IIWXI INTERNET IDENTITY WORKSHOP 11

A WORKING GROUP OF IDENTITY COMMONS

NOVEMBER 2 – 4, 2010
MOUNTAIN VIEW, CALIFORNIA

Book of Proceedings

Notes gathered and compiled by Kas Neteler & Heidi Nobantu Saul

Version 1

please send missing notes to
iiwnotes@gmail.com

Facilitated by Kaliya Hamlin and Heidi Nobantu Saul

IIW is Produced by
Kaliya Hamlin, Phil Windley and Doc Searls
www.internetidentityworkshop.com

Table of Contents

Day One – Tuesday November 2nd

Session 1

Intro to Personal Data Storage (T1A)

Convener: Drummond Reed & Paul Trevithick
Notes-taker(s): Joe Andrieu
URL: http://iiw.idcommons.net/Intro_to_PDS

Tags for the session - technology discussed/ideas considered:

PDS
Personal Data Store
Personal Data Service
PDS Ecosystem
Personal Data Spectrum

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

Input for a wikipedia article
A place for my stuff

Could be a store for personal data
Could be data store controlled personally (initial VRM usage)

Shared understanding:
1. Controlled by person (required?)
2. Virtually distributed
3. Seamless permissioned access (sharing)
4. Can be provided by a service provider
5. Portability
6. Interoperability
7. Ownership/co-ownership/authority
8. Data is extractable and semantically distinguished

Use Cases
1. Sharing of Electronic Health Care Records
2. Sharing of photos
3. sharing of address books/contacts

Must distinguish between
1. a store of personal data (database or file)

Who owns that transaction?
Who owns the data?

Ultimately it's about how we give individuals control.

"Our" data /is/ distributed. That's fact. We have different levels of control and rights over that data.

What we are talking about is a layer of control.

Perhaps we need a totally new word.

Joe: If you can share from it, it's a personal data store.

Content

Trust Frameworks as Analog o Digital Converters (T1B)

Convener: Scott David
Notes-taker(s): Jamie Clark
URL: http://iiw.idcommons.net/Trust_Frameworks_Analogue_to_Digital_Converters

Tags for the session - technology discussed/ideas considered:

trust_framework, taxonomy, contracts, risk_allocation, UI

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

Slides: http://iiw.idcommons.net/File:Nov_2_Rethinking_Personal_Data_Workshop.pdf

[slides]: "Facilitating Personal Data Transactions in a Secured Manner on a Global Scale": part of presentation for WEF (Davos) prep session on "Rethinking Personal data" workshop, New York, September 2010; should be posted shortly to OIX website

What's the international law of identity?
There isn't any.
Can we do things with law and/or rules and/or tech to weave together the disparate systems that interact?

What should identity systems do? Meet "system participant" (user) needs. Such as:
 - data subjects need identity integrity
 - replying parties need assurance
 - identity providers need risk reduction
These high-level 'needs' share some basic lower-level functional requirements like, security, reliability, UI, etc.

What can tech and law do about this?
-- technology tools guide data movement & protect data at rest
-- legal rules create duties to incent behavior

-- By far most of the data breaches I've seen (S. David) were human error, not tech failure. So the human rules and incentives matter.

 A "Trust Framework" is a possible documentation style ("term sheet"?) for the agreed risk and reliance arrangements between system participants.

There is some "low hanging fruit" of law and practice guiding these duties:
 -- In the US: NSTIC, Levels of Assurance. In some states, data breach laws.

-- Privacy laws like HIPAA, Gramm-Leach, FICA, etc.
 -- Fair Info Practice Principles (originally US DHEW 1973) - levels of control
ABA drafting a report on Federated Identity which addresses a taxonomy of issues and actors; OIX doing a "risks wiki"; some out for public review now; posted work product expected early 2011(?)

One difficulty is operationalizing assurance which is mostly processed by end-users as emotional states like "trust", "reliability." Quantification needed, to clear the semantic fog here.

The idea here is to address some recurring liability issues, but not all. 80/20 approach, not boiling the ocean. May be industry groups and self-regulatory efforts that give rise to the best evolving solutions.

First step is a candidate common analytical framework, to get to "apples-to-apples" on some of the risks, practices and concepts

Inspirational vision: UI simplification - risks and control issues displayed simply like red-light-yellow-light-green-light displays.

Audience: Frameworks generally get developed in a context of siloes - noninteroperable specailized cases. Is there a "metalanguage" for crosswalks among the privacy practices of those siloed players? Or 15% of them, anyway, for scalability's sake.

Decline of User Centric Identity (T1D)

Convener: Dick Hardt
Notes-taker(s): Dick Hardt
URL: http://iiw.idcommons.net/Decline_of_User-Centric_Identity

Tags for the session - technology discussed/ideas considered:

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

User centric technologies are in decline. InfoCards are past their due date and OpenID is moving away from being user centric.

