the size of a persons "community"

* ultimate goal? 1 ID everywhere or lists of IDs to manage
* Complex data management issue?
* Disaggregated apps issue
* Registery of handles? How to navigated discontinuous information

* Identity flow - how do services get info to map a

* NVISIBLE INFRASTRUCTURE (SAML, XRDS, OpenID, OAuth, InfoCards, Portable Contacts, Gadgets, WS-*) giving VISIBLE BENEFITS (Friends, Activity Stream, E-Commerce, Calendar...)

* Compelling Economic Cases
    * Trusted providers
    * Identity Assurance
    * Different Authentication contexts
    * Federated Log-In

* Realizing that running your own user/password system is stupid.
* Solve more of a business problem then just Identity.

* MARKET PLACE OF PROVIDERS
* Managed Card Providers we've heard of

* High Value Claims
* "42"
* Why do we need a "big bang" why not steady evolution

* HIGHER DEGREE OF PAIN (eg. more ID theft more losses)

* What is the Big Bang? " Where the norm becomes that the first identity request default is that identity is distributed ie. When the ah to create lead accounts is turned off by default

* The metric is that number of distributed identity sessions is graded then the alternatives.

SESSION 1

Session for Newbies

URL: http://iiw.idcommons.net/Session_for_Newbies
Convener: Judi Clark
Notes-taker(s): Skip Baneyi
Attendees:

* Judi Clark,	* Abby Jenkins,	* Joseph Holsten
* Skip Baneyi,	* Eric Draghi,	

A. **Technology Discussed/Considered:**

Open ID

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

From David Recordan re: OpenID

Reuse existing credentials elsewhere
Embed microformats in OpenID page
Flexibility w choosing ID Provider (Yahoo, Google, self-managed)
Future of OID 2.0 point directory at IDP; no need to know your old URL
Phishing is a problem on the web regardless; passwords can be used, info cards can be used
Multiple DIDs are not a failure, they can be a benefit

Open ID: delegated authentication (user /login)
Oauth: deligated web service auth

Problems being solved: multiple accounts

Chi.mp: account/activity aggregator (can you have diff profiles/persona/faces?)

PIP.verisignlabs: secure opened (hardware tokens), browser plugins (login/logout), Gives RP a sense of trust that verisign has verified who you are (brand)

MyVidoop: has a SMS based option (opt in) for authorizing first time w browser
Image based (image grid)
2 factor auth (req'd to set account up or for new browsers)
book mar? and browser plugins for non OID sites

Open ID UX State Machine Improvement

URL: http://iiw.idcommons.net/OpenID_UX_State_Machine_Improvements
Convener: Johannes Ernst
Attendees:

* John Panzer	* Tom Brown	* Alberto Cobas	* Raj Mata
* Eric Sachs	* Randy Farmer	* Dick Hardt	* Henrick Bieging

next steps: We will write-up best practices for RP session timeout & RP/IDP interaction

At IIW 2008b, one topic was "OpenID UX State Machine Improvements." The discuss centered on best practices for websites around password timeout/reprompt policies. The following is a summary of some of the suggested best practices for website administrators (either stand-alone sites, or sites using federated login).

Website runnings its own login system
Persistent or Session Cookies: When a user logs into your site, you have the choice of setting a session cookie or persistent cookie to identify their account. A persistent cookie is kept on the user's computer even if they restart their web browser, while a session cookie is removed when they restart their browser. Thus, a persistent cookie tends to be more user friendly, and a session cookie has the potential to provide higher security. Many websites let the user decide which type of cookie to use by providing a "Remember Me" checkbox, but even in that case the website needs to decide whether to have the box checked by default, or not. The general best practice for all but the highest security websites (like banks or online health records) is to default to using persistent cookies. The potential security value of session cookies is very small because it requires a user to login on a computer shared by many people (like a web cafe), and be smart enough to close their web browser, but not logout of the OS session, and then requires the next person to notice this fact and decide to do something malicious. The actual reports of this happening are incredibly low as compared to other security problems like malware on web cafe computers, or shared family computers which remember a user's password to make logins easier in the future.

Cookie lifetime: For either persistent or session cookies, it is possible to stamp them with the time they were issued, and then decide to force the user to re-authenticate after a certain time period. For the highest security websites (like banks or online health records), a timeout period of a 1-2 hours is common. For a few other higher security applications (like E-mail) a timeout period of 2 weeks is common. For most any other application, timeouts are generally not needed, though it is good practice to invalidate existing cookies if a user's password is changed (though this can be hard to do on large websites that run across multiple data-centers). It is also good practice to update the timestamps on the user's cookie every time they re-authenticate.

Risk based security: Some applications use more fine grained controls to decide when to force a user to re-authenticate. The most common is that if a user wants to change their password, they usually have to re-authenticate as part of that process using their old password. Other uncommon actions like making large purchases can also be good points at which to force a user to re-authenticate.

Last logins: While it is not common, some websites will keep a persistent cookie in a browser with the names of the accounts that have previously logged into the current website. However, now many web browsers have built in functionality similar to that as part of their password management features.

Website that is a relying party to Federated Login
Last Login: If a user is authenticated via federated login, their browser's password management feature may not auto-fill the required information about their identity provider. In that case, it is helpful to keep a cookie with the user's identity provider and use that as the default value.

Persistent or Session Cookie: If the user's IDP supports invisible logins (meaning they will assert the user's identity back to the RP if the user is already logged into the IDP), then the simplest approach is to always use session cookies to track login state, but use a permanent cookie with the user's IDP, as well as a flag to indicate whether the user had previously manually logged out of the RP site. If the session cookie is missing and the manual-logout flag was not set, then the RP can attempt to do an invisible login via the IDP. Otherwise the RP can show its login box pre-filled with the last known IDP.

Cookie lifetime: If the user's IDP supports an option to force a re-authentication (or require it if the user had not re-authenticate in x minutes) as well as invisible logins, then when the potential timeout period has been met, the user can be redirected to the IDP to see if they have more recently re-authenticated, and if so then the timeout period can be update based on that last re-authentication time. If the user's IDP does not support an option to force re-authenticate, then the RP should do its own "best effort" timeout, and show a login box after that time with the last known IDP entered if possible.

Risk based security: This require's the user's IDP to support the option to force a re-authentication , and if so it can be used as described in the previous "risk based security" section.

Clickjacking & CSRF attacking OpenID

URL: http://iiw.idcommons.net/Clickjacking_and_CSRF_attacking_OpenID
Convener: Andy Dale (=Andy)
Atendees:

* Steve Williams,
* Jeff Hodges,
* Larry Cymkin,
* Joe Steele
* Jon Nichols
* Paul Bryan
* Scott Bloomquis

Technology Discussed/Considered:

Open ID, InfoCard (briefly)

Discussion notes:

Overview of CSRF && clickjacking - Clickjacking can get around CSRF nonce protections

With OpenID -- this becomes much worse
-- redirect to target site via CSRF
-- use click-jacking to have user OK on their OP site?

Mitigations
-- Use frame-busting code
-- Don't let GET change stuff
---- POST is still vulnerable -- but can't do that from image tag
-- Use nonces for forms (for CSRF -- Steve Williams @ Digg mentioned)
---- can do this for OP login request also (allowed by OpenID)
---- reverify at the RP before accepting auth
-- Partition session cookies by process
-- Show a dialog?
-- Show an entry page always?
-- Use HTTPS -- then Referrer header can be trusted
-- Can education fix this?

Q: Does clicking on an IFrame transmit click to frames beneath?
-- transparent, low opacity iframes make this question moot

* Transparent SSO is the issue -- global OP cookie is an example of this

* The real fix is intelligent clients --- maybe a better browser?

* If everything at RP is fixed -- you are ok
-- no XSS vulns
-- nonces for requests
-- frame-busting code
-- limited cross-domain policy

* Mention "important security code uses Javascript" to get user to turn it on
-- supposed to mitigate vulnerabilities
-- could expose more vulnerabilities

Q: Why does browser not prevent clicking when opacity drops below some level?
-- what is that level?
-- what about "look alike" sites which are not opaque?

Q: What about InfoCard?
-- Charles Andres showed a UI-less clickin for InfoCard
-- Exposes same vulnerability?

Relationship icon: we need one

URL: http://iiw.idcommons.net/Relationship_Icon:_We_need_one
Convener: Joe Andrieu
Notes-taker(s): Charles Andres
Attendees:

* Drummond Reed,
* Doc Searls,
*ex AOL guy,
* Charles Andres,
* Terry Hayes,
* Paul Trevithick,
* Nika Jones
* Mike Osburn,
* Phil Windley
* eve maler (by phone),
* ian Henderson,
* Terry Hayes

Technology Discussed/Considered:

We can open a socket, remove some packets

a. VRM – r-button – richer than a link button -- creating human relationship
b. http – link (you know you were there or not) and where it goes
c. tcp/ip – packet/socket/connection

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

We need a relationship icon – what people do with eachother
Need to know everything complex about my relationship with….

Asa Hardcastle is creating examples for us to experiment with… we are learning as we go, trying to map the story to a process and code

C – vendor open to rel
D – buyer is open to rel
O – relationship formed

Varients – one magnet greyed out,

CRM – the relationship is some data trail. Period.
Relationship means some action.

What are the actions and what state is displayed via the button?
Markup in the page to show (you, or your agent)
Actions associated with the button.
Architecturally significant thing; relationship actions and state both offered by the vendor and aggregated from your relationship services. (what Switchbook is doing) Adding richer value by providing enhanced services beyond the software that creates the relationship.

Third party Augmentation (relationship) Services – Adaptive Blue (Project Glue)
Data is not connected to services now.
Make it social – connect with friends about things you 'visit' – i.e. a fave movie – Blockbuster is a relationship service, but not VRMing it yet.

Data and service portability
Silos are ok as long as you can get your data out, and use it/link it somewhere else.

We are dealing with action and state (of relationship)

Given you have the rel-button, we can have richer semantics than just a link.
State, capture state, user agent renders metadata about that. History.

So what is the VRM angle on this? What are the VRM Actions?

- users have some control over (this) and you (vendor) should be interested in it.
- Something that happens on the user customer side that the vendors need to adapt to, rather than the usual way of treating customers like cattle or worse.

Can it be used with "The Mine" ? (Adriana's Alec Muffet's project)
Can it be viral (like London war chalking)

Where does button appear?
Examples shown on i-phone by Doc – buttons – podcasting. Streaming,
Live streaming
Podcasting (cached locally)
Non-live streaming (never cached locally)

Mike's view:

- what happens when you click on the r-button?
- Shared model
- Today you have hicost low value connections
- Yellow page ads no relationship
- Switch to low cost high value relationship (requires trust – or spiffs)
- Here as I as a vendor are willing to offer to you
- Customer selects

Actions you can take without the vendor (e.g. bookmark the relationship)
Actions that the vendor can take after you take some action to develop the relationship

Context:

- bank is a vendor when you are interacting with the bank.
- Bank is a partner when I write a check

What you can do unilaterally (customer)
Ditto (business)
What you can do together

Third Party Assurance for Identity Interactions

URL: http://iiw.idcommons.net/Third_Party_Assurance_for_ID_Interactions
Convener: Lena, Kanna, Fugen F
Notes-taker(s): Lena
Attendees:

* Kevin Trilli
* Joan choi
* Greg Haverkamp
* Hiroki Itoh
* Jim Fenton
* Mary Ruddy
* Taksuki Sakushima
* Nicholas Givotosky
* Hank Mauldin
* Ksheerabdhi Krishna
* Didan Perrot
* Matt Klein
* Denises Tayloe
* Mike Jones
* Gabe Wachob
* Lena Kannappan

Discussion notes:
Great conversations form cross industry participants including financial, government, social, telco etc…

- Need Taxonomy/better definitions
- Is liberty alliance covering all the possible assurance + equipment?
- How about anonymous attributes?

OpenID and OAuth Hybrid

URL: http://iiw.idcommons.net/OpenID_and_OAuth_Hybrid
Convener: Yariv Adan
Attendees:

* Martin Atkins
* Axel Nennker
* Max Engel,
* Karen Zlenko,
* Jorgen Thelin,
* Alex Rosen,
* Praveen Alavilli,
* LP Mavrice,
* Jono Kane
* Jonas Hinn
* Scotty Logan
* Mike Lee
* Scott Kveton
* Laural Boylen.

Technology Discussed/Considered:
OpenID & OAuth

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

OpenID and OAuth flows are confusing to users if you have to do both of them at once. This session is about how we can combine the OpenID & OAuth flows to combine authorization and authentication in fewer steps to help enhance usability. This is doing what "Facebook Connect" does but with open protocols. MySpace will be doing exactly this (Max Engel in the crowd).

Use OpenID to embed the OAuth token while user is verifying their identity
- this would be a much better user experience

Google has a proposal for the OpenID/OAuth extension for doing this
- supports both OpenID and OAuth provider scenarios

Links on Googles work on this:
Google OAuth & Federated Login Research - http://sites.google.com/site/oauthgoog/
Usability research on federated login - http://sites.google.com/site/oauthgoog/UXFedLogin

Phase one is having to write a lot of this code against multiple sites; Yahoo, Google, MySpace, Facebook and others. This will pave the way to protocols and ways to automatically discover API's and how to get at things like friends, calendar, etc.

Joseph Smarr is doing the OpenID/OAuth flow on the white-board -> get pic on flickr

1. Consumer key - "unregistered consumers"
2. Require token reuse?
3. Desktop/mobile
4. Stateless RP's
5. Scope
6. SP create req_token during consent?

Do we need to support request tokens for anything but desktop clients? Web clients don't need it.

Today, OpenID and OAuth require several round-trips. This combined approach eliminates many of those round-trips.

EHL: why not have OpenID most of the heavy lifting for this?
David Recordon: RP's are not using stateless mode, its a fallback mode.
check_authentication needs to be there for sure.

Joseph offers up the idea of removing several of the steps in the OpenID + OAuth transaction knowing that we may be sacrificing some security for the user.

Session results:

* Still need to answer if we continue to use the req_token ... this is for unregistered RP's
* Read the hybrid protocol and participate in the OpenID working group on this
* New draft coming out with potential changes based on these discussions

** How do we get this moving forward?
** What do we need for library support?
** Who is going to launch with this?

SESSION 2

Dissecting Consumer Identity, or, Are We Trying to Do Too Much?

URL: http://iiw.idcommons.net/Dissecting_Consumer_Identity
Convener: Jim Fenton, Cisco
Notes-taker: Eric Sachs
Attendees:

* Eric Sachs,	* Tom Brown,	* Dave Crocker,
* Skip Beney,	* James Mclaughlin,	* Andrew Nash

Technology Discussed/Considered:
Identity management, as broken into:
- Identifier Management
- User Authentication
- Provision of User Attributes

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

Problem: Mainstream consumer websites (Amazon, LLBean, etc.) face new problems that enterprise intranets don't (trust, anonymity, etc.)

Discussion of trust barriers:
Relying Party <-> attribute providers
Can an IDP in the middle bootstrap finding each other?
Can the IDP cache attributes and re-assert them?
Can an attribute provider trust the IDP trust the IDP to get the user's permission to share attributes with a relying party?

What are the most important attributes?
Age, name, country, >21 flag, etc.

How is the permission to share information obtained?
Policy expressed by user to IDP, or query to user each time information is shared (hint: this can be very tedious and lead to bad decisions)

ID-Legal

URL: http://iiw.idcommons.net/ID-Legal, http://wiki.idcommons.net/ID-Legal
Convener: Judi Clark
Notes-taker: Judi
Attendees:

* Jeff Stollman,
* Lucy Lynch,
* Greg Hevencamp,
* Judi Clark,
* Kaliya Hamlin,
* Gabe Wachob,
* Mike Kirkwood,
* Charles Andres

Technology Discussed/Considered:
ID technology broadly

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

International considerations for conference: how to be inclusive of all interested parties. Question from last call:

How do we enhance/foster interactions/conversations between attorneys and technologists?

Lucy: "attorney" is too narrow: needs to be policy makers, judges, others that represent global interests.

Jeff: if new admin calls on tech people, needs to be driven from policy point of view.

Greg:: tech people more likely to be consulted, acknowledged

Lucy: equal balance of regulators and technologists to hear both sides' concerns

Kaliya: seriously consider having conf in DC area, winter or spring, could be an amazing event

Jeff: outside of regulators, many corps have public policy people, get them energized, esp global standards. (They know how to play the game, we don't.) These topics play to everyone that has a website.

Kaliya: asks Lucy if she has convened evens in DC, Lucy said possibility.

Kaliya: 3 major components: venue/space/time/logistics, setting context, invitation

Lucy: if we're pulling people from regulatory envt, might ask them to prepare 10 min presentation of what their issues are, their interest in this space

Gabe: “Legal conference” (MCLE credit implied, etc); what we’re really looking for are policy people. Add to the title. Important.

Lucy: much more interested in inviting John (Int’l MOUs, negotiations, up to speed on issues), someone from PrimeLife (Euro issue on policy, focus on user experience).

Mike: Platform by Apple iPhone, has lots of functionality—find legal team that made that work, good operating case (negotiated w/ telcos, etc)

Lucy: Meta level of expressing invitation

Jeff: how much national and how much global? Need good balance

Kaliya: need to focus three components above

Mike: Health & use cases at barcamps: check speakers and agenda topics that might add to flow

Lucy: from identity side: whose issues are interest to match up? Data portability, how to engage

Charles: financial transfer of liability associated w any of these transactions. Renee Lloyd w Berkman Center—her work is relevant to this discussion

Jeff: volunteers to help with group that develops invitee list

Gabe: Regulatory liability risk (can’t shift risk), financial rish management (more private sector, market may figure this out). Stuff like COPPA and health management. Increasing regulatory framework. Careful not to turn event into argument (battling agendas)

Kaliya: likes the questions about who is essential to attend (and from other groups).

Mike: superstruct: anonymous legal team, available when issues came up, won cases on behalf of small legal issues relative to social causes E.g., Japan: OpenID and transactions are done.

Gabe: Pubic policy vs private market structures; need regulatory people.

Mike:Legal team is a tool that acts to resolve conflicts as they arise. E.g., demo of guy hacking proof of concept for making info cards accepted on iPhones.

Lucy: don’t ask regulators what we can/can’t do. Ask what technologies can enable communications, what do we need to be aware of for policy support without encumbering underlying capabilities.

Mike: Apple chose to work w telco (regulators).

Lucy: handoffs between proprietary frameworks: making things interoperable, using language to develop link between technology and policy rules

Gabe: is this an advocacy group or about interesting conversations? There are other advocacy groups out there, many of which I agree with

Jeff: various topics, prioritize them into workable list, cluster when appropriate, develop agenda

Kaliya: agenda is not relevant, is unconference

Lucy: initial conversation is fire starter for event, broadening scope of conversation.

Charles: start w philosophy, change agents, parties who want to learn from each other, event works toward real change

Lucy: Washington DC is probably a great place; what is reasonable timeframe for building event? (spring)

Mike: Uber-theme: move iiw to DC?

Charles: asked Kaliya about Boston conf

Lucy: how many people? Kaliya: 80, now over 100. Lucy: between 40-100 is about as much as we can handle in this space.

Gabe: is it limiting to call it “Internet” identity

Lucy: identity is a hot topic now, getting policy makers to limit their focus from cybersecurity, trust and controlling the world…

Mike: Health; in context of healthcare you’re just someone who may work or fail. Be nice if the agenda included them, would add to conversation

Jeff: sponsors? Appropriate names in commercial space would attract

Action items:
Kaliya and Lucy will draw up a timeline for 50-80 person conf, also meta=thematic agenda-like guidelines
Talk with Dazza re policy space (also join him at lunch table today!)

Portable Contacts

URL: http://iiw.idcommons.net/Portable_Contacts
Convener: Joseph Smarr

Boeing Authentication RoadMap

URL: http://iiw.idcommons.net/Boeing_Authentication_RoadMap
Convener: Marty Schleiff
Attendees:

* Nat Sakimura,
* Sebastian Rohr,
* Andy Dale,
* Shin Apachi,
* Hiroki, Itoh,
* Mary Ruddy,
* Abbie Barbin,
* K Sheerabdhio Krishna,
* Praveen Alavilli,
* Macduff Hughes,
* Allan Schiffman,
* Jeff Shan,
* Lena Kannappan

Using the Relationship Layer to Create Trusted ID/Age Credentials for Social Networks

URL: http://iiw.idcommons.net/Using_the_Relationship_Layer_to_Create_Trusted_Age_Credentials
Convener: Kevin Trilli – Assert ID

Technology Discussed/Considered:

Converting a social network profile into a trusted identity/age credential by combining peer verification with social network analysis

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

- The proposal discussed how certain social network profiles can be converted to higher assurance identity credentials by leveraging the social graph as a peer verification method ("web of trust".) However to enable universal applicability, the method is needed to quantify, in a standardized fashion, how trustworthy a credential is to a relying party. An algorithmic approach was proposed to score each asserted and verified attribute.

- Feedback included concern of mass collusion by kids all faking their ages, the purely online nature of the process, and direct involvement of ? consumers. (NOTE: the first two points are considered by the algorithm of the current approach)

- Other comments acknowledged it useful as a broad approach to creating verified identities where incentives to lie are not so high universally.

- Other suggestions included looking into easier attributes to verify initially that could provide a filter for the initial constituents & a foundation for specific attributes like age.

More detail can be found at assert ID.com, or by contacting jnchoi@stanford.edu

OpenID Authentication 2.1

URL: http://iiw.idcommons.net/OpenID_Authentication_2.1
Convener: David Recordon, John B
Notes-taker(s): Martin
Attendees:

* John Bradley
* Dan Balfanz
* Martin Atkins,
* AxelNennker,
* Scott Blumquist,
* Breno de Mediros,
* Yariv Adam,
* Jorgen Thelin,
* Mike Mell,
* Mike Jones,
* Jim Pravetz,
* John Panzer,
*Alberto Cobas,
* Brian Eaton,
* Will Norris,
* Henrik Biering,
* David Richards,
* Raj Mata,
* Mike Lee,
* Allan Schiffman,
* Gabe Wachob,
* Eran Hammer,
* Joseph Holsten,
* Kannan Seshadri

Technology Discussed/Considered:
OpenID

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

2.0 has been finalized
bunch of implementations
found lots of spec bugs

also gone and done oauth and email addresses and other things. Can we support these in the core spec?

* Making the spec more readable and fixing bugs (eratta)
  - Delegation
  - Error handling

* Adding a security appendix
  - could be a separate document referred to by the spec
  - possibly produced by separate group
  - Who controls this security page?
    - Security committee could look after this.
    - or Allen at Yahoo! will be editing a security document

* Clarifying XRI
  - Currently there's no firm message about whether RPs MUST support XRIs or not.
  - Need to clarify how exactly XRI should be used with OpenID.
  - Similar to the whitelist question.

* Clarify if RPs can white or blacklist what OPs they accept, and vice-versa.
  - Discovery of type of identifiers an RP supports.

* Clarifying IRI
* Updating discovery. Possibly including the new-fangled XRD discovery.
* Clarifying whether association over SSL must/can use diffie-hellman.
* Discovery of support of checkid_immediate.

Exploratory work:

* Signature mechanisms. Looking at additionally supporting the mechanisms defined in OAuth so that they can be closer together.
  - Possibly deprecating the current signature mechanism.
  - Public keys?

* Email-shaped identifiers for OpenID
  - Could be a separate working group?

There was consensus that email-shaped identifiers would be worked on by a separate group and possibly rolled into 2.1 if it's done in time.
* Smart/rich clients?
  - Could be in this WG unless it ends up being a big change in which case it could be its own WG.
- There's another session about this.

SESSION 3

OpenID Foundaiton Update

URL: http://iiw.idcommons.net/OpenID_Foundation_Update
Convener: Brian Kissel, Eric Sachs
Attendees:

Slide 1: OpenID Foundation Customer Research Committee November 11, 2008
Slide 2: " 18 Organizations " 8 OpenID Providers (OPs), 8 Relying Parties (RPs)
Slide 3: Ranking Areas of Interest
Slide 4: Positive Feedback
•OpenID is viewed positively: open, lightweight, extensible, etc.
•OpenID addresses an important market need, OpenID (or something like it) will have broad adoption sooner rather than later
•Strong market adoption from net savvy technologists, people with early adopter values, user-generated content websites and small Web 2.0 companies
•Market drivers
    •Move to open web, interoperable framework
    •Growing on-line activity levels (research, e-commerce, social networks, etc.)
    •Increasingly web savvy consumers
    •Move to user-centricity, growth of user-generated content

Slide 5: Positive Feedback (cont.)
•Technology enablers
•Acceptance of open source software, software as a service (SaaS)
•Matured web technologies Business benefits cited
•Allow consumer users to move from website to website easily and seamlessly, manage their web identity in one place, get personalized info in a trusted way
•Provide SSO federation across multiple web properties within a family of sites (internal) Provide federated SSO with partner sites (external)
•Holy Grail: Consumers will be able to move seamlessly across all sites on the web in an authenticated session
•Streamline registration, reduce drop-off rate of potential visitors at registration, increase conversion rates of site visitors to registered users
•Reduce customer care costs associated with password maintenance

•Provide a higher-quality brand experience; get consumers more easily engaged and interacting; retain them better, longer
•Learn more about consumer users via user-centric identity tools (SREG, AX, OAuth, MySpace Data Availability, Portable Contacts, etc.)
•Enable revenue-sharing arrangements between OPs and RPs

Slide 6: Areas for Improvement
User Experience
- •Over complicated user experience
- •UI design, sign-on flow, attributes, URL as identifier, inconsistent user experience across OPs and RPs, reconciliation of multiple user accounts, sign-off, etc.
- •Lack of consumer understanding of OpenID

Data
- •Many large OPs not sending SREG data today, email is most requested field
- •Lack of a flexible international data scheme with ability to adapt it to local customs, business models, etc.

•Business/Legal
- •Not all business managers fully understand the business benefits of OpenID
- •Legal and regulatory frameworks not fully developed
- •Security/Trust/Privacy issues require further development
- •Possible need for some kind of OP certification program

•Adoption
- •Few large companies have implemented it broadly yet
- •OpenID supporters and Foundation Board members appear to be more focused on the technology than the business applications and needs

Slide 7: Initiatives Underway
- UX
  - Yahoo, Google, AOL, Microsoft, MySpace, Facebook, JanRain, Vidoop, Plaxo and others met at Yahoo for a user experience (UX) summit to discuss ways to improve the OpenID user experience between OPs and RPs.
  - Yahoo streamlined their OP login process, Google LSO initiative, JanRain RPX
- Data
  - Google is providing verified email via AX, Yahoo and AOL evaluating SREG deployment, MySpace to provide profile and friends data, Plaxo supporting Portable Contacts
- Legal Framework
  - Yahoo and Google are developing templates for legal and business agreements governing OP/RP interchanges
  - NRI leading on Trusted Data Exchange (TX) extension
- Security
  - The PAPE authentication security standards have been officially submitted for public review and final ratification
  - OIDF Security Committee has been formed, chaired by Tony Nadalin of IBM

Open Social: Beyond gadgets in Social Networks

URL: http://iiw.idcommons.net/index.php?title=Open_Social:_Beyond_Gadgets_in_Social_Networks
Convener: Kevin Marks

Common Marketing Messages

URL: http://iiw.idcommons.net/Unified_Marketing_Messages
Convener: C Andres
Notes-taker: Alex Rosen
Attendees:

* Charles Andres
* Hank Mauldin
* Dave Crocker
* Lucy Lynch
* Mary Ruddy
* Alex Rosen
* An Bui
* Cliff Gerris

Technology Discussed/Considered:

- Marketing messages
- Information Card Foundation
- Higgins
- OpenID Foundation

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

- Key Takeaway: Let's work on this charter at http://wiki.idcommons.net/Unified_Messaging_Charter
- Must make messaging consistent with what's out there now
- How to work withthin worldwide legal constriants and documents around these?
- What's the difference between messaging the neterprise and the end user?
- What are the use cases/pain points to focus around? Is making a list even possible?
- This shouldn't turn into a technology discussion. It's how to get common messaging to companies working in this space and looking to deploy identity solutions
- Can we/should we influence marketing plans of OpenID and Info Cards
- The key is to create the language that establishes what this even is. Think of the credit card: people understand what the solution is and what they do, so they can talk specifics.
- Consider functionality vs. value
- **Add to the wiki!!!** http://wiki.idcommons.net/Unified_Messaging_Charter

i-cards on the i-Phone

URL: http://iiw.idcommons.net/I-cards_on_the_i-Phone
Convener: Markus
Notes-taker: Hiroki I (from NTT Nippon Telegraph and Telephone Corp.)
Attendes:

* Randy Farmer
* Tim Burks
* Phil Windley
* Jonathan Nichols
* Hiroki Itoh
* Scott Stefanski
* Terry Hayes
* May Branscake

Technology Discussed/Considered:
QT plug for iPhone using Java platform
User centric
How to (solve – not solve) security issues

Discussion notes:
Future Focus: using this technology when the user wants to log in some website on his/her PC

Online Identity In The Context Of Civic/Government Engagment

URL: http://iiw.idcommons.net/Online_Identity_in_the_Context_of_Civic/Government_Engagement
Convener: Lou Klephner

Discussion notes:
Discussed the issues surrounding Civic/Government on-line identity

- Secret Ballots/Privacy Concerns
- One time votes vs adjustable
- Who is the customer? Government? Citizens? Advocacy
- What is the long-term governance plan? Groups?

Online BigDialog with President-elect Obama

An MIT hosted event promoting civic participation and open government
URL: http://iiw.idcommons.net/Online_BigDialog_with_President-elect_Obama
Convener AND Notes-taker: Dazza Greenwood, CIVICS.com -

Technology Discussed/Considered:

The ultimate identifier for "good enough" individual authentication is a phone number for that person. It can be checked and it provides good quantitative ability for restricting fake users (if people from the same IP address sign up for 100 accounts with telephone numbers with unique telephone numbers, can check if numbers are valid, etc) For other people, maybe use a number to a person who can vouch for you (e.g. a social worker, notary, etc) - OR - outsourced to dollar/name services like the KBA of credit companies, etc.

LOOK AT:
* Yahoo Design Patterns for Reputation
* mag.nolia.com
* loki plus google gears API and consider Skyhook integration with tagcloud heatmap
* need mechanisms for presence on many sites (facebook app, myspace, etc) with abstracted username so we can have a single core-identity that is integrated rather than duplicated
* look at openID plus facebook connect plus MS windows live delegation, etc…

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

We need a low bar to mass participation, perhaps just IP address at first, and an voluntary higher bar for additional identity and authentication to assure one vote per person, allow for anonymity without unaccountable abuse, the ability to sort to the President/President-elect by "top questions by Americans", permit deeper personalization and cross-services for eGovernment participation in the future.

Additional advantages flow from additional authentication, like you get to rate on more metrics, you get to have your question counted for prizes and incentives (like getting a flight to MIT and possibly getting a "call back" from President-elect Obama), you get more advanced analytics and sorting by other peoples demographics (but with no names), etc.