The belief is this is due to a lack of industry players with significant financial incentives to make it happen, as well as players with negative financial incentives.

The other reason is that the technology was immature on launch and was not able to meet security, functionality and/or usability requirements.

OAUTH Listening Tour (T1E)

Convener: Mike Jones
Notes-taker(s): Sunir Shah
URL: http://iiw.idcommons.net/OAuth_Listening_Tour

Tags for the session - technology discussed/ideas considered:

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

OAuth

Who's here and what do we want to get from this session?

* Brian Campbell, OAuth2 for Ping; SAML OAuth profile
* Sunir, FreshBooks. OAuth for App Sotre
* Patrick Harding, Ping.
* Harish. Implemented OAuth 1.0. Want to move to 2.0
* Hiroki, NTT. how to deploy openid and oauth in enterprises
* Steve Weiss, AppDirect. OAuth to integrate with vendors. keep up to date
* Dirk, Google. implemented OpenID+Oauth hybrid
* Jacob, ATT. Where is OAuth2 going.
* John Trammel, Adobe. OAuth2 and OpenID connect projects
* Vijay, VMWare. How can we use OAuth to specifically for app authentication,

authorization
* Mike Donaldson, Ping. Realization of OAuth2
* Marius, Google. OAuth2 implemention while supporting OAuth 1.0
* Macduff Hughes, google
* Nat Sakimuri, Nomura Research Institute, mobile web app flow
* Tom Addison, Ping. Use cases for OAuth
* Mike Jones, Microsoft. Spec work on OSes and identity. Recently chosen to edit the bearer tokens portion of OAuth2 specifications.
* Dev, Grad student at Berkeley. Security research wrt OAuth
* Frank, eBay. Teams implementing OAuth2.0
* ??, Google China, federated login project

Eran is going to be editor of basic OAuth flow. Mike editor of how to use bearer token to obtain access.

Section 6.

What is the bearer token portion of OAuth2?

Section 6.

Problems implementing OAuth2 while supporting OAuth2
* the way headers are described is not clean when trying to also support

OAuth1.
** the way headers are defined are similar to Basic scheme, but using OAuth.
and then you just have the token. No using post way to disambiguating from

OAuth1 because all characters in Oauth2 are allowed in 1 (or vice versa). We
know that tokens can't have commas so that's how we distinguish
** eran wanted different endpoints for different protocols, but in reality that is
not feasible
** It's ugly to try parsing with one Strategy and if it fails, try another

Strategy
** My preference is the scheme name for OAuth2 should be "OAuth2". It's fine
if it were "OAuth", then it should be a name=value pair.
** signatures are coming to OAuth2, so at some point you have to deal with
signed OAuth tokens
** up until version 5 or 6 scheme name used to be "token"
** isn't it normal to use key-value pairs;version=
** Basic contradicts all other RFCs. Basic is not standard. Should have
name-value pairs
** Basic is a huge precedent, but typically a list of name-value pairs.
* BNF is ambiguous
* Post very query parameters use cases unclear

NRI is using OAuth2 as basis for OpenID Artifact binding
* using post instead of header because in our case the token can get pretty
big

Google: If you have to parse the whole post it's a huge hit. We'd rather have
it in the query parameter

How many profiles do I need to support?
* not required to support everything. depends on use cases
* no conformance
* OAuth2 you have to support header method

The split of when to use bearer tokens and when not to.. is there guidance?
* What will help the implementor to decide what is appropriate?
* the generic answer is to write guidance documents about when it is
appropriate to use a bearer token, what are the risks are you taking, when is

that inadequate in a security context
* finishing the security consideration section is what's missing
** HELP REQUESTEd: input on what language should be in security section

Each section should have its own security section

I don't think you can assume security consideration for bearer vs user tokens are the same.

The OAuth framework would describe the hooks for token scheme. Signture would use hooks to add more fields for signing

Goal of turning Internet Draft into standards tract

Eran believes when we have draft 11 including the split, it will go out for comment. It's possible that Draft 12 will become the standard

We will attempt to get to final text and have standards directors review it.

Eran believes the standards directors to change a should to a must, e.g. MUST use TLS.

TLS assumes a particular kind of deployment. We don't have the same requirements as Google and Facebook. The SHOULD makes more sense for our case.

I work in gov't: Long history of stovepipes (vertically integrated application stack). You need to know everything from top to bottom. So OAuth used in closed environment, so a lot of security considerations don't apply to use in the same ways. It's one of my goals that the OAuth spec doesn't drift far away from our use cases that we have to be really out of compliance.