Talk to people who did iPhone application for Obama that showed who they need to call in key battleground states from their contact list - gave an "action" and was a success - contact: dom@iphonedevcamp.org (mention the blog guy)
==========
D. Joseph Greenwood, JD
I.net: http://CIVICS.com
E.mail: dazza@media.mit.edu
M.obile: +1-650-504-5474

SESSION 4

OpenID Foundation Japan Experience "Business & Marketing"

w/ Japan Airline Case Study etc

URL: http://iiw.idcommons.net/OpenID_Foundation_Japan_Experience
Convener: Nat Sakimura, Nomura Research Institute
Notes-taker: T Sakushima, NRI America
Attendees:

* Didain Perrot
* T. Sakushima
* Vijay Simha
* Shin Adachi
* Andrew Nash
* James McLaughlin
* Hiroki Itoh
* Henrick Biering
* Karen Zelanbo
* Minglian Pei
* Gabriel Wachob
* Lena Kannappan

What Discussed
The presentation slides are here:
http://www.slideshare.net/nat_sakimura/open-id-japan-presentation-for-iiw2008b-presentation/

Nat highlighted some facts to show how successful OpenID is in Japan:
-In survey that OIDFJ made, almost 28% aware OpneID and 15% actually has used it.
-32 companies are members of OIDFJ and the number is still increasing.
Most of them are major companies in industries like financial, e-commerce, telco(mobiles/ISP).
-The current member list can be found at http://www.openid.or.jp/memberlist.html
-OPIDF is partnering with Liberty Japan SIG for many ID related promotion activities.

Also he covers the Japan Airline(JAL) use case. JAL actually uses OpenID as SSO solutions for affiliates.

B. Notes, Key understanding, Questions, Observations, and Action items

Not all of the members are actually using OpenID yet, but they are now considering it along with their business strategies and compliance issues. For example, Japanese mobile carriers are mandated for ID portability and they will have to keep user's account even though the user switches to another carrier. DRM for purchased contents through mobile connection (e.g music) are tied to mobile accounts. Contents must be accessible from the account that an user moving to.

The key success factor of OIDFJ is to driving promotion for 3 different domains simultaneously:
1)Consumers
2)Bisnesses/Developers Community
3)Government

For 1)Consumers, to catch media attentions is very important. The magazine for average Internet users even covers OpenID. Actually the word "OpenID" is on the cover page of the magazine with a Japanese pop singer. The OpenID awareness survey is conducted regular bases to see the progress periodically.

For 2)Businesses, visiting over 100 companies really helps their understanding of OpenID and discuss specific issues one by one. It is time consuming however it is must approaches for business communities. Many technical seminars are conducted through OIDFJ and Liberty SIG. Many use case ideas are shared in seminars. Nat emphasizes that "Security" must be talked in each visit or seminar otherwise OpenID is completely misunderstood.

For 3)Government, as a consulting firm, NRI leverages the position to have many discussions with government agencies and also assist them in many researches including Assurance Programs, Digital Signature and E-Authentication.

Nat introduced the JAL case study as one of example of business use case discussion with OpenID prospects. What is call "Trust Exchange" extension actually comes from one of discussions with JAL. Customers of JAL can use their mileage membership account(a account number tied with an OpenID) for SSO in JAL's affiliate sites (hotel reservation, rent a car, etc.)

Questions?

Q:What is the value proposition to consumers when promoting OpenID to them?
A:Mostly SSO and ease of managing accounts. Audit trail and strong authentication were also raised from participants.

Q:In the JAL case study, it can be implemented by SAML. Why is OpenID chosen?
A:Ease of implementation especially RP sides. Also various popular languages like PHP and Ruby can be used.
Those script languages are preferred languages for many developers, so more candidates of RPs can be expected.

--
Tatsuki Sakushima
NRI Pacific - Nomura Research Institute America, Inc.
TEL:(650)638-7258
SkypeIn:(650)209-4811

Planning the Next OSIS Interop

URL: http://iiw.idcommons.net/Planning_the_next_OSIS_Interop
Convener: OSIS Committee Members
Notes-taker(s): Mike Jones

The OSIS session at IIW during which we planned themes for the 5th OSIS Interop was lightly attended. Attendees were: Charles Andres, Denise Tayloe, Mike Jones

Based on the input to OSIS as of today, these are the interop themes planned for inclusion in I5:
- Deeper OpenID feature testing – already a plan of record. Owner John Bradley.
- Compliance with the OASIS standard versions of WS-Trust and WS-SecurityPolicy. Owner Mike Jones.
- Ongoing Interop. Pamela Dingle has agreed to clone the I4 portions of the wiki to create the I5 wiki pages.
- Use of verified claims, starting with the ICF age-18-or-over claim. Owner Charles Andres.

These possible themes had been discussed, but heretofore no specifics or owners have emerged, and therefore unless this changes, will not be included in I5:
- Situational interop. (Although one could consider the "use of verified claims" theme to be a situational interop, so we could declare victory here.)
- Concordia scenarios. These could still be included but would need precise definitions and owners very soon.

Yours for the interop committee,
-- Mike

VRM What We're Working On What's Next

URL: http://iiw.idcommons.net/VRM_What_We_Are_Working_on_Whats_Next
Convener: Doc Searls
Notes-taker(s): Judi Clark
Attendees:

* John Kelly
* Alex Rosen
* Mike Ozburn
* Joe Andrieu
* Doc Searls
* Jeff Stollman
* Tim Burks
* Greg Havercamp
*Jim Fenton
* Salim Ismail
* Judi Clark
* Greg Biggers
* Rob Regan
* Robert Simon
* Nick Givotovsky
* Abby Jenkins
* Lou Klepner
* Terry Hayes

Technology Discussed/Considered:
VRM broadly

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:
Advertising, even if improved to Nth degree, is still guesswork. Hard to get out of that mentality. Some ads are essentially catalogs (Vogue, etc). CRM basically same, can limit the amt of info that companies can know about their customers.

VRM is approach from other side: let people manage relationships w vendors. Trying to think thru ways to work out identity problems before relationships (in progress, we might be close enough).

Andre: 3 layers of identity. First version based around individual (federation). Having customer in control has ben theme running thru since beginning. Anybody can relate to anybody. Implied promise. VRM is one way to address it.

Players:
(Britt B has Gov Rel Mgmt). Parties involved: Joe (Switchbook) and Doc, Adriana (in UK – MINE project), Iain Henderson (Personal data store, volunteer personal info).
Allen Mitchell (buyer centric commerce forum).

Other tech: Higgins, Windley's kinetics, lots of convergence (my stuff works with your stuff).

Information card: Doc witnessed conversation btwn Paul T (Higgins) and Kim C (Microsoft) hashing out information cards. Now w Drummond Reed (XRXI) and Charles Andres (I cards).

Spawn tech:
Azigo (card selector and related services).

Single use case: change of address. We do it commonly, user is authoritative source, post office spends billions of dollars on this issue. Iain is doing it w Royal mail.

VRM is doing work around public media/broadcasting: PRI, NPR, PBX, 2 others. Grant possible to develop a radio w REL button.

Rel button now in two states: open or closed. Planning on implementing on iPhone or Android. Class of files/data on server for podcasting is store/forward. Rel button to implement donations, facilitates options like spooling the show or interacting w listeners, etc.

Story of royalty rates for streaming radio/broadcasters: RIAA. Streaming rates set by gov, but not equitable for streaming stations that have lots of listeners. Contrast w MLOT: money left on table: people

paying for goods they're getting; not advertising nor donation. Like a shareware or Pay choice. Channel conflict as people move to Internet and away from location-based stations; needs to be fixed.

How does VRM deal with customer-side problem? Doc is unusual because he sends money to 10 diff radio stations. Wishes he could store some info that station could receive a message. Many things in the world that we want, but no way of codifying ways of promoting our need/want.

Joe: current legal framework for sharing data falls under copyright.

Doc: important distinction: copyright is a sell-side issue. we're trying to solve problems from the other side. Working on Terms of Service.

EULAlizer: identifies/flags certain terms in EULA agreements

Desire to walk into a relationship on our terms. Loyalty cards.

Personal RFP: Doc's loyalties: Chulula Hot Sauce not available in Boston. Pete's Coffee. Dot Tel (new domain puts extensible data, zip into DNS (e.g., personal address manager).

Personal use cases? Address change management, and personal data store. Public radio. Search maps (no easy way to move search history from one provider to another; new way to move data around, with appropriate rights bundles)

Health care data: user as originator/authority and point of driver.

Questions: how to engage, what is expectation level, and when's next VRM workshop? Mailing lists. Several committees, is basically barn raising. Next workshop date not set yet.

Browser Extension Convergence

URL: http://iiw.idcommons.net/Browser_Extension_Convergence
Convener and Note Taker: Paul Trevithick

We had a session on trying to converge towards a single browser extension for these four browsers: IE, FF, Safari, Chrome. Or, at least that's how it started off.

Today we've got lots of browser extensions for different browsers each of which generally supports a specific protocol (e.g. OpenID or I-Card or…). What we'd like to get to is having one multi-protocol browser extension for each browser–that is, a total of four extensions. And eventually, we'd like to see these built into the browsers themselves.

We started by creating a quick inventory of the existing browser extensions:

1. Firefox: Sxipper (OpenID, UN/PW)
2. Firefox: Higgins: HBX4FF (I-Card)
3. Firefox: OpenInfoCard (I-Card)
4. Firefox: DigitalMe (I-Card)
5. Firefox: OpenLiberty (SAML)
6. Firefox: Verisign Seatbelt (OpenID)
7. Firefox: IDIB (OpenID…)
8. IE: Microsoft's I-Card built-in
9. IE: Higgins: HBX4IE

We then made a list of protocol "families" that we think each extension should support:

1. Username/Password (Form-based, HTTP Auth, WS-Security)
2. OpenID (OpenID, SAML)
3. I-Card (ISIP→IMI-TC)
4. Kerberos
5. SAML (SAML SSO, SAML ECP)

We also made a list of possible "packaging" options for these extensions, though this didn't really lead to any discussion:

1. Browser-native add-on/extension/plug-in
2. Flash
3. Java
4. Gears
5. Silverlight

We discovered that there was an opportunity to first agree on the specifications for auth discovery across protocols. This became the next part of the meeting…

Part 2: Browser Support for RP Auth Discovery
Everyone agreed that creating common specs for this was a good idea, whether or not they were interested in creating implementations. We saw that we could use XRDS as the basis for discovery of a relying party (RP) site's authentication support for multiple protocols. The RP site would publish an XRDS document that would allow a "smart client" (well, a browser extension) to discover information about what protocols were supported and how they might be used to authenticate to the site.

Today I-Card tech embeds an HTML <object> tag, but Axel Nennker has put forward here [1] and here [2] a variation where instead of an embedded <object> tag we use a link/rel approach. Meanwhile, Scott Kveton and other OpenID folks have also been looking at using XRDS to discover RP auth metadata. In a similar manner XRDS SEPs could be defined for SAML, UN/PW and Kerberos.

So the consensus was that we should pursue this common approach to RP Auth Discovery.

[1] http://ignisvulpis.blogspot.com/2008/10/information-cards-with-xrds.html
[2]http://iiw.idcommons.net/Iiw2008b_XRDS_for_OpenId_and_Information_Cards_and_other_%22Services%22

HTTP Discovery - XRD

URL: http://iiw.idcommons.net/HTTP_Discovery
Note Taker: Eran
Taking Resource URI and finding metadata
Requirements:
* Should be able to get the metadata without accessing the resource.
  * You don't know what it is yet, so you shouldn't be interact with it yet.
* The the resource can point at its metadata.
* Must be accessible to different levels of developers.
  * Can't *just* require headers. Must also support an HTML solution.
* Must work with web architecture.
* Must be friendly to little and big players.
  * The same solution for your blog should work for a large company.
hueniverse.com

	Resource Declaration	Direct Metadata Access	Web Compliant	Scale Agnostic	Extendable
1. HTTP Response Header (Link, X-XRDS-Location)	+		+		
2. HTTP Response Header over HEAD	+			+	+
3. HTTP Header Negotiation	+			+/-	
4. HTML <Link> Element (<Meta>)	+		+	+	
5. HTTP Content Negotiation (Accept)		+			
6. HTTP OPTIONS Method		+	+		+
7. WebDAV PROPFIND Method (MGET, ARK)		+/-	+/-		+/-
8. Custom HTTP Method		+			+
9. Static Resource Mapping (Prefix, Suffix)		+	+/-	+/-	
10.Dynamic Resource Mapping (Templates, /site-meta)	+/-	+	+	+/-	+/-

A combination of 1, 4 and 10 seem promising.

For dynamic mapping:
a. DNS
b. Known Location (like /robots.txt)

b is the /site-meta proposal.

Additional background information from Drummonds Post
http://www.equalsdrummond.name/?p=172

XRD Begins
For most people, watching the evolution of technical specifications is like watching a glacier move. To those of us living the process, though, there can be a great deal of drama to it ¬in fact it s much more like climbing an icefall inside the glacier (anyone doubting how much adrenaline that takes should read John Krakauer s description in Into Thin Air of climbing Mt. Everest s Khumbu Icefall). For example, the failure of the OASIS Standard vote on the XRI 2.0 specifications last May ¬the first ever in 40+ OASIS Standard votes ¬was a watershed in the interaction of two standards bodies (W3C and OASIS).

The repercussions from that event have been equally unpredictable. Who would have thought that just four months later the XRI TC and W3C TAG would have rough consensus on how to resolve their differences? Or that the discussions would spill over to the much larger topic of uniform metadata discovery on the Web? Or that enough interest would develop in the XRDS discovery format to beget a new spec intended for uniform metadata discovery for any type of URI or XRI?

But that's just what has happened. Two weeks ago at the Internet Identity Workshop, Eran Hammer-Lahav, author of the OAuth Discovery spec and founder of the XRDS-Simple list, led a marathon session on a new uniform metadata discovery specification to be called XRD 1.0. With 20 to 40 people in attendance all afternoon, Eran first ran through his exhaustively-researched blog post on HTTP and discovery, then through the proposed simplifications to the current XRDS/XRD schema. By the end there was rough consensus on XRD as a mechanism for uniform metadata discovery across all the different Internet identity and data sharing specs that need it (XRI, OpenID, OAuth, OpenSocial, XDI, Data Portability, etc.)

The name "XRD" is itself quite revealing of the evolutionary path to this point. When the OASIS XRI TC first developed the XML-based metadata discovery format we needed for XRI resolution back in 2003, we called it XRID (XRI Descriptor). We made it as simple and generalized as we could simply because any resource could have an XRI, so there was no telling what type of metadata might be needed over time. We focused primarily on one clear requirement: given input identifier x and service type y, define how to discover service endpoint URI z.

By 2005, when OpenID grew to the point of needing a discovery format, the authors of the Yadis (Yet Another Discovery spec) authors looked at XRID and saw something very close to what they needed. But XRID assumed you needed a sequence of descriptors corresponding to an XRI resolution chain. With OpenID a sequence wasn't needed because an http(s) URI would have just one descriptor. So the XRI TC renamed the metadata format to XRD (Extensible Resource Descriptor) and created a separate XML wrapper element called XRDS (XRD Sequence) for cases like XRI resolution where you needed to wrap a sequence of XRDs.

However for cross-compatibility between XRI and OpenID, OpenID discovery just assumed the outer XRDS wrapper element even if it contained only one XRD, and so the discovery format became widely known by the wrapper element, XRDS.

It wasn't until Eran's deep-dive on uniform metadata discovery that he recognized that the base case should be the other way around, i.e., for most URIs the the base discovery document should be an XRD, and only in cases like XRI resolution do you need the XRDS wrapper element.

Since the XRI TC had already made the decision to split off XRDS into a separate spec from XRI Resolution in our next generation of specs, it was easy to just call this new specification XRD 1.0 (1.0 3 reflecting that it is the first standalone specification for XRD). We didn't realize until the XRI TC F2F meeting the day after IIW, however, that XRD as both a metadata discovery format and protocol would be comprehensive enough that XRI 3.0 Resolution could become simply a "profile" of XRD 1.0 —and thus dramatically shorter.

We also didn't realize how badly many different stakeholders want a Web-wide metadata discovery mechanism. Within a week after IIW we had six new people join the XRI TC to be part of the XRD work, and as of this writing nine more are in the queue.

So the roadmap of the next generation of XRI TC outputs is clear now. We will produce two OASIS Standard-track specifications:

* XRI 3.0 (including Syntax, Resolution, and Bindings) as a uniform syntax and resolution protocol for shared semantics across hierarchical URI schemes.
* XRD 1.0 for uniform metadata discovery for any URI or XRI.

Stay tuned for updates - this set of specs are going to set speed a glacier speed record.

SESSION 5

OpenID Trust Exchange (TX) Extension

URL: http://iiw.idcommons.net/OpenID_Trust_Exchange_Extension
Convener: Nat Sakimura, Nomura Research Institute
Notes-taker: T Sakushima, NRI America

What Disscussed

- TX protocol in detail especially "Contract" concept
- Why TX and Why not AX?
- Is the name right?

The presentation slides are here:
http://www.slideshare.net/nat_sakimura/introduction-to-openid-tx-proposed-extension-presentation/

Notes, Key understanding, Questions, Observations, and Action items:

Nat introduced the quote from Gartner. It says that OpenID will continue to be implemented widely, but it will be relegated to low-risk applications unless security weaknesses are addressed and stronger authentication options and secure attribute exchange functionalities are added."Also says that "Avoid OpenIDfor use in financial transactions and other transactions involving sensitive information.

Data encryption, non-repudiation and audit trailing were the requirements for OpenID when JAL decided to use it for its SSO solution among its affiliates.

The highlights of TX are the following:

- Trust Tokens/Contracts are to be stored as legally binding"contract"that can be produced to authority when necessary.
Contracts are signed by two parties(OP/RP) using defined public key cryptography algorithms such as RSA1024bit, DSA, ECDSA.
- Two bindings (POST and Artifact) to meet both broadband and mobile connectivity requirements.
Artifact binding is a TX's protocol binding to communicate in a back channel because of the limitation of many mobile phones which just handle 128kb of data at a time.
- A default data transfer method (key/value pair and RESTful API) is defined in the spec; however, other methods are can be used as far as specified in the contract.
- The asynchronous/artifact binding/notification features are also considered in TX for mobile phone authentication. In this case, the authN is delivered out of redirection flow for web browsers it is done separately in asynchronous manner.
- TX is actually used for Japan Airline(JAL)'s SSO solution with its affiliates(travel agencies). JAL has 25 million millage club members and 3000 transactions per day are handled.

The basic sequence of TX is as follows:
- An user with a browser visits an e-commerce site(RP) and it triggers regular OpenID authentication(ID/Password authN at an OP) when he checks out the shoppingcart at RP.
- After RP shows an order form and the user decided to purchase(by pressing a "Buy" button) and RP check his current authentication status(if level2, strong authN) and redirects him to another OP for strong authN and value-added services such as payment.
- When the user redirected, the RP sends a "Contract" proposal with terms of usage of his data, its digital signature, and its X509 certificate. The RP also initiates the 2nd authN(strong authN) to the OP with value-added services.

- If the OP verifies the signature on the proposal and agrees it from the RP, the OP creates a response message out of the proposal and add data requested into the proposal. The OP signs it and this proposal becomes the "Contract". The OP sends it back to the RP with its X509 certificate.
- The RP verifies the signature on the contract and use the data based on the terms specified in the contract.

There was the discussion if Attribute Exchange(AX) can be used for a mean to implement TX. Dick Hardt suggested defining the payload schema for TX Proposal/Contract data and passing one-time URL pointing to the data through AX. Dick and David Recordon suggested discussing TX capabilities as a part of the AX WG. The current charter must be modified, but using public keys is the common interest, so it is an option for driving TX.

The name "Trust" is fuzzy, David suggested using a different term. Paul Madsen suggested "Contract Negotiation".

Questions?

Q What were use cases and requirements for TX when it was initially developed?
A The primary requirement was to protect PII(personal identifiable information). When PII is passed around among parties, agreement of usage and the authenticity is necessary.

Q In security standing point, SSL protects from eavesdroping and MITM atack when a form is submitted. Why is signature necessary?
A The primary purpose of TX is creation of "contract". Proof of agreement by both parties, non-repudiation, and audit trail are required.

Q What is "artifact binding"?
A It is passing only handles of data not data itself in back channels. SAML has the same protocol binding.

Q How does TX manage (public) keys?
A In the current proposal spec, PR's public key is pushed in request messages.
OP's public key is published in XRDS.

--
Tatsuki Sakushima
NRI Pacific - Nomura Research Institute America, Inc.
TEL:(650)638-7258
SkypeIn:(650)209-4811

Higgins White Paper

URL: http://iiw.idcommons.net/Higgins_White_Paper
Convener: Hank Mauldin
Attendess:

* Mayr Ruddy	* Jeff Stollman	* Nick Givotovsky
* Randy Farmer	* Jim Burks	* Abbie Barbir

Discussed/Considered:
Outline for document

Introduction
- Exec summary
- Audience – tech and business managers
- Problem description – use cases/studies

Context
- Current status

Higgins
- Positioning
- Design Principles
- Architecture
  - Implementations
  - Deployment/ usage
- Did we solve the problems

Conclusion

Health ID Trust

URL: http://iiw.idcommons.net/Health_ID_Trust
Convener: Mike Kirkwood

Mike presented a set of slides that showed a concept of a Health Trust, or common entity, for paying for OpenID, Information Cards stack for consumers and the integration points in the applications they use. The presentation focused on the economics of hooking up Health Providers, Portal Providers, and Identity Providers. It showed that in simple terms, the model for charging enterprise licenses for each Health Provider to join the OpenID or Information Card was a dis-incentive to adoption, as each company pays for the same person, and each integration point the person's total ID provider costs go up. It creates additional costs to service providers and creates risk for them in preparing for growth of their user population, as well as operational overhead in managing the licenses. The group agreed that it does make sense to look at the economics of a Health Trust, and that it would be closer to the model in countries that provide common health services.

Next steps discussed:
1) Start a script of user scenarios for using a health stack [not started yet]
2) Start a review of a user centric health stack could include several technology components. A brief description of how each might be part of a package provided to consumers.

OpenID. A unique OpenID could be reserved for each of the people represented by each country

that supports Health ID Trust. The system assumes a total of all population. It is the logon accepted at each site I use when I want to prefill information about myself. Since there are privacy concerns with ID/Pseudonyms, it is expected that a set of level of obscurity lives between the site and the requester of information and logon. It is this ID that all common reporting will be run for validating base information requests.

OAuth is setup as a way for me to have an secure channel for assertions between me and my providers, and my providers and other partners I may access. It is focused on the mechanics around certificate discovery and validation between endpoints. A relying party arrangement is setup for me between My Portal (if any) and my primary doctor. As well, I am setup with keys to providers that support my health portal, and am creating a relationship with them that allows me to be private and portable in several directions (my portal keeps a snapshot of aggregate keys and monitors apps that it uses, an individual app can be converted between portals).

Discovery is the mechanic that allows me as a consumer to use my data around my health to find services that match my needs. A key part of the Health ID Trust is enabling a key set of attributes and values that support robust and flexible discovery mechanics. It is expected that this will be a hybrid set of tools and functions, tying into existing processes and communication tools such as B2B, tag-clouds, seo, and web sites, as well as be directed to a more robust set of processes that support rich discovery requests by a person to an provider. [The HTSPE specifications for Hospital Emergency Status EDXL is a good example of discovery that will help the user find the right hospital in an emergency]

Representation is a set of tools that allow discovery to be fulfilled by a vendor. This will follow industry standard documents, freeform, and conform vocabularies (ndc, rxNorm) and other specific company vocabularies

Information Cards are used to provide a base set of information for the user, available by exchanging the card. In this stack, information cards are going to be used for several things for a person in their life, and different combinations of the cards will support different sharing scenarios. There will be individual cards (company @ provider) and generic card for all health, that allows base information exchange across all systems. This one is the one intended to be printed.

HIPPA compliance of the receipt of information across the endpoints, and validity of the person as they sign up will require a second form of authorization, this will be grouped with information in the discovery. A set of information cards that contain credentials with signing authority to receive documents will be the goal. The endpoints are extended to real signature, ip address, voice, photo, or in-person in different situations. An all online solution is the goal of this base flows this stack will support for consumers, with appropriate caveats for key out-of-band processes and situations.

CCR - The Continuity of Care Record specification from ANSI is a key piece of current health provider portability. The Health ID Trust supports a base form, as well as mechanics for further delegation of elements, updates to the code, and key vocabulary maps required to manage the integration. HC7, CCD, EDXL and other industry standards are invited to participate.

Data Portability frameworks support the base mechanic and expectations from parties sharing the data. In Health ID Trust, it is a set of agreements and governance for each of the key parties that

participate. ID Providers, Portal Providers, Application Providers, Health Providers, Payor Providers, Friends, Family, Doctors. [LINK]

WhiteList will be used to allow each party, for example portal, to define a set of end points for parts of the Open ID and extended fields and documents that are exchanged between parties. At the base level, it says whether an account can be imported into another system and that endpoint being the host location for the profile. Health ID trust is requesting a peering relationship with all these models to support this in the open terrain.

Family ID. A similar concept to OpenID, but for family validation. This is a mechanic that is validated by a marriage license, and is a new entity that binds the individual identities for individuals. It is leveraged and verified for legal and tax records.

FOAF (Friend of a Friend) Used to pull in contacts from applications and sites.

XFN Used to pull in contacts from applications and sites.

Certificates for connecting CCRs between providers, Health ID Trust, and portals is done through issuing certificates that can leveraged through systems like XRDS, ebXML, and other mechanics to share information between providers on behalf of a person.

Proofing for validating information access in paper form and levels of access, will be represented as flags in profile, with contextual processes on how to process based on requirements of system. Base case will include: in-person, photo, signature, voice

Session between providers is a key domain of the portal, which will have the UI controls for managing the experience for the user. Mechanics to authorize data will be done at the ID provider and not require session between consumer and information flow.

ebXML registry can represent HC7, CCD, RxNorm, and other industry vocabularies between parties, starting at the authoritative source and provide a mapping layer.
VRM

Hardware Based ID Exchange for Social Networking

URL: http://iiw.idcommons.net/Hardware_Based_ID_Exchange_for_Social_Networks
Convener: David Brown
Notes-taker(s): David Brown

Technology Discussed/Considered:
Hardware Tokens and Mobile phone applications for transferring contact data between users.

Discussion notes,

Hardware ID Tokens for Social Networking
Some observations from Poken's experience
User needs
Authentication (a web 1.0 problem)
- Bank login
- Corporate VPN

Exchange of IDs (a web 2.0 problem)
- Lets meet on facebook, etc.
- Portable contacts / open social

Price
- Low cost hardware is possible

Anatomy of a token 2.0
Communicate between themselves
- To transfer IDs

Process/Store
- manage an ID securely
- Record communicated IDs

Communicate to a computer/the Internet
- Relate the Token IDs to identity card data

1) Communication between Tokens
Wireless?
- WiFi, Bluetooth, IR – all have "crowded room" and parametization problems
- RFID, NFC – passive/active problem

Physical connection?
- Not user friendly

Mobile phone based?
- Needs s/w install, fragmented hardware/OS market
- Wireless (WiFi, Bluetooth, IR) - as above
- Camera, QR code
- Operator vs. manufacturer politics/conflicts

1) Communication between Tokens
The solution (according to Poken)
- Needs a spontaneous data exchange solution designed for this purpose
- Usability/ergonomics important for this specific human interaction
- Wireless is most natural
- Active/active
- Small form factor & price

2) Process/Store

Low end processor
    Can work around processor limitations to do 128bit encryption/authentication because data transfer siue is small
Store communicated IDs
    FIFO store (eg. For last 64 contacts)

3) Communicate to a computer/Internet
USB works fine
    Emulate USB mass storage
Computer provides:
    Internet networking
        TCP/IP, DNS
        SSL over the internet
Web infrastructure provides:
    Token ID to Identity cards data
    Data portability, APIs
    Future: OpenID providers, Higgins, etc.

Token 2.0 side features
Timelines
Parental control
    If my child met them in the real world then they can friend them online
Low cost alternative for some Token 1.0 uses
Trust

XRDS for Open ID and Information Cards

URL : http://iiw.idcommons.net/XRDS_for_OpenID_and_Information_Cards
Convener: Axel Nennker
Notes-taker(s): Axel Nennker

Technology Discussed/Considered:

XRDS, Open ID, Information Cards

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

We had some discussion about XRDS for Open ID yesterday already and there seems to be some support in the Open ID community. But there wasn't any real conclusion.

Future steps:

- Write the spec for IC and submit it to the ICF Browser Ltegialia(?) WG
- Write spec for Open ID and submit to an Open ID Foundation WG

SESSION 6

Productizing the Open Stack

URL: http://iiw.idcommons.net/Productizing_the_Open_Stack
Convener: Johannes

Concordia User Identity Reference Model

Convener: Marty Schleiff
Participants:

- Marty Schleiff
- Lucy Lynch
- Macduff Hughes
- Henrik Biering
- Paul Bryan
- Randy Farmer
- Drummond Reed
- Hank Mauldin
- Bob Morgan

Technology Discussed/Considered:

Development of a Concordia User Identity Reference Model

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

We listed links to related information:

- Concordia Wiki - http://www.projectconcordia.org/index.php/Concordia_Identity_Reference_Model
- Evolution of an example model - http://identityhappens.blogspot.com/
- OpenLiberty Identity Landscape - http://www.openliberty.org/wiki/index.php/Identity_Landscape#Identity_Domains
- Higgins Data Model Intro - http://www.eclipse.org/higgins/documents/Higgins-Data-Model-Intro.ppt
- Higgins Context Data Model - http://wiki.eclipse.org/Context_Data_Model_1.1
- Abi & Colin mention an ISO model that cannot be shared at this time.
- SIG 17 at ITU-T is doing closed work around identity that includes a model.

We tried to get concensus about what a Digital Identity is, and didn't quite get there. Some thoughts included:

- A bag of attributes of something which collectively match exactly one entity, usually including at least one identifier.
- Digital Identity is not just about authentication or authorization, but commonly used for that.

We discussed some approaches we might take to build a model:

- Bob asserts big organization notion of an identity model different than other notions.
- Randy – let's do the least possible. He's interested in the common pieces of an identity model. A clean way to graphically describe the minimal digital identity that is used in distributed identity systems.
- Paul - Define common design patterns that people can adopt, rather than redefining their own new patterns. For example Grouping is a common design pattern.
- Marty – maybe other design patterns would be user, account, privilege, etc.
- Lucy – interested in the pieces that can be defined into workflow diagrams about the use of identity information, and other useful diagrams. Maybe the pieces are like Vision icons used to compose diagrams.

Several expressed interest to continue discussions:
Hank, Paul, Bob, Lucy, Macduff, and Marty expressed interest to continue the discussion (did I forget anyone?). Maybe others are interested to, but some people had already left by the time we asked who wants to continue.