We should stop changing things. We have six implementations of Draft 10.
* but signatures, bearer tokens not included?
* draft 10 is OAuth framework. fix that so it will be faster to do signatures spec.
* breaking existing deployments is part of the risk of implementing a draft
* making changes should be focused on bugs

Client Implementors guide
* message sequence charts
* detailed example flows of headers and exchanges
* a little more of the Why does this profile work, and why does it exist like this?
* should live on OAuth.net as an implementor's guide

Where is 2-legged OAuth in the spec?

* I don't see an analog in OAuth2
* Native application is closest
* Some profiles supposed to address that
* signed OAuth profile group should address that
* signed http requests
* at IIW east a bunch of people went through those sections

We're using the client credentials profile replaces what would have traditionally been 2-legged OAuth.
* We send short term bearer token across the wire to the protected resource

As OAuth2 is more modular, many ways of doing the same thing.
* client credentials flow /assertion flow to get access token
* bearer token
* token with signature

Can there be a recommended implementers guide for best practice to support 2-legged OAuth?

Activity Streams (T1F)

Convener: Monica & Kevin Marks
Notes-taker(s): Kevin Marks
URL: http://iiw.idcommons.net/Activity_Streams_101

Tags for the session - technology discussed/ideas considered:

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

Presentation from Monica:

http://prezi.com/yxvtypx-aani/activity-stream/

notes:

http://storify.com/kevinmarks/activity-streams-101-session-at-iiw

VERIFIED IDENTITY CLAIMS – Scenarios and Business Models (T1G + 4G)

Convener: Ariel Gordon (Microsoft)
Notes-taker(s): Ariel Gordon (Microsoft)
URL: http://iiw.idcommons.net/Verified_Identity_Claims_1

Tags for the session - technology discussed/ideas considered:

Verified Claims; Identity Attributes; Privacy; Privacy Enhancing Technology; Cryptography; user-centric technology: user control.

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

(Context) Microsoft's Verified Claims Team is working with customers and partners on Privacy Enhancing technology for identity information sharing.

These sessions were about sharing perspectives on higher value transactions that are hindered by the lack of trust online. What are businesses doing now for identity proofing? (out-of-band boostrapping solutions, accepting low levels of identity verification and the higher fraud level? Etc.) Can we figure out ways to raise the trust bar in a privacy enhancing way and without introducing too much friction for the user?

Canonical examples: age verification for online gambling, purchasing wine online; verified car ownership and information for participation in an online auction.

John Bradley
Trust frameworks are key--certification for identity proofing, privacy and more (e.g. certifying identity providers to US Government standards).
Pseudonymous Level 3 scenario? E.g. prove that the user is a doctor without disclosing the real identity. This isn't a scenario that the government supports.

Greg from Sierra Systems (?) in British Columbia
Setting up "next gen" identity services for individual services and businesses
They care about Legal Name, DOB, Residential Address, Birth Location (jurisdiction, how supporting documents are verified)

Other folks in the room: we care about the following verified claims
  * Employer
  * Administrative role (in enterprise scenarios)
  * Credit Score / Has a credit card (and can actually buy something) / Has Credit History
  * Verified claims of relationship (parents, spouse, kids)
 Kim Little from Lexis Nexis

Helping customers with Identity Proofing needs. Determine if a person can receive a regulated good: right age? Right location? Have occupancy or ownership of the house they're receiving a service for.
Lexis Nexis provides these kind of services? (by aggregating data from different sources and offers these services).
Note: one claim is "I'm employed", another claim is "I'm employed by Company X"
Is Employed: typically useful for establishing ability to buy some financial services.
Important to distinguish professional identity (am I employed somewhere/by company X) and personal identity

Sending a document to a new address (not associated to my credit card). How do I prove my relationship to this address?

Emily Soelberg from ATT
They do In-person Verification, credit check, etc. Almost 100 million customers. Wanting to understand how they can leverage that.
Valuable verified attribute: Geolocation. Cellphone location can be used to verify that the user is in the same location that the transaction is taking place, and reduce fraud.
Not only B2C but also C2C--peer to peer transactions: interesting to be increase trust between strangers so that they can get in business together (e.g. selling a used car).

Jon Webb from PlayStation Network.
One of their biggest problem: users don't value their identity, create multiple accounts, are sources of fraud and other problems. Don't have many fraud problem wrt credit card in the US but they are operating in 70 countries with cellphone payment methods or pre-paid, not as trustworthy as credit-card in the US or Europe. They're looking for ways to increase the verification while keeping friction low.
COPA regulation in the US: companies are restricted by law about what information they can collect.

TSA use case
Can this individual carry a gun (don't care who this person is)

Lloyd Burch from Novell
Medical use case. Blue Cross providing a pseudonym identity + claim that this person is an auditor
Data minimization principles: banks understand it. Very different from the Web 2.0 crowd that are trying to maximize the information they collect.
Hard for businesses to find a balance between minimizing data and monetizing the data they have: e.g. banks already have the Liability associated with collecting user's high value information (SSN...), so they might as well try to monetize it.