The Tripartite Identity Pattern

URL: http://iiw.idcommons.net/The_Tripartite_Identity_Patter
Convener: Randy Farmer
Attendees:

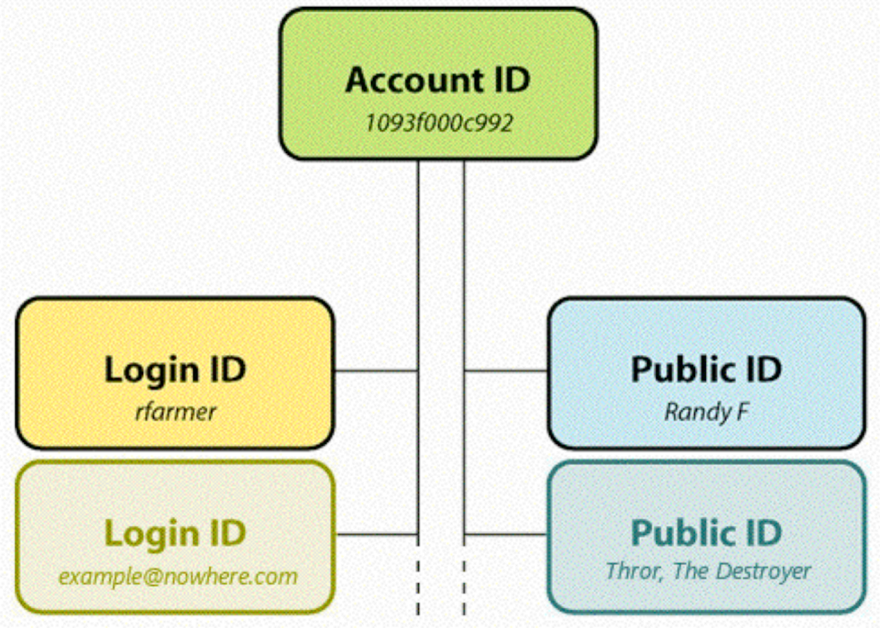
* Skip Baney
* Cliff Gerrish
* Jim Fenton
* Joon Nak Choi
* Nika Jones
* Jon Canlas
* Lisa Dusseault
* Jeff Stollman
* Larry Cynki

I updated my blog post on this topic with the session notes. The original post is here: http://thefarmers.org/Habitat/2008/10/the_tripartite_identity_patter_1.html

One of the most misunderstood patterns in social media design is that of user identity management. Product designers often confuse the many different roles required by various user identifiers. This confusion is compounded by using older online services, such as Yahoo!, eBay and America Online, as canonical references. The services established their identity models based on engineering-centric requirements long before we had a more subtle understanding of user requirements for social media. By conjoining the requirements of engineering (establishing sessions, retrieving database records, etc.) with the users requirements of recognizability and self-expression, many older identity models actually discourage user participation. For example: Yahoo! found that users consistently listed that the fear of *spammers farming their e-mail address* was the number one reason they gave for abandoning the creation of user created content, such as restaurant reviews and message board postings. This ultimately led to a very expensive and radical re-engineering of the Yahoo identity model which has been underway since 2006.

Consistently I've found that a tripartite identity model best fits most online services and should be forward compatible with current identity sharing methods and future proposals.

The three components of user identity are: the *account identifier*, the *login identifier*, and the *public identifier*.



Account Identifier (DB Key)

From an engineering point of view, there is always one database key - one-way to access a user's record - one-way to refer to them in cookies and potentially in URLs. In a real sense he account identifier is the closest thing the company has to a user. It is required to be unique and permanent. Typically this is represented by a very large random number and is not under the user's control in any way. In fact, from the user's point of view this identifier should be invisible or at the very least inert; there should be no inherent public capabilities associated with this identifier. For example it should *not* be an e-mail address, accepted as a login name, displayed as a public name, or an instant messenger address.

Login Identifier(s) (Session Authentication)

Login identifiers are necessary create valid sessions associated with an account identifier. They are the user's method of granting access to his privileged information on the service. Historically, these are represented by unique and validated name/password pairs. Note that the service *need not generate* its own unique namespace for login identifiers but may adopt identifiers from other providers. For example, many services except external e-mail addresses as login identifiers usually after verifying that the user is in control of that address. Increasingly, more sophisticated capability-based identities are accepted from services such as OpenID, oAuth, and Facebook Connect; these provide login credentials without constantly asking a user for their name and password.

By separating the login identifier from the account identifier, it is much easier to allow the user to customize their login as the situation changes. Since the account identifier need never change, data migration issues are mitigated. Likewise, separating the login identifier from public identifiers protects the user from those who would crack their accounts. Lastly, a service could provide the opportunity to attach multiple different login identifiers to a single account -- thus allowing the service to aggregate information gathered from multiple identity suppliers.

Public identifier(s) (Social Identity)

Unlike the *service-required* account and login identifiers, the public identifier represents how the user wishes to be perceived by other users on the service. Think of it like clothing or the familar name people know you by. By definition, it does not possess the technical requirement to be 100% unique. There are many John Smiths of the world, thousands of them on Amazon.com, hundreds of them write reviews and everything seems to work out fine.

Online a user's public identifier is usually a compound object: a photo, a nickname, and perhaps age, gender, and location. It provides sufficient information for any viewer to quickly interpret personal context. Public identifiers are usually linked to a detailed user profile, where further identity differentiation is available; 'Is this the same John Smith from New York that also wrote the review of the great Gatsby that I like so much?' 'Is this the Mary Jones I went to college with?'

A sufficiently diverse service, such as Yahoo!, may wish to offer multiple public identifiers when a specific context requires it. For example, when playing wild-west poker a user may wish to present the public identity of a rough-and-tumble outlaw, or a saloon girl without having that imagery associated with their movie reviews.

Update 11/12/2008: This model was presented yesterday at the Internet Identity Workshop as an answer to many of the confusion surrounding making the distributed identity experience easier for users. The key insight this model provides is that ***no* publicly shared identifier is required (or even desirable) to be used**

for session authentication, in fact requiring the user to enter one on a RP website is an unnecessary security risk.

Three main critiques of the model were raised that should be addressed in a wider forum:

1. There was some confusion of the scope of the model - Are the Account IDs global?

   I hand modified the diagram to add an encompassing circle to show the context is local - a single context/site/RP. In a few days I'll modify the image in this post to reflect the change.

2. The term "Public Identity" is already in use by iCards to mean something incompatible with this model.

   I am more than open to an alternative term that captures this concept. Leave comments or contact me at randy dot farmer at pobox dot com.

3. Publically sharable capability-based identifiers are not included in this model. These include email addresses, easy-to-read-URLs, cel phone numbers etc.

   There was much controversy on this point. To me, these capability based identifiers are outside the scope of the model, and generating them and policies sharing them are withing the scope of the context/site/RP. Perhaps an interested party might adopt the tripartite pattern as a sub-pattern of a bigger sea of identifiers. My goal was not to be all encompassing, but to demonstrate that only three identifiers are required for sites that have user generated content, and that no public capability bound ID exchange was required. RPs should only see a the Public ID and some unique key for the session that grants permission bound access to the user's Account.

SESSION 7

Consumer Auth – Who Cares?

URL: http://iiw.idcommons.net/Consumer_Auth_-_Who_Cares%3F
Convener: Louie Gasparini
Presentation of Deck given at RSA Europe

* **Internet Services Begin Safe & Convenient**
* May 1995 – Wells Fargo Launches Internet Banking
  - Limited offerings meant few passwords to juggle
  - SSL Encryption was secure enough
  - Phishing and Malware non-existent
  - Banking & Electronic Commerce was Safe & Convenient

As more services became available a new challenge arose

How to Manage Multiple Passwords!

* **The Password Management Problem**
  - Average user has 6.5 password shared across 3.9 sites
  - Users averaged 25 accounts that require passwords
  - Users typed their password 8 times a day
  - Most users choose lower case only passwords unless forced to do otherwise
  - 0.4% of users annually typed passwords at phishing sites
  - 1.5% of Yahoo users forgot their password each month

    -> Matches what I have seen in Internet Banking Sites
  - password is the most popular password
  - password1 was used .22% of all myspace accounts

* **What do consumers want ?**
Convenience! (image of post-its around computer)

* **Centralized Authentication as the Solution**
Can there be a single ID provider for all web sites?

* **Banks as the Consumer Authenticator**
- As we now reminded, banks are built on trust
- For a bank to play in this arena, it must be secure
- In late 1990s, banks explored options here
    - Certificate Authority- Who is the root?
    - Smart Cards - Mondex
    - Bank branded client side wallets - SET
        - 971 pages to describe SET!
- Ultimately, banks did not enter into this market
    - Heavy weight solutions & lack of convenience
    - US Bank Mergers & Y2K shifted internal focus

However, "Verified by Visa" does demonstrate a potential model for financial institutions

* **Consumer Authentication Scorecard**
Banks as the Authenticator

Requirement	Banks
Convenience	✗
Privacy	✔
Safety	✔
Coverage	✗
Control	✗
Trust	✔

* **Microsoft Passport – Single Sign-On**
- Microsoft Passport launched in 1999
- Positioned as single sign-on for all web sites
- Criticized by the Electronic Frontier Foundation in 2001 for privacy concerns
- Resulted in Federal Trade Commission ruling
- Criticized in 2003 for security flaw
- Industry competitors and other concerned entities worked to form alternative solutions

* **PassPort Privacy Terms**
* **Passport Security Flaw Identified**

* **Consumer Authentication Scorecard**

Requirement	Banks	PassPort
Convenience	✗	✔
Privacy	✔	✗
Safety	✔	✗
Coverage	✗	✔
Control	✗	✗
Trust	✔	✗

* Can governments be the consumer authenticator?

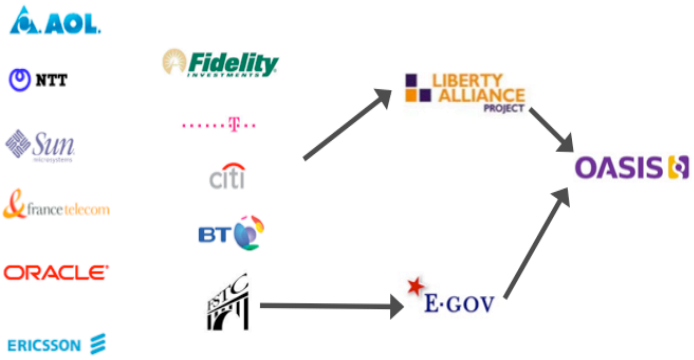
* Consumer Authentication Scorecard

Requirement	Banks	PassPort	Gov
Convenience	✗	✔	✗
Privacy	✔	✗	✔
Safety	✔	✗	✔
Coverage	✗	✔	✗
Control	✗	✗	✗
Trust	✔	✗	✔

* **Federated Authentication?**
Can there be multiple federated authenticators for web sites?

* **Liberty Alliance**
- Formed in 2001 to establish open standards, guidelines & best practices for federated identity management
- Contributed spec to OASIS and became SAML 2.0
- Popular in business use cases for partner and customer authentications
- Introduced Identity Assurance Framework (IAF) in August 2007
    - Supports mutual acceptance, validation and life cycle maintenance across identity federations
    - Extends EAP Trust and US e-auth frameworks

* **Finance, Government and Corporate Use Cases**



* Consumer Authentication Scorecard

LIBERTY ALLIANCE PROJECT — Similar to Banks and Government

Requirement	Banks	PassPort	Gov		
Convenience	✗	✔	✗		
Privacy	✔	✗	✔		
Safety	✔	✗	✔		
Coverage	✗	✔	✗		
Control	✗	✗	✗		
Trust	✔	✗	✔		

* **Centralized? Federated? Who's in control?**
What problem are we trying to solve?
"Why did Intuit bring Quicken to market and beat the banks at home banking?
Because the banks forgot about the consumer." - Scott Cook , Intuit Founder

* **Authentication for the Consumer**
What is OpenID?
- OpenID eliminates the need for multiple usernames across different websites, simplifying your online experience.
- You get to choose the OpenID Provider that best meets your needs and most importantly that you trust.
- OpenID is still in the adoption phase and is becoming more and more popular.
- Today it is estimated that there are over 160-million OpenID enabled URIs with nearly ten-thousand sites supporting OpenID logins

Source - OpenID.net

* **Authentication for the Consumer**
- Easy to use – louiegasparini.aol.com
- Wide industry support

AOL Google YAHOO! Microsoft VeriSign IBM myspace.com a place for friends

* **Consumer Authentication Scorecard**

OpenID

Requirement	Banks	PassPort	Gov	Open ID	
Convenience	✗	✔	✗	✔	
Privacy	✔	✗	✔		
Safety	✔	✗	✔		
Coverage	✗	✔	✗	+	
Control	✗	✗	✗		
Trust	✔	✗	✔		

* **Authentication for the Consumer**

✔ OpenID is Open!

! OpenID is Open!

What about Security?

* **Willie Sutton**
  - "Slick Willie"
  - Robbed ~ 100 banks 1920's -1952
  - Executed robberies in disguises
  - "Gentleman", in fact, "quite polite", like being at the movies
  - When asked why he robbed banks, Sutton simply replied, "Because that's where the money is."

* **Security Concerns**
  - Open – Any site can use OpenID
  - Increases vulnerability to Phishing
  - SSL is not required in spec
  - Introduction of third party (ID provider) adds complexity
  - Who controls the quality of the identification
    - The end user based on the ID provider they select?
  - ID Provider has knowledge of every login

OpenID was designed by a blog site for blog usage
OpenID can benefit affiliated sites

Cross site support will grow from business needs of the sites not from needs of the users
Perhaps it is better to be called ClosedID?

* **Consumer Authentication Scorecard**

Requirement	Banks	PassPort	Gov	Open ID
Convenience	✗	✔	✗	✔
Privacy	✔	✗	✔	✗
Safety	✔	✗	✔	✗
Coverage	✗	✔	✗	✗
Control	✗	✗	✗	?
Trust	✔	✗	✔	✗

* **Authentication for the Consumer**
  - Is OpenID really all that open?
  - All major sites that support OpenID are providers ONLY
  - OpenID was designed by a blog site for blog usage
  - OpenID can benefit affiliated sites
  - Cross site support will grow from business needs of the sites not from needs of the users
  - Perhaps it is better to be called ClosedID?

* **CardSpace**
MicroSoft CardSpace
- Client Side Software for Identity Selecting
- Stores references to identities, presents them as visual cards
- Provides a consistent UI for ease of use
- Can contain identities and claims
- Can be managed (issued) or personal (self issued)
- Built on top of WS-*
- Token format agnostic, can work with OpenID, SAML & Windows LiveID
- CardSpace is infrastructure not an authority

* **LiveID**
- Originally .net Passport
- Used mainly for Microsoft and affiliate sites
- Email security flaw in 2007 quickly addressed
- MS hired Kim Cameron a prominent critic of PassPort
- LiveID is a cornerstone for MicroSoft web properties

* **Consumer Authentication Scorecard**

Requirement	Banks	PassPort	Gov	Open ID	LiveID
Convenience	✗	✔	✗	✔	✔
Privacy	✔	✗	✔	✗	? +
Safety	✔	✗	✔	✗	✔
Coverage	✗	✔	✗	✗	✗
Control	✗	✗	✗	?	?
Trust	✔	✗	✔	✗	?

* **Private**
- Password Managers
- Desktop, Portable or Network Based
- Destination Sites do not need new software
- Privacy & Security under control of the credential owner
- Most implementations are convenient and safe
- Can offer additional features such as form fill and content management services

* **Desktop Password Managers Issues**
- Master key & encryption strength
- Keys may be stored in the clear after unlocking
- User must deal with data management of their hard drive
- Portability between machines is cumbersome at best
- Convenience, privacy, safety & coverage are pretty good
- Information Cards – Offers this feature
    - Default is no master key (windows protection)
    - Can lock all with one PIN

* **Portable Password Managers Issues**
- Pretty good encryption
- Must have your hardware component with you
- Some users will view this as less convenient
- If you loose it, you must start from scratch
- If you keep a backup, how do you keep that secure?
- Still need to be a data manager
- Convenience, privacy, safety & coverage are pretty good

* **Network Based Password Manager Issues**
- Web site that securely stores login details
- Login details managed and accessible in the network
- Accessible from the network with proper authentication
- Eliminates risk of loss of data due to lost or damaged personal computer
- Risk of compromised master login is the same as central, federated and open models
- Privacy, trust, coverage and convenience can be superior
- Safety can be addressed with additional security features

* **Consumer Authentication Scorecard**

Requirement	Banks	PassPort	Gov	Open ID	LiveID	Private
Convenience	✗	✔	✗	✔	✔	✔
Privacy	✔	✗	✔	✗	? +	✔
Safety	✔	✗	✔	✗	✔	✔
Coverage	✗	✔	✗	✗	✗	✔
Control	✗	✗	✗	?	?	✔
Trust	✔	✗	✔	✗	?	✔

*** Conclusions**

- Finance, Government & B2B use cases will benefit from Oasis & Liberty Alliance efforts
- Portals, ecommerce sites & their affiliates will benefit from “closed” solutions that may be proprietary or based on Open standards (LiveID , OpenID, Facebook Connect)
- The consumer looking to solve their password management problem can benefit today from password managers with appropriate security features

VRM UI Session

URL: http://iiw.idcommons.net/VRM_UI_Session
Convener: Doc
Attendees:

* Joe Andrieu
* Drummond Reed
* John Bradley
* Johannes Earnst
* Nick Glvotovsky
* Judi Clark
* Abby Jenkins
* Greg Biggers
* Mary Hodder
* Hank Mauldin
* Kevin Marks
* Christopher Carfi

Lots of r-button projects in progress
* Iain Henderson's Personal address manager
* Implementation for radio apps / iPhone
* Radio Paradise reference app

Three states; two icons
- Nothing
- Open (actions availabe, none take)
- Closed (relationship action has been taken)

Reason for r-button: enable REAL relationships between individuals and vendors/entities; not 'fake' relationships of CRM
Rbutton started as ways to represent relationship
Rbutton specifies (person who marked up page) must represent entity to have relationship with
    URI the mechanism?
What about in chrome of browser?
What about the variety of entities?
What about scalability if you're polling 100 entities on a page?
    Feasibility in practical terms - too much computational overhead?

* Job of Relationship manager = discover all relationship services; contact them; determine if/who I have relationships with

* User Agent uses RM to poll RS for entities
* We don't need a standardized entity ID, but pockets of shared identifiers
    You don't need a URI - could be well-formatted XRI/h-card/semantic data about an entity
* A URI could be used as a discovery service rather than UID, showing us which RS's are available

Alternative: Quad-state r-button (only shows one half) - this would show when vendor is at the table vs. just user-driven relationship services.

How is r-button different from an aggregator that figures out preferred online service provider for users? (i.e. r-button is

only part of the VRM discussion; how does this really change things?)
    Answer: services must be VRM compliant
    Outcome: the specific cases for r-button today are not particularly compelling, but are good for describing and specifying
    Payment escrow, medical records, and personal RFP is very different from r-button service aggregation and offer a compelling vision of the future use of a distributed, user-driven relationship ecosystem
* Three groups of RS's (vendor, user, third-party)

TWEETS & PICS:
@drummondreed whiteboard of how relationship discovery works for rbutton entity relationship services #vrm #iiw2008b http://twitpic.com/lecm

Quad state r-button vs tri state r-button photo #VRM #IIW http://twitpic.com/ldmn

The Value of Verified Identity (Verified Claims)

URL: http://iiw.idcommons.net/Value_of_Verified_ID
Conveners: Denise Taylee, RL "Bob" Morgan
Attendees:

* Matt Klein	* Jeff Stollman	* David Brown
* Jeff Shan	* Kevin Trills	* Terry Hayes
* Marty Schleiff	* Lucy Lynch	+ dozen more

Technology Discussed/Considered:
Relying party and identity/claim provider relationships where data about subjects is "verified" rather than ? asserted.

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

"Verified" is probably too narrow a concept. The real differentiation for some claims/attributes is that they are claimed by the asserting party to be useful for or compliant with some defined business process. This might involve some defined verification method (or set of methods) but might also involve things like user consent, notification of others (eg parents), auditing etc… The state of the art is to bake notions of "verified" (etc…) into claim definitions or business agreements. An interesting subject is permission management ("can use feature X"). Defining authority is not always clear, ef for age. Large intersection with Level of Assurance concepts.

Adding "verified" or "complaint" decoration to each delivered claim is appealing but too complicated so far. Many of their issues were dealt with in PKI certificate policies 15 years ago, but this has seen little use, and even there proliferation of per-company policy attributes was a problem.

Sub-Service Discovery From OPS

URL: http://iiw.idcommons.net/Sub-Service_Discovery_Form_OPS
Convener: Joseph Smara, Eric Sams

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

- Consensus that it's useful for RP's and users to get access to the user's services
- Probable that OP's could support opt-in censer to release this data
- Strawman technical proposal using AX and URI's for each service

SESSION 8

Combining OpenID and SAML

URL: http://iiw.idcommons.net/Combining_OpenID_and_SAML
Convener: Hiroki Itoh
Attendees:

* Paul Madsen
* Dave Crocker
* Greg Havercamp
* Shin Adachi
* Nat Sakimura
* Tatsuki Sakushima
* Vijay Simha

Technologies Discussed/Considered:
Proxying Assurance through SAML
Authentication Context and OpenID PAPE

Discussion Notes:
* More and more use cases have protocols sequenced
* Sequencing OpenID and SAML may require maping between OpenID PAPE and SAML Authentication Context
* May need to provide guidance on how to map between OpenID PAPE & SAML AC
* Project Concordia will have a demo of these use cases at RSA 2009

Activitiy Streams / Portable Activities

URL: http://iiw.idcommons.net/index.php?title=Activity_Streams
Conveners: Will Noris & Kevin Marks

Strong Auth Usability + Demos

URL: http://iiw.idcommons.net/Strong_Auth_Usability_and_Demos
Convener: Eric Sachs
Notes-taker(s): Eric

To see videos of this session go to:

http://sites.google.com/site/oauthgoog/UXFedLogin/strongauthvideos

Proxying Assurance for Open ID & SAML

URL: http://iiw.idcommons.net/Proxying_Assurance_for_OpenID_and_SAML
Convener: Paul Madsen
Notes-taker(s): Paul Madsen

Technology Discussed/Considered:

Proxying assurance through SAML
Authentication Context and Open ID PAPE

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

- More and more use cases have protocols sequenced
- Sequencing Open ID + SAML may require mapping between Open ID, PAPE + SAML authentication context
- May need to provide guidance on how to map between Open ID, PAPE + SAML AC
- Project Concordia will have a demo of these cases at RSA 2009

Exploring the Construction of Online Identity + Definition of Terms

Exploring the Construction of the Online Identity

Convener: Thu-An Bui
Notes-takers: Alex Rosen, Kaliya Hamlin
Attendees:

* Larry
* Alex Rosen
* Kaliya Hamlin
* Tim Burks
* James McLaughlin
* Jeff Stollman
* Mary Breusake
* Dave Brown
* Jeff Hodges
* =NRG

Discussion notes:

Questions:
Information

Poken to
Location based tools – more contextual information, also time stamped

I came to IIW thinking it was going to be something else.
More Social Media, Marketing, Online Reputation Management
How you manage your presence online.

That is what all the people who will use this stuff will eventually care about – they care about how it manages their presence.

People signed up for google, yahoo, plaxo.
From what I have heard OPenID – universal identity – a lot of it is how do you communicate to the users what the technology is in a way that is not scary.

There are a lot of people here talking about identity plumbing
Riffing on that – there is a scenario – people here are working on BETA-Max and VHS is going to wipe us out. Facebook = VHS

Look

Kaliya had convos w/ adults that facebook freaks them out – regular people. Until you have the last person who uses rotary phones die, you have older people who don't use facebook the same way younger people do

Facebook is a sucky app, despite it, has the presence.

Sites that accept open id? who accepts FB Connect? CBS

Scenario – risk that is not being acknowledged – almost being dismissed

Business factors, user acceptance → drives to adoption

What plumbing will be most widely adopted in the most winning mass audience, consumer space

Influence, factors of importance?

Strong enough understanding – msft passport was fought? FB Connect is similar
Not seeing the evil empire backlash

The difference is facebook is easiest.

I think some of the backlash –
Facebook is an alternative

An: SO that is one way of looking at online Identity.
Asking the room about

Online reputation management from a consumer perspective.
How do you think about yourself and how do you present yourself online – constructionist framework

All of you atriubtes – the stuff you put into a form.
When you think about personal online identity – which of those frameworks and why

Judi – context – who do you talk to and
What kind of person do you need to be in the world – personal representation, representation of the company,

Active -
Passive – googling self seeing what people say

Ipseity – features unique to you (DNA, Date of birth)
Transiant – attributes unique to you. (Age)
Contextual – multiple persona

Community does not do a good job of sharing the lexicon
Different people mean different things about authentication

What I would like to get out of this discussion.
Yes there is an issue of we are all part of "a" community.

We haven't figured out what it

Identity
There is a clear definition
How do you integrate people who don't have background and what to become involved
How do you get them involved with the least pain as possible
How do you leverage their talents and ability

People might be might be new to the community.
Vastly larger community – that has a different community.

One of the complexities.

What does identity mean – extremely many facited notion
The stuff that is unique to our innerselves

Federated identity – reputation and trust
Selves as member of groups

Citizens – rights responsibilities

Economic profile

'the digital us" trackable in a digital world.

Digitalidcoach.com/ - identities tab

Lexicon – not clear and agreed upon.
Jeff questioned its usefulness

Issue of Control that we are asserting over identity.
"who is we"
Consumer control of what the

Constructionist – my personal story – what are the tools I will use to create my online identity – twitter and a blog, it is a skill we need to teach people – how they construct it online.

Mistaken notion that one can own one's identity.

We in the online world use the word online identity to much.
Best way to influence online identity

Erving Goffman – Presentation of the Self

We can influence it –
The notion of identity is contextual.

My notion of my identity or his notion of my identity

Do you think it could be called identity - reputation

Not the same –

Reputation is the uttering of the image

Powerful thing about facebook and twitter.

Project and construct views of people.
=JeffH – his attempts presenting himself

Three different cases
Varying level of "careful"
What does it mean to be careful?

This comes into play when using online dating service

Spectrum of findability—some people want to be more some want to be less

Natural names and identifiers are not congruent, but they're intersecting. They only intersect a little in global sense. Task of id system when deploying is deciding how much you want them to intersect. Hard to make a strong intersection—often makes people unhappy.

Future of Reputation, Daniel Solove—read
Also- Digital person
Understanding privacy
He suggests changes to regulatory and legal environment to better accommodate identity

Japanese laws on spam are on per message action.

But what should the regulation be and who should regulate?
Govt should be more transparent with data they have on us, so should all entities
Facebook should have to tell us everything they store about us

Have to consider EULAs. These often make people waive rights without them knowing.

Going to where people don't want to be repositories of all this info anymore. It's burdensome. Do we want entities thathandle this and compete for business?
This is taking a long time to come about
Credit Bureues

How does this fit into a verified identity model with naming? How to name things so endusers understand?
Personas? These are contextual
Attributes?

Potential outcome: How to define/explain these terms to public. Could we make common craft videos for key concepts in this space so people can understand us?
Mass market users care what this does for them, not what it's called.

Persona or Profile??? Do people know what persona means?
OECD paper on 'what is identity'

Narrow the frame andthen define the term within the frame, or else you end up in circles.

Personhood has been argued over for many thousands of years. In legal sense, a corporation is a person. Corporations also have brand identities.

Paper by Eric Olson. Go to Stanford Encylopedia of Philosophy. 'The problems of personal identity.'

Danah Boyd has research on after death digital shrines. Facebook papers, etc. being taken over after death to preserve and spread information.

What's next? Do we want a Google Groups, a wiki to make a glossary?
YES!!!
Can use ID Commons wiki

What are the colloquial uses of these terms as they're actually used online and really
Don't want the ontological framework for the existential condition

Context setting comes before definition.

SESSION 9

Non-CorrellatableID with OpenID 2

URL: http://iiw.idcommons.net/Non-CorrelatableID_with_OpenID_2
Convener: Joe Andrieu
Attendees:

* Yarvi Adam	* Jim Fenton	* Scott Bloomquist
* Terry Hayes	* Steve Williams	* Jeff Stollman

We talked about OpenID, in multiple versions: 1.0 and 2.0
1. non-correlatable stuff isn't always used! Yahoo!

2. good to have post-facto correlation (at dashboard level)

3. Suggested pattern, which we should advocate
always use directed id (non-correlatable tokens)
allow discoverable persona (display names)
allow public, authenticated ID (for reputation)
allow post-facto, intentional correlation (for

It seems that the lack of these things are reasons NOT to adopt modern identity approaches, so we should find a unified way to enable all of these, to get the broadest number and type of applications using identity.

We also talked about why we want non-correlatable ids, or directed Identity.

Noted that by teaching people to use OpenID, we are teaching them to use correlatable IDs. But in fact, we would do well to invest our energy teaching folks that are non-correlatable.

Does the non-correlatable technology give folks a false sense of privacy, when they are actually almost always giving far more data that, in fact, enables correlation?

1. we need to educate to protect identity
2. we need to give ways to enable that protection

Without giving a false sense of security.

Desktop and Mobile Client UI Support for Federated Login

URL: http://iiw.idcommons.net/Desktop_and_Mobile_Client_UI_Support_for_Federated_Login
Convener & Notes-taker: Eric Sachs

Discussion notes:

UX research on Desktop Apps using federated login and/or OAuth

Last updated: Nov 5, 2008 8:56 PM
If a website exposes APIs for private user data that are accessed via rich-client applications (desktop apps, J2ME mobile apps, etc.), then it can be hard for that website to become a relying party for federated login. The reason for this is that most desktop apps have a hardcoded user interface that asks for E-mail/Password to authenticate users. The same is true for websites which expose APIs, but which authenticate users via some second fatctor auth solution such as USB tokens, phone, InfoCard, etc. While the website with the API might be able to easily changes its login flow by updating code on its servers, it can be much harder to update the code on all the rich-client applications, especially if some of them were built by 3rd party developers.

Google has been evaluating the user experience of federated login in rich-client apps to determine what method can be used, assuming the website owner and client app developer are willing to modify their code. This document describes a prototype that we built and tested with our user research team.

One of the options we considered, but did not pursue, was to force all users of the the desktop app to use the OAuth protocol to authorize the app to access the user's data. Roughly that flow would take eight steps as listed below:

1. User clicks sign-in on the app
2. User is told they will be redirected to a web browser to authorize the client app to access their data
3. The web browser is launched and the user is sent to the login page of the website with the data. If that website uses second factor auth for authentication, then it could send the user through the standard flow for that authentication process.
4. If that website was a relying party for federated login, then the user could indicate their IDP on that RP website, and they would be redireted to the IDP to authenticate (and that IDP might in turn use second factor auth). If the user's account was not associated with an IDP, then they could authenticate directly to the RP website.
5. Once the user was logged in, they would be shown a screen that describes the application asking for their data, and asks the user if they approve giving that app access to their data
6. If the user gives their approval, they are then shown a confirmation page and are asked to manually switch back to the application
7. When the user switches to the application, it will have a screen with a "Continue" button for the user to click after they have given approval
8. The user will click the "Continue" button and now the application will work.