Google is working on verified email addresses.

Pamela Dingle from Ping

Too much friction: I'm not going to set up the list of address for my family if I ever want to ship a package to them.
Protecting revenue stream: cost vs. Risk.

Pat Mangiacotti from Equifax
Equifax is validating identities for Governments and private corporations. Validating 1.5 million identities every day!
Also investigating: reversing the business model whereby consumers will effectively verify their identity on online social networks and being able to prove that they are who they say the are.
Employer information: one of Equifax's subsidiary has one of the largest employment information (validating employment information and income). Used for large purchases.
Using Trust Frameworks?

UX: for the low value, high volume transactions, the friction need to be close to zero. Many businesses accept the fraud risk to keep the user friction low. Can we as an industry enable identity verification with minimal friction?
Group agrees to have a follow-up session on Wednesday to specifically discuss UX.

Bret Tobey from Assa Abloy
Biggest manufacturer of locks/solutions for a range of customers from hotels to rack space to corporate offices to locker rentals in ski resorts. Can they leverage federated identity solutions to simplify their problem? They don't want my full identity, but a minimal set of PII e.g. do I work for this company or did I pay to get access to this locker/rack space/filing cabinet?
They're interested in reducing friction and data minimization (i.e. minimal disclosure)

Ben Goodman from Novell
University and corporations should be able to assert the information that's on my LinkedIn profile.

Participants:

Thomas Hardjono	MIT-RC
Fan Xia	Google
Nishant Kaushik	Oracle
Guibin Kong	Google
Mike Mon	Booz
Jeff Hodges	PayPal
Eve Maler	PayPal
Ben Goodman	Novell
Stuart Proffitt	Novell
Rooly Eliezerov	Gigya
Emily Soelberg	AT&T

Henrik Biering	Peer Craft
Brian McGinnis	Janrain
Jeff Stollman	Secure Identity
Bret Tobey	Assa Abloy
Pat Mangiacotti	Equifax
Charles Andres	PBB
Dean Landsman	
Markku Mehtala	
Jon Webb	Sony PlayStation Network
Greg Turner	Sierra Systems
Kimberly Little	Lexis Nexis
Ariel Gordon	Microsoft

UMA – User Managed Access 101 (T1I)

Convener: Eve Maler
Notes-taker(s):

Tags for the session - technology discussed/ideas considered:

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

Eve sent PDF of slides - not in wiki and

Session 2

OpenID, OAUTH & Social Networking for Online Retailers (T2A)

Convener: Brian Kissel & Ashish Jain
Notes-taker(s): Slides submitted by Brian Kissel
URL: http://iiw.idcommons.net/Social_Networking_for_online_retailers

Tags for the session - technology discussed/ideas considered:

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

Link to slides: http://iiw.idcommons.net/
File:OpenID_Foundation_Retail_Advisory_Committee_Overview.pdf

Thoughts to Consider…

- Increasingly, consumers want to research and execute purchases on the web, and the trend is accelerating with younger generations
    - In order to gain mindshare and market share, you need to know more about customers
    - With more consumers and retailers interacting via the web, "identity fatigue" is becoming an issue: "if its too much effort I'll just buy it from Amazon"
    - How do you get more visitors to register on your website, remain engaged, and login early during each return visit? How do you ensure that user profile data is complete and up-to-date?
- Social Commerce is a reality. What friends recommend is becoming more important than banner ads, search results, or even customer ratings and independent reviews (c|net, Consumer Reports)

Social Marketing

- The trust factor of friends' suggestions can make a big difference. Loopt's users are 20X more likely to click on a place their friends had liked or visited than a place that simply ranked higher in search results.
- "Improving search has always been about improving relevance," Augie Ray of Forrester said. "But the thinking now is that getting information from your immediate social network is what will really make results more relevant."

- "People are likely to find what your friends are saying about the iPhone 4 or a Chinese restaurant more helpful in a Web search," said Matt Cutts, a software engineer who oversees search quality at Google.
- http://www.nytimes.com/2010/09/13/technology/13search.html

Benefits of 3rd Party ID and Social Networks for Retailers

- **Higher Registrations:** Increase conversion of visitor to registered user by 25% to 50%*
- **Better Login:** Reduce forgotten password costs and frustration by up to 50%*
- **Increased Referral Traffic, SEO, and Brand Projection:**
  - Allow users to share activities (purchases, product reviews, blogs, surveys, video views) with friends on social networks (Facebook, Twitter, Yahoo, Google, MySpace, LinkedIn, Microsoft, etc.) with links back to your websites
  - Customers as advocates, project your brand beyond your website, links back improve SEO
  - Websites seeing anywhere from 5 to 25* referral visits for each social publishing link
  - Referral visitors are highly qualified and come with active identity accounts for easy registration & login
- **Collecting Rich Customer Data:** Build richer customer profiles by using customers' existing online accounts - name, verified email address, shipping address**, phone**, payment info**, nickname, language, zip code, age, friends lists, address books, personal interests & hobbies, photos, etc.
- **Improved Mobile Experience:** Provide a much quicker and simpler user experience via mobile applications
- **Website Federation:** Single sign-on (SSO) for your customers across multiple web properties and component solutions (commenting, rating and reviews, customer feedback, community, etc.).

OpenID Foundation

- Founded in 2007
- Non-profit, open-standard technology organization like Linux Foundation
- Promoting open standards for user-managed identity
- Board members include folks from Google, Yahoo, Facebook, PayPal, Microsoft, IBM, Sears, NY Times, and NPR
- OpenID Foundation members include: Google, PayPal, Facebook, Yahoo!, CA, Microsoft, IBM, LexisNexis, VeriSign, BBC, Booz | Allen | Hamilton, GameShop, PingIdentity, JanRain

Identity Providers and Technologies [picture]

Integrated into Leading Technology Platforms
You may already be using one of these on your websites… *Social Network &*
Community Platforms KickApps, Viewpoints, Talki, Wetpaint

Customer Feedback Tools Get Satisfaction, IdealScale, Uservoice

CMS Turnkey Plug-ins WordPress, Drupal

Content Communication Platforms Disqus, Echo, Pluck

- Sears Sign-in and Social Publishing Demo
  Visitor arrives at Sears website and clicks sign in…
- Offered choice of 3rd party ID providers…
- Customer selects Google and grants permission…
- Logged in, personalized experience…
- Offered opportunity to write a product review…
- Customer writes personal product review…
- Review received by Sears, offered chance to share…
  Can be configured for multiple social networks…
- Customizable Sign-in Interfaces: HP
  Favicons for initial engagement, contextual messages for each ID provider

IIW & ID Commons Intro (T2B)

Convener: Kaliya Hamlin
Notes-taker(s):
URL: http://iiw.idcommons.net/ID_Commons_-IIW_Intro

Tags for the session - technology discussed/ideas considered:

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

Slides can be found here - http://www.slideshare.net/Kaliya/iiw11introtalk

Open & Federated Social Networking (T2C)

Convener:
Notes-taker(s):
URL: http://iiw.idcommons.net/Open-Federated_Social_Networking

Tags for the session - technology discussed/ideas considered:

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

Deep Dive - OpenID AB (T2E)

Convener: Nat Sakimura, John Bradley
Notes-taker(s): Nat Sakimura
URL: http://iiw.idcommons.net/Deep_Dive_OpenID_-_AB

Tags for the session - technology discussed/ideas considered: tech

Attendees:

Nat Sakimura, John Bradley, Chuck Moltimore, Pat Patterson Bob Blakley
Mat Tebo, Eve mailer, Diana Smetters, George Fletcher, Dirk Belfanz, Greg Turner,
Josef Holston, Mike Jones, Tony Nadalin, Marius Scuritescu.

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

Discussed on the details of the OpenID Artifact Binding 1.0RC2 Spec.
https://openid4.us/specs/ab/

Feedbacks:
* Split 8.3 so that chapters goes with data flow.

* Remove client_id definition sentence 2 because it will break existing oauth2 implementations.

* Fix example in 5.3 (=stale)
* Looks like Connect is a duplicate work. Why cannot we converge to OpenID ABC?

VRM Development (T2F)

Convener: Doc Searls
Notes-taker(s): Gon Zifroni
URL: http://iiw.idcommons.net/VRM_Development

Tags for the session - technology discussed/ideas considered:

VRM, independence, symmetrical relation, reverse-cookie, demand first, pull, anonymity

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

Doc Searls starts with a general description of VRM:

You should be in control of the data you generate. In a digital world it is convenient to have all your relations under your control: centrally controlled by you.
> The set of identifiers that give you access to services online.

Problem addressed:
The independence of the individual both independent of anybody else but at the same time able to engage with multiple people.

Iain Anderson of MyDex gave (once) an example that grew out of the kernel of VRM, the change of address. I want to be able to change my address for multiple services at the same time, although various services have single interests in my identity.

XDI (Drummon Reed)
PDS
MyDex
Information Card (Ms)
R-card (relationship card)
Switchbook
Mine! project
Kynetix
Azigo

Iain came up with 4000 variables negotiated within a relationship. There are symmetrical relationships with equal power on both sides. While with asymmetrical relationships you sign a ULA > Web services and business models are anchored on this. "We tell you what the relationship is". You may have a lot more interest about what you buy in the store than they do, but you don't have access to it nor control over it.

Following a question by Susan (Value Networks), Doc gives the example of the loyalty card (green stamps catalog): tracking what you're buying in the store, targeted ads. But they don't know what you actually want, they tell us what we want: intent is not captured.

Joe's response: Game about open systems to being beholden to services. Statement: if an alternative emerges services will adopt it.

Doc talks about multiple pricing schemes to incent buyers to use self-checkout scanning in shops. In a nutshell the history of e-commerce is "1995, the invention of the cookie. The end."

There's more talk about intent "vendors don't know what I want to buy next".

Doc talks about Kynetx: everything is an n point, with an event and a rules-set described by rules-engines.

Joe continues: Kynetx is about augmenting your experience: some of the Google results you might have a relationship with which Google doesn't know about but can be surfaces for you from your end.

Write rules for queries by users/buyers going by shops/stores checking their inventory based on your query.

Supply <> Demand
Routing our intentions: individuals express their demand to generate supply. What's the downside of the store saying they have it? Third party needed to ensure their reputation. If companies are advertising wrong data about their stores: leverage the regulations or social reputation (trust).

Demand <> Supply
 Opposite of CRM where sellers own the relationship with buyers.
 Supply chain automation (question by Ace Swerling)
 Notion that the customer brings a lot to the table
 Reverse auctions example for just in time manufacturing
 Key example is the personal RFP, example of demand driving supply
 Priceline.com, Kayak alerts, consumer type of behavior, LivingSocial, Blippy, Shrout
 Is social the backbone of VRM or not? Are relations the fourth party?
 Joe's comment "Nobody owns email,Ä¶but it wasn't initially."

The r-button in one configuration can say: "I'm willing to deal with customers on your terms"
 With emancyterm both terms (seller, buyer) can be matched up.

Question: Is it similar to ad-exchange? 3 parties: Publisher, Advertiser, User.
Joe says key distinction: the publisher website could have other websites behind it. "You're broadcasting your needs" > Personal generated claim or preferences. Diff with ad-targeting: Groupon is still push from the vendor. The fact that I Like Lady Gaga does not mean that I want to buy the album, I already have it!

(see Reverse-cookie)

Remark: Yes but we tell google all the time what we're looking for, what we want.
Ankit Kapasi: point to point sharing, share within contacts.
> The systems that we have without gesture we find suspicious.

How can we do some of the things we have offline online: offline we have anonymity "I want less identity when I walk into the store". Why can't I take my shopping cart from one site to another?

Problem of this discussion are the commercial examples. Discuss retail commerce without thinking like marketers. Let's try other examples. Why can't I change my credit card when I'm loosing it, while not loosing all your trusted relations?

Kevin Marks talks about how Webfinger helps discovery under the user's control.

No Base String (T2I)

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

Tags for the session - technology discussed/ideas considered:

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

"No Base Strings - Signing JSON"

Examples:

=== ENVELOPE
base64url(sig)

.
base64url({
"algorithm": "RSA256",
"payload": base64url({"a":"b"})
})

=== POSTCARD
base64url(sig)

.
base64url({
"algorithm": "AES256 RSA256",
})
.
base64url(encrypt({"a":"b"}))

==== MULTISIG POSTCARD

base64url(["base64(sigj)","base64(sig)"])
.
base64url({
"algorithm": "HMAC256 HMAC256",
"iv": "1244"
})
.
base64url(encrypt({"a":"b"}))

=== JSON ENVELOPE

```
base64url({
"signature":base64url(sig),
"envelope":
 base64url({
 "algorithm": "RSA256",
 })
"payload": base64url({"a":"b"})
})
```

=== Votes
Envelope is required? (required won)
Postcard vs Envelope (postcard won)
Dots vs JSON as the outer (dots won)
Algorithm encodes profile (shove everything in the algo. Algorithm defines keys in envelope).

Session 3

Attenuated Redelegation (T3A)

Convener: Alan Karp
Notes-taker(s): Eve Maler
URL: http://iiw.idcommons.net/Attenuated_Redelegation

Tags for the session - technology discussed/ideas considered:

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

Twitter OAuth echo: http://dev.twitter.com/pages/oauth_echo

OAuth redelegation: http://tools.ietf.org/html/draft-vrancken-oauth-redelegation-00

Alan's "Horton" protocol: http://research.google.com/pubs/archive/33037.pdf.

WEB (in) Security (T3B)

Convener: Jeff Hodges
Notes-taker(s): Jeff Hodges
URL: http://iiw.idcommons.net/Web_inSecurity

Tags for the session - technology discussed/ideas considered:

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

=JeffH & Dev

Devdatta Akhawe (UCBerkeley <http://www.cs.berkeley.edu/~devdatta/>)
presented on..

"Web (In)Security and Identity Implementations"
<http://powerpoint.officeapps.live.com/p/PowerPointEmbed.aspx?
Fi=SD550F80E1556EC4FC!119&E=1&Fo=1&wc=>

..wherein he discusses a vulnerability found in Facebook Connect's implementation, and another bug -- a 'design bug' -- found in a web single-sign-on protocol (WebAuth). The latter protocol is very similar to various 'front-channel' HTTP-redirect-based web single-sign-on protocols such as SAML web browser SSO profile, OpenID, etc.

The papers where these findings are discussed in detail are..

The Emperor's New API: On the (In)Secure Usage of New Client Side Primitives
http://www.cs.berkeley.edu/~devdatta/papers/w2sp10-primitives.pdf

Several new browser primitives have been proposed to meet the demands of application interactivity while enabling security. To investigate whether applications consistently use these primitives safely and adequately in practice, we study the real-world usage of two client-side primitives, namely postMessage and HTML5's client-side database storage. We examine new purely client-side communication protocols layered on postMessage (Facebook Connect, Google Friend Connect) and several real-world web applications (including Gmail, Buzz, Maps and others) which use client-side storage abstractions. We find that, in practice, these abstractions are widely used insecurely, which leads to severe vulnerabilities and can increase the attack surface for web applications in unexpected ways. We conclude the paper by offering insights into why these abstractions can be hard to use safely, and propose the economy of liabilities principle for designing future abstractions. The principle recommends that a good design for a primitive should minimize the liability that the user undertakes to

ensure application security. We suggest enhancements to the existing browser primitives to make their secure use more practical.

Towards a Formal Foundation of Web Security http://www.cs.berkeley.edu/~devdatta/papers/websec-csf10.pdf

<https://cid-550f80e1556ec4fc.office.live.com/fullscreen?resid=550F80E1556EC4FC!118&filename=csftalk_19Jul_final.pptx&wx=p&wa=p&wv=s&wc=officeapps.live.com&wy=y&wp=y>

We propose a formal model of web security based on an abstraction of the web platform and use this model to analyze the security of several sample web mechanisms and applications. We identify multiple distinct threat models that can be used to analyze web applications, ranging from a web attacker who controls malicious web sites and clients, to stronger attackers who can control the network and/or leverage sites designed to display user-supplied content. We propose two broadly applicable security goals and study five security mechanisms. In our case studies, which include HTML5 forms, Referer validation, and a single sign-on solution, we use a SAT-based model-checking tool to fid two previously known vulnerabilities and three new vulnerabilities. The case study of a Kerberos-based single sign-on system illustrates key differences between network protocols and web protocols and finds a vulnerability that arises because of the way cookies, redirects, and embedded links are used.

The web security model is available as opensouce..

https://code.google.com/p/websecmodel/

Jeff Hodges (PayPal <http://kingsmountain.com/people/Jeff.Hodges/>)

Presented this talk..

The Need for Coherent Web Security Policy Framework(s) http://w2spconf.com/2010/slides/steingruebl.odp

Web-based malware and attacks are proliferating rapidly on the Internet. New web security mechanisms are also rapidly growing in number, although in an incoherent fashion. In this position paper, we give a brief overview of the ravaged web security landscape, and the various seemingly piece-wise approaches being taken to mitigate the threats. We then propose that with some cooperation, we can likely architect approaches that are more easily wielded and provide extensibility for the future. We provide thoughts on where and how to begin coordinating the work.

The position paper underlying the talk is..

http://w2spconf.com/2010/papers/p11.pdf

..and mentioned recent developments since the talk was originally conceived (May-2010)..

* WebSec working group now established in IETF

  - chartered to complete current in-progress specs on..

    - HTTP Strict Transport Security (HSTS)
    - Origin
    - Content-sniffing

  - as well as develop a requirements document for web security policy framework

* HSTS now natively implemented in Firefox 4 and Chrome 4+

  - anticipated just the sort of attacks that Firesheep utilizes

  - onus is now really on web site operators to offer truly secure site access

* WebAppSec working group being established in W3C

  - in-progress W3C specs on CORS and UMB will move over here

  - will be home for Mozilla Content Security Spec (CSP

---
end

VERIFIED IDENTITY CLAIMS – An introduction to U-Prove privacy-enhancing technology (T3C)

Convener: Craig Wittenberg (Microsoft)
Notes-taker(s): Ariel Gordon (Microsoft)
URL: http://iiw.idcommons.net/Verified_Identity_Claims

Tags for the session - technology discussed/ideas considered:
Verified Claims; Identity Attributes; Privacy; Privacy Enhancing Technology; Cryptography; user-centric technology: user control.

Participants

Craig Wittenberg	Microsoft
Ariel Gordon	Microsoft
Jan Unger	
Tim Cole	KuppingerCole
Bret Tobey	Assa Abloy
John Fontana	Ping Identity
Jon Webb	Sony PlayStation network
Nishant Kaushix	Oracle
Takeshi Kitagawa	NTT Communications
Mark Horstmeier	Kynetx
Matt Tebo	Proviti
Greg Turner	Sierra Systems
Mike Min	Booz
Guibin Kony	Google
Aravmdan Ranga	PayPal
Tom Leon	AOL
Jim Fenton	Cisco
Dale Olds	Novell
Ben Goodman	Novell
Fady Semaan	AOL
Henrik Biering	Peer Craft
Stuart Proffitt	Novell
Jeff Stollman	Secure Identity
Ambarsh Malpar	CA
Alex Ran	Intuit
Thomas Hardjono	MIT Kerberos

Peter Capek	Self
Lloyd Burch	Novell
Kimberly Little	LexisNexis
Frank Travestino	eBay
Heather Ford	UC Berkeley

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

Link to slides: http://iiw.idcommons.net/File:U-Prove_technology_overview-Nov2010.pdf

Verified Identity Claims -- Technical introduction
Craig Wittenberg presented the U-Prove technology
U-Prove well respected in academia. Originally created by Credentica; purchased by Microsoft two years ago; incubated as part of the Verified Claims Team .

Similar characteristics as X.509 certificate but with much better privacy characteristics.

Craig presented a few scenarios, starting with Alice purchasing wine online and proving that she's over 21 and that she's a resident of WA state.   Other scenarios included leveraging a German eID to access citizen and private services.

Many clarification Q&A followed on the technology and its benefits, including:

Q: Why not do back-end attribute exchange? Why go through all this trouble for exchanging attributes?
A: There are scenarios with privacy requirements such as un-traceability. If you take the case where Governments issue identity claims, there are requirements for the government not to be able to trace where the user is using his proof of age (for example). Depending on the geography, the privacy requirements may come from the government itself or from Privacy Groups.

Q: If there is a Cloud Service that stores and releases information, does it effectively create a secondary IdP?
A: If there are no client side bits, there is effectively a "broker" in the cloud that manages the user's private keys. Microsoft and its partners are investigating different ways to build the u-prove verified claims agent that mitigates those issues.

Facebook as PDS (T3D)

Convener: Joe (Switchbook)
Notes-taker(s): Ankit Kapasi
URL: http://iiw.idcommons.net/Facebook_as_a_Personal_Data_Store

Tags for the session - technology discussed/ideas considered:

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

Place where I share "my data" with service providers

•

Data provided from Facebook:
o Basic- name, friend list, gender, likes
o Extended
o Everyone data set

•

Permission to data set granted at first interaction
o By user
o By service
Instant Personalization – Facebook now moving towards opt-out instead of opt-in
o No permission ceremony
Authentication and then website uses OpenGraph API
FB did right
o Scaled quickly
o People submitted data without thinking about it (was it a trick?)
o Start with the .edu and connected within
o Allowing websites to cache the data, critical to website growth
Missing from FB platform:
o People don't have ability to control terms of data use
o Incomplete and non-customizable (e.g., cant add your own public key)
o Tweak the permissions after time passes
o Open Standards / Substitutable (can now download copy of data)
o Verification of identity and specific data elements
o Setting per Vendor
o Stability in Privacy and other policies
o Terms for users on the 3rd party website

JSON Token Spec Work (T 3E & 4E)

Convener: Mike Jones
Notes-taker(s): Mike Jones
URL: http://iiw.idcommons.net/JSON_Tokens

Tags for the session - technology discussed/ideas considered:

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

MIKE's Notes:
We held two back-to-back sessions today at IIW (after lunch in space E) intended to produce consensus positions on JSON Web Tokens, including signing and encryption. Substantial consensus emerged, which is described in the notes below.

These consensus decisions were in place by the start of the session:
· There is an envelope (a.k.a. header) that completely describes the cryptographic algorithm(s) used
· There is a payload (a.k.a. body) that is distinct from the envelope
· There is a signature that is distinct from the envelope and payload
· Base64url encoding without padding is used to encode the parts above
· The compact token representation separates the three encoded parts above by periods
· No line breaks or other whitespace may be present in this representation
· Encryption must be supported as well as signatures
· The token representation should be compact
· In particular, this means that multiple base64url encodings of the same content should be avoided
· Any need for canonicalization should be avoided

Open issues identified at the start of the session were:
· Ordering of the fields
· Ordering of the signing and encryption operations
· What can be in an envelope (a small fixed set of things or is it extensible)?
· What to sign (envelope.payload or just payload)?
· What can be in the payload (only JSON token objects or arbitrary base64url encoded byte streams)?
· Do we need to support multiple signatures?
· Should we specify a JSON serialization as well as a compact serialization?

These issues were resolved as follows:
· Ordering of the fields
By a vote of 8 to 1, people preferred the ordering envelope.payload.signature over the ordering signature.envelope.payload. Two reasons were cited: First, this allows

for stream-mode operations, where consumers can begin operations