The flow makes some security people happy because the user never enters their password into the client application. However it makes usability much much worse, and any evil client application on most operating systems can do other evil things to the user's computer anyways such as installing malware.

Therefore Google decided to try to find an approach that avoided using OAuth when possible, but fell back to it when necessary. The approach we took was to have the client app display the same style login box that Google suggests that websites should use. If the user enters an E-mail and password in that login box, it is sent via a proprietary Google ClientLogin API back to the webserver to see if it can be validated. If the webserver can validate the credentials, then the desktop app can immediately access the user's data. If it cannot validate the password, then the webserver can either return an error indicating that the user should try again, or it can return an error indicating that the user must be sent through the OAuth flow. Similarly, if the user enters an E-mail into the login box, but chooses "help me sign in" then they are always sent through the OAuth flow.

To help improve the OAuth user experience, we made two further optimizations:

1. For steps 3/4, we chose to launch a full web-browser instead of trying to launch an embedded browser in the client app. The big advantage of this approach is that the user is normally already logged into the website, and thus the user skils steps 3/4 and it sent immediately to step 5
2. For steps 6/7/8, we had the website create a new cookie in a pre-determined location, and the client-app would constantly poll in the background for the existance of that cookie. Once it detected that cookie the application would force itself to the foreground and then immediately access the user's data from the website

This prototype application was tested with 11 users who were each told to open a message from their administrator in their inbox, and the message asked them to install a new tool that would give them access to their contact list offline. Here were the two primary goals of the test, and the results:
Goal 1: Evaluate whether users were surprised by the non-traditional login box
Result: None of the 11 participants detected it was a non-traditional login box. That is in line with the previous studies we did. This is a strong indicator that we could change our desktop apps to use this login box and it would have no detrimental impact on normal usage

Goal 2: Get feedback on browser/OAuth flow for users whose domains were SAML enabled.
Result: 10 of the 11 participants completed the flow and found it easy, but identified some UI optimizations we could make (the first participant ran into bugs that we fixed for the others). The addition of the auto-detection of the approval process was important and without that we would need to significantly improve the UI. However even in the case without that auto-detection, it is important to note that for users from SAML enabled domains, we do not have any other reasonable alternatives to offer them anyways.

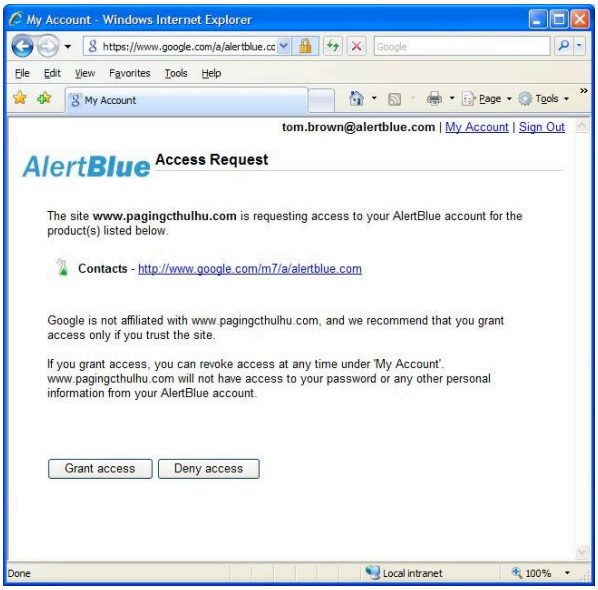
A copy of the prototype application is available here:
http://eric.sachs.googlepages.com/hybridlogin.exe
It only works on Windows and requires .NET Frameworks v2. It is optimized for Internet Explorer, so make sure your default browser is set to IE using Start-Set Program Access and Defaults (It works on firefox, but is not yet as user friendly). We have also provided videos of using this prototype application with multiple federated login technologies and multiple strong authentication technologies.

To test it, launch the application, and try to login with a regular Gmail account by entering your E-mail address and password (see screenshots below). The app will now

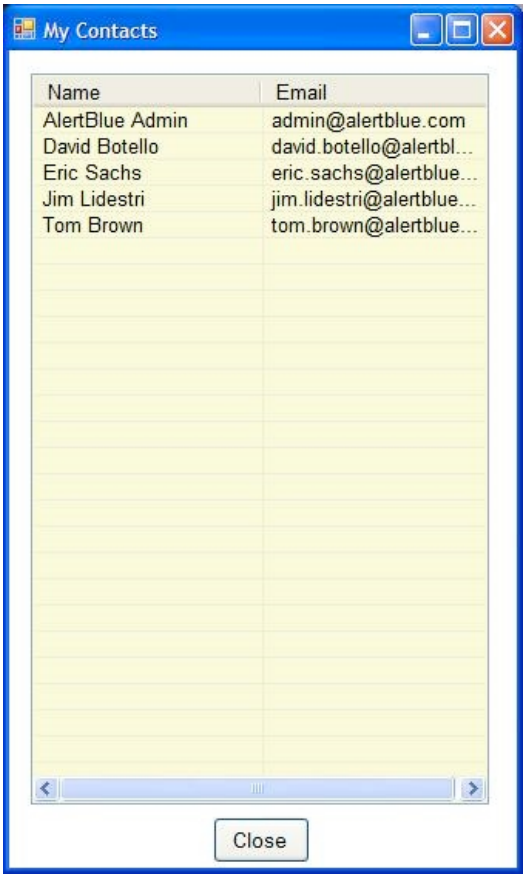
You can now test the application with a domain that is hosted on Google Apps For Your Domain, including domains that are running their own SAML IDP (and even with SAML IDPs that use a second factor auth such as tokens or InfoCard). To do this, enter the E-mail address in that domain and choose "help me sign in" (as shown in the first screenshot below). If you don't have an account on AppsForYourDomain, then enter an @gmail.com address and choose "No, help me sign in" and you will also be sent through the OAuth flow.
Note: The user/employees may mistakenly type their password in this login box (like in the second screenshot below). However it will work even if they make this mistake. The app first sends the E-mail to the Google servers to find out if the domain is SAML enabled, and if so, it forces the user through the OAuth flow, otherwise it sends the E-mail/password to Google directly to be validated. This prototype version only has a hardcoded list of SAML domains (try tom.brown@alertblue.com as an example), but if you want to force the system to do the OAuth flow for your domain, then choose "help me sign in." A later version of this prototype might even be able to check a registry setting to see if the enterprise had hardcoded their domain name, and in that case the desktop application could skip the login screen and start the OAuth flow immediately.

The app will launch your the user's default browser (which should have been set to Internet Explorer), and send you through the flow required to login to that address. If the user is already logged into their IDP and/or Google, then they will not even need to see the login screen.
Note: The login page below is for a domain that is not SAML enabled. A SAML enabled domain would show its own login page, and might prompt the user for a second form of authentication such as a token/certificate/Infocard.

The next page they will see is the OAuth approval page (screenshot below) to confirm they want the app to have access to their contact list. The current page refers to some fake domain, however the final version would display the name of the application instead.
Note: The server cannot verify the identity of the application, but it can display a description of the application. If that description does not match the application the user has installed, then some users will correctly click the Deny Access options.



Once the user gives their approval, the browser will try to redirect to a destination page, and then the desktop app should automatically jump to the foreground and display their corporate address book (screenshot below)
Note: On firefox, you will see a destination page that tells you to manually switch to the desktop app and click the "continue" button



Eric Sachs
Product Manager, Google Security

Identity Scenarios Future Mapping

URL: http://iiw.idcommons.net/Identity_Futures
Conveners: Kaliya Hamlin, John Kelly
Attendees: Tom Brown,Jeff Stollman,
Interested (wasn't in session): Nicholas

What is Future Mapping?

* strategically incomplete stories of the future
* engagement around these stories

The goal is to make future possibilities more real.

News Stories are developed Engage with people around these stories

* How did it happen?
* why was it good?

Peeling back the stories to root causes. Clusters of Driving forces.

Scenarios are built and then advocated for

These help outline a landscape of possibilities that gives a shared way to talk about the future

This process is "Live Wear" 35 people are gathered that represent a cross section.

Changing Understanding and views of the future.

Some background in the late 90's there was 6 firms that did scenario planning - with the dot com bust all of them folded except GBN that was acquired by Monitor Group/Shell Oil. The big customers government agencies like the NSA.

We talked about Ipseity - the core identity - the individual point of coordination.

We believe in the concept of scenario planning but the question around what the commercial relevance is.

Next step is a phone call November 25th.

HERE IS THE DOCUMENT WE WERE DISCUSSING.

Mapping The Future of Digital Identity

A proposal for community based interactive scenario planning.

by Kaliya Hamlin, Identity Woman and John Kelly

The exchange of identity credentials and profile traits in return for the provision of services is the essence of the new *digital deal.* That deal often isn't a very good one, in part because it's not just one, but many, the subsidiary components of which are accountable only to their own frames of reference, but the sum of which produces a total digital profile with exposure out of all proportion to those expressed within any subsidiary implicit or explicit "identity rights agreement" whatever that agreement may actually be called.

This fact isn't readily admitted by industries or individuals on the more profitable sides of that digital deal, in which

user-generated and related data is variously monetized without concrete understanding on the part of the person as to the terms of the relationship and its actual costs and rewards. - Nicholas Givotovsky, in the Identity Gang
The problem is the translation of the complex social and legal issues around identity into these protocols. How to come up with a reference list of identity tokens for age, location, contacts and all kinds of other issues? How to organize the management of relationship data? Which contractual relationships are implicitly or explicitly involved that need to be sorted out? The idea of having Creative Commons-like licenses for your personal data, which then can be described in a lawyer-readable, a human-readable, and a machine-readable form met quite some interest. But this is mainly a usability issue. The different use cases you want for this are much more complex and diverse than the few standard types of re-using text or music.
This leads to the conclusion by many participants: An interdisciplinary perspective is really needed on the issue of identity.
- Ben Rath, Report on IdentityCamp http://bendrath.blogspot.com/2008/06/identitycamp-lessons-learned-in-bremen.html

Mapping The Future of Digital Identity

The Digital Deal raises many Questions:

> *Who are these people who now show up on-line? Can we be sure? What can we find out about them? Where have they clicked? What do others say about them? Do they have substantive rights as humans, irrespective of their status as citizens or consumers? Do any of those rights control the treatment of data linked to them? Should they have privileges based on their achievements, connections, endorsements or purchases? What about vulnerabilities? Do they have health insurance? Any genetic predispositions?*
>
> *What did they have to give up to be identified as who they are? What was their Digital Deal? Was that exchange based on informed consent? A law or principle? Or was it the accidental result of a seemingly technical fix that, once in place, was too expensive to reengineer? Will the Digital Deal gain momentum after a preemptive move by an aggressive vendor or government that will be poorly understood at the time? Or will it be a series of incremental private negotiations among government agencies and their corporate constituents?*
>
> *How can we as a business or institution manage information about individuals with whom we may or may not have transactions that they are aware of? Should we have a dialogue with them about our intentions, their aspirations, how our products work or don't work for them, and how they could be improved? Does one of our competitors or a government agency have a claim on how individuals represent who they are? Do the rest of us have to go through their database, vetting and license agreement? Can't we just talk?*
>
> *And what is the appropriate role for government in supporting citizens representing themselves to other institutions? How can governments provide effective law enforcement, combat digital criminals, and not substitute blanket surveillance for disciplined, appropriately focused investigations?*

The questions multiply. It may seem that we are mixing issues of civil rights with business strategy and government policy. We are, because they are becoming increasingly intertwined. All of them hinge on the question of digital identity.
Digital identity, how it's constituted, represented and understood, will itself establish the practical basis of human rights, because, for good or ill, the enforcement of those very rights will depend upon the recognition of humans by information systems. How digital identity is managed will also profoundly affect the basis for competition between businesses as they use of shared communication resources. Everyone from global corporations and NGO's to local charities and neighborhood farmers or service providers will be seeking the scarce attention and loyalty of individual consumers, producers, and citizens. And access to these citizens will, again, be primarily by means of their digital identity.

Current Trends
We are now facing an increasingly dangerous online environment - fraud with phishing and pharming is rampant. Corporations are tracking people's behavior online and targeting them through massive linked database systems. Government regulation and surveillance of the online space is increasing - disregarding norms of how similar issues

are dealt with in physical space.
At the same time, Live Web, Web 2.0 Social media and networking tools are flowering online. Some of these are closed proprietary efforts while others are pushing towards openness. Many diverse efforts have the potential to have long lasting impact.
Virtual worlds are allowing some to transcend the limits of their real world identities as minorities, people with disabilities, or non-citizens. Virtual identities (avatars) instead allow individuals to emphasize the parts of an identity they choose to assert or reveal while hiding other characteristics. At the same time, the anonymity of virtual identities exposes well intentioned on-line education and collaboration efforts to involuntary interruptions and harassment from anonymous spammers and griefers.

Who Understands these Issues?
The community that has formed over the last four years around the development of user-centric digital identity (1) has developed a rich understanding of this problem space, some key principles and some understanding of what would be good design and best practice within digital identity systems.
This diverse community has grown in a steady but significant way from a small group of idealistic technologists to a cluster of major enterprise vendors developing and testing the interoperability of potential components of open standards based end-user identity management tools - the basis of an identity-meta system or an identity and relationship layer of the web.
The Identity Community has a several rich repositories of exchange that have been developed. The Identity Gang mailing list founded in 2004 has over 2500 messages posted. There are over 50 community members blogging about the subject many of whom are aggregated on the PlanetIdentity.org blog.
The ID Media Review group has formed to collect the range of relevant books, white papers, academic papers, podcasts, government and think tank reports, online videos and movies that cover identity topics. This is led by Bob Blakley and Kaliya Hamlin.

Mapping the alternative futures of digital identity
The Identity Futures group at Identity Commons lead by John Kelly and Kaliya Hamlin is considering a comprehensive interactive future scenario planning exercise. As presently envisioned, it would have four phases

Phase I: Refinement and Capture of Existing Knowledge
The initial phase will focus on capturing and learning from the most relevant existing online resources in the community - specifically the mailing list and blog archives. This effort may employ textual analysis. The mailing list archives are closed and must remain so because of the agreements under which the conversations where initiated. Key assumptions and implications of that discussion can, however, be summarized, cleared with those who wrote them (if quoted directly) and made available to the public.
The Id Media Review project contains a range of material that applies to questions surrounding digital identity. Many pointers to works in the life of the community have been collected. By organizing, contextualizing and summarizing these works, we will provide access to them for business leaders, government policy makers and technologists to better inform their choices as they continue to evolve digital identity systems.
Both of these projects create publicly accessible resources on identity issues so that significant discoveries don't have to be "re-learned." Both of these projects are valuable in and of themselves to make already developed raw information more accessible and useful. The value of this information will be amplified in Phase II below.
Past experience with other complex issues suggests that significant tacit knowledge remains buried in the unspoken intuitions and assumptions of professionals working on the frontiers between digital and real-world identity. Security experts fighting identity theft, publishers of digital content, social networking entrepreneurs, business strategists, and some government regulators have experience that could inform choices about digital identity, anticipating a range of desired and undesired outcomes.
Interviews will be conducted with 25-50 people selected from this community using a well established methods. These interviews will be combined with the earlier research to create 80 to 120 possible future milestones describing particular micro-outcomes in the evolution of digital identity.

Phase II: Developing Scenario Building Kits
Developing a rich set of scenarios that explore significant possible variations in outcomes and also inform and support decision makers who may have to cope with these variations is a challenging task. With a topic as unsettled as digital identity the best people to help create scenarios do not work for any single company or agency. It requires the wisdom,

not of a "crowd," but of a sufficiently diverse range of stakeholders with varying expertise and interests. The engagement needs to be concentrated to make use of the limited time available from people with the most in-depth expertise. To that end, the proposed interactive scenario planning process will develop scenario building kits. The kits will include 80-120 hypothetical future milestones, a framework for choosing and applying milestones to different outcomes, and a set of four distinct clusters of assumptions that could determine how digital identities will evolve. These kits will allow participants to select rather than compose most of the elements need to flesh out a scenario for the future of digital identity within the limited time frame (~ 2 days) of an interactive scenario planning workshop. This method of converting in-depth research into scenario building kits was developed and refined at Northeast Consulting and Nervewire Inc. over a fifteen year period.

Phase III: Crowd-Sourcing the Experts in an Interactive Scenario Workshop

An interactive scenario planning workshop will bring together 25-35 "experts" – stakeholders who have been part of an identity exploration community and can contribute technical, business, social and professional knowledge about the risks and opportunities of evolving approaches to digital identity.

The activities during this two day workshop will provide a well structured, high intensity, data-rich platform for advocacy and refinement of competing views. Teams will select and advocate interpretations of the potential linkages between emerging technologies, social networking applications, civic engagement, protection of rights, law enforcement, intellectual property, business models, and the clash of cultures as they relate to the key alternatives available for the design and implementation of digital identity.

The output of this workshop will be a rich and refined data set of clarifications, ranking votes, and speculations that map out the possible futures for digital identity. It will support discussions among business competitors, activists and government agencies about the best principles, policies, investments and actions they should advocate or implement over the next 3-5 years.

Phase IV: Repurposing materials for participatory distribution

Even the best run meetings and workshops often cannot transcend the curse of 'shelf-ware' – generating well received reports that remain on shelves as their findings are overruled by apparently more urgent needs. To overcome this limitation, the output of the scenario workshop will be reconstituted into a mini-workshop kit that will support a two to eight hour interactive engagement with new audiences. The underwriter of this project will be able to use the mini-workshop kit to conduct participatory demonstrations of the process used by the main workshop and engage participants in voting on outcomes. The distributed workshops will achieve several purposes:

- bring an understanding of the implications of digital identity to a wider audience
- create a common language for cross functional teams to support ongoing interactions between their efforts and public developments in digital identity
- validate existing data on the judgments of the expert group and monitor changes in the perceptions and preferences of new constituencies

Next Enabling Steps

We are looking for a commitment from a major player(s) committed to leadership in anticipating and advocating the best possible future of Digital Identity.

SESSION 10

OASIS Identity Metasystem

URL: http://iiw.idcommons.net/OASIS_Identity_Metasystem
Convener: John Bradley, D Reed, Mike Jones
Notes-taker(s): Mike

Discussion notes:
This session discussed the goals and work plan of the OASIS Identity Metasystem Interoperability Technical Committee (IMI TC).

We shared that the committee had completed the first committee draft of the Identity Metasystem Interoperability specification and that it is available for public review. That spec consists of the merger of the content of the Identity Selector Interoperability Profile V1.5, A Guide to Using the Identity Selector Interoperability Profile V1.5 within Web Applications and Browsers, and Application Note: Web Services Addressing Endpoint References and Identity. The Security Considerations and Conformance sections of the committee draft are known to require more work on the part of the committee. This draft is available at:

http://www.oasis-open.org/committees/download.php/29978/identity-1.0-spec-cd-01.doc
http://www.oasis-open.org/committees/download.php/29979/identity-1.0-spec-cd-01.pdf

We also shared the output of this specification is intended to be backwards-compatible with these input documents.

We discussed the coordination with the OASIS Security Services TC to create a SAML 2.0 token profile for use with Information Cards, and that this will likely be the second work to come out of this TC. Also, we discussed that specifications for such innovations as Higgins Relationship Cards and the CardSpace "Geneva" CardTile are likely to be submitted by their inventors to the TC.

DeWitt Clinton led a discussion of the OASIS IPR Regime that the work is being conducted under. It was noted that the IPR Regime for the IMI TC work is the same as that for the underlying specifications, such as WS-Trust.

-- Mike

Starting Up

URL: http://iiw.idcommons.net/index.php?title=Starting_Up
Convener: Greg Biggers
Notes:?

Taxonomy of Trust or what the world of warcraft can teach us about ID

URL: http://iiw.idcommons.net/Taxonomy_of_Trust
Convener: Alex Rosen

1. Reputation is at the basis of trust

2. We can think about 3 kinds of reputation:
•explicit (eBay),
•implicit (Facebook), and
•performative (World of Warcraft).
    - Performative is really the most interesting, but also the hardest to do online.

3. Trust is the glue that holds together social interaction online, but for it to work, the 'types' of trust need to be varied and differentiated so that trust is harder to game.

4. Where does openID, xrds, etc. fit into this? Do they support performance-based reputation and trust?

5. http://www.assertid.com/ is doing a lot of work in this space. JC from this company discussed their model and how social networks build trust.

You can download Alex's Thesis '"Distributed Consolidation: Identity, Reputation, and the Prospects for Online Social Interaction"' Here http://dspace.wesleyan.edu/dspace/handle/1967/92

IMPROMPTU SESSIONS

What are the Business Models (un)Conference

URL: http://iiw.idcommons.net/What_are_the_Business_Models_of_ID_Conference
Conversants: Louie Gasperini, Stephen *who works with Phil*, Kaliya Hamlin,

We talked about the lack of business people at the conference and the NEED to figure out the business models.

We thought a highly focused 1.5-2 day event this winter could help move this conversation forward.

We decided to go forward with an invitation and finding a place.

Likely dates are late Feb early March.

Likely place in the mountains.

CLOSING

URL: http://iiw.idcommons.net/index.php?title=Community_Awards_08b
At the end of each IIW we place gifts in the middle of the circle and invite people to give them to those at the conference and in the community that have made contributions that were meaningful.

Dick Hardt: to Eric Sachs for moving things fowarrd

Eric Sachs: to Eran Hammer for talking about discovery

Jeff: to Kaliya for endless energy

Eric T: to Drummond for loosing

Drummond: to our Barista

Mike Jones: to to John Bradley for being aware of esoterica Drummond

Drummond: to Joe Andrieu for helping support VRM

Joe: to Doc for being visionary and being crazy open source guy

Doc: to Phil W for organizing things here

Mary Ruddy: to Eugene Kim for being guiding light and continuous participation in ID Commons

Dazza: for Civic ID and civic ID guy to Dazza for ?

Kaliya: to An (with one N) for bringing great energy and spirit

An: to AlexMR for scholarship paper (senior year)

Gary Marx: to Jay Smarr for ?

? to Nat Sakamura for ?

Nat: to ?

Jeff H to Judi Clark for diving in, making nice contribs

Lucy L: to Marty and Charles for being unifying voices

Marcus: to guy in brown t-shirt for doing something really cool

Drummond: to Hank for going down to the router level of stuff

Greg Biggers: to Joe Andrieu for being his official ambassador

IDENTITY COMMONS

Summary

URL: http://wiki.idcommons.net/Main_Page - & links off this page

The purpose of Identity Commons is to support, facilitate, and promote the creation of an open identity layer for the Internet -- one that maximizes control, convenience, and privacy for the individual while encouraging the development of healthy, interoperable communities.

Facilitating broad community dialogue and increasing the diversity of perspectives in the emerging field of user-centric identity is a unique and critical role that Identity Commons currently plays. This role is becoming even more important as the community grows and as the vision of a decentralized, user-centric identity layer for the Internet comes closer to reality. Identity Commons must continue to create opportunities for both innovators and competitors, for both the big guy and the small fry to come together in a safe and balanced space.

Identity Commons fulfills this role in a variety of ways. Continuing gatherings such as the Internet Identity Workshop and Identity Open Space are natural next steps. Doing such gatherings under the auspices of IC enables organizers to leverage common operational resources while focusing their energies on bringing the right people and content to these gatherings. IC can also play a supportive role for other ad hoc gatherings both face-to-face and online as well.

On the technical side, IC can be a voice for multiple, interoperating and possible competing identity standards and reputation networks. IC encourages the development of systems that achieve zero customer lock-in, thus always providing users of identity systems the choice to move without the risk of losing the accumulated fruit of their labors/participation. Further, IC can assist efforts to create transparency in the operations of the identity systems and their associated services, so that users who are not as technically adept could feel secure in their actions.

Identity Commons is open, inclusive, and bottoms-up, community of groups. We share an agreement and agree to abide by a set of principles to help assure this. Membership resides in the Community Groups. There is a Stewards Council - with a representative from each group.

We provide a minimal structure for supporting community activities, and we hold space for the entire community to collaborate, and facilitate dialogue.

Identity Commons, inspired by the core principles of Chaordic Commons, consists of Working Groups and a Stewards Council. The basic structure has been referred to as an "upside down umbrella" because the vast majority of the activities and decision-making occur within the Working Groups, which have tremendous autonomy -- so much so that a Working Group can be a complete separate legal or social entity whose own charter or incorporation need not make any mention of Identity Commons.

The Principles of Identity Commons:

1. **Self-Organization.** Enable any working group to self-organize at any time, on any scale, in any form, around any activity consistent with the Purpose and Principles.

2. **Transparency.** Fully and transparently disclose the Purpose and Principles of each working group, any requirement of participation, and any license or restriction of usage of its work product.

3. **Inclusion.** Conduct deliberations and make decisions by bodies and methods that reasonably represent all relevant and affected parties.

4. **Empowerment**. Vest authority, perform functions, and use resources in the smallest or most local part that includes all relevant and affected parties.

5. **Collaboration.** Resolve conflict without resort to economic, legal, or other duress.

6. **Openness.** Conduct, publish, and archive communications in a manner that facilitates open and trusted interactions within and across all working groups and the public Internet.

7. **Dogfooding.** When feasible and appropriate, employ the work product of Identity Commons working groups to facilitate the operation and interaction of Identity Commons itself.

IDENTITY COMMONS WORKING GROUPS LIST

URL: http://wiki.idcommons.net/Working_Group_Descriptions

Community

The Identity Gang, this is the mailing list for the digital identity community. The gang, formed in 2004, also collaboratively developed a lexicon related to digital identity technologies and issues. The active mailing list has over 500 members - to avoid spam registration is required. mailing list.

Internet Identity Workshop supports face to face conversation about internet-wide digital identity and it's implications. User-centric identity has been a topic of particular interest. This twice a year event aims to support the whole marketplace, especially individuals contributing their voice in open inclusive conversation. These events have a reputation of being incredibly effective for getting real work done and moving the industry forward.

Newbies 4 Newbies This working group was formed at the Dec 2007 Internet Identity Workshop to support by a group of "newbies" to connect with their peers who were inspired by the community but wanted to make sure documentation and material about the topics in the community were more accessible. They have regular conference calls and are working on the development of the Starting

Business

VRM (Vendor Relationship Management) This group grew out of Doc Searls original 'rental car use case' put forward at Digital Identity World 2004. VRM, or Vendor Relationship Management, is the reciprocal of CRM or Customer Relationship Management. It provides customers with tools for engaging with vendors in ways that work for both parties. Project VRM is currently under Berkman Center for Internet and Society at Harvard Law. Participants are working to create the ecosystem of tools, protocols, and services that help users manage vendor relationships. It has five committees, Vision, Standards, Organization, Usage and Compliance. There are several active mailing lists, a blog, regular conference calls and an community of software vendors working on building standards based tools to make it real.

Technology – Standards, Interop and Code

Information Card Foundation
Advance the use of the Information Card metaphor as a key component of an open, interoperable, royalty-free, user-centric identity layer spanning both the enterprise and the Internet. A 501c(6) trade association, ICF is open to any individual or organization. Community members comprise the majority of the Board of Directors. Current Community members are active participants in Identity Commons, Information Cards, Open ID, OSIS for interoperability, Concordia, The Higgins Project, Microsoft CardSpace, the Bandit Project, The Pamela Project, Project VRM, Identity Schemas, and XDI.

OpenID
The purpose is to advance development, implemention, and adoption of the OpenID framework of specifications for user-centric identity. This working group is organized as a 501c3 non-profit corporation. The group is open to any individual or organization interested in the advancement of OpenID. Specifications and open source code are maintained by meritocracy.

OSIS (Open Source Identity Systems)
OSIS brings together many identity-related open-source projects, and synchronizes and harmonizes the construction of an interoperable identity layer for the internet from open-source parts. Its first deliverable is interoperability with Microsoft CardSpace, although OSIS also encompasses alternate technologies such as OpenID and SAML.

This is one of the most active groups in making the metasystem vision come alive and has participation from a range of both big and little technology vendors. They are having their third major Interop Event with over 200 tests through to the RSA Conference in April 2008.

Identity Schemas
To promote interoperability between identity systems by making it easier to find, understand, and reuse the semantics of identity attributes defined in existing schemas. They have clearly articulated the problem space and deliverables to address it. There is an active mailing list and face to face meetings happen at events like the Internet Identity Workshop and Data Sharing Summit.

Higgins Project
Higgins is an open source identity framework. Higgins is a framework that enables users and applications to integrate identity, profile, and relationship information across multiple data sources and protocols. End-users can experience Higgins through the UI metaphor of Information Cards.

SAML Commons
The purpose of this working group is to advance development, implemention, and adoption of SAML, in particular by producing SAML profiles that enable its use with other technologies such as XRI, OpenID, etc.

XDI Commons
The purpose of this working group is to advance practical deployment, usage, and best practices for the XDI (XRI Data Interchange) protocol under development by the OASIS XDI Technical Committee.

Pamela Project
The Pamela Project exists to information-card enable popular open source web frameworks, with the goal of allowing administrators to install rather than code information card support into their sites. It also is working to make it easier for people of all skill levels to understand and use this technology.

Social / Legal / Policy

ID-Legal
This group was formed at the 2008a IIW - at a session wondering what it would be like to have a conference that was 1/3 lawyers and 1/3 techies in identity and 1/3 other people. It is working on organizing a conference for mid 2009. There is a mailing list you can join.

Kids Online
This group is focused on developing finding and disseminating good, effective and shared practices around kids safey online while not loosing sight of the fact that they are kids and want to have fun there too. The group primarily meets face to face and is had its first conference November 13, 2008.

XDI.org
The purpose of this working group is to provide community governance of open public infrastructure based on the XRI & XDI standards.

ID Futures
The Purpose of the Identity Futures Group is to engage in interactive (shallower) and indepth consideration of potential future events and scenarios for an identity layer of the web. The first step in this was at Digital Identity World 2007 where we developed 50 future identity related events and mapped them. More scenario development and planning is being coordinated.

ID Media Review Group
"The Book Club" is here to support the Identity Commons community engaging with books, movies and other media that cover identity related topics. We do this by collecting a bibliography and by reviewing and discussing these media. We use the issues raised by these works to inform our work innovating the identity layer of the web and help us understand and address the social, psychological, legal, privacy, security, regulatory and ethical issues. The bibliography is growing and further collaboration is planned to engage with these works.

Photo Group
The photo group aims to serve as a community hub for identerati with interests in photography, as a gallery in which identity community photographers can display their work, and as a resource for people looking for photographs which illustrate aspects of identity.

IC Operations

IC Evangelism & Marketing
Provide content that will help Identity Commons, its member groups, and individuals more effectively communicate the goals, principles, and messages of Identity Commons. Assist in any evangelism efforts to bring appropriate working groups and individuals to become Identity Commons members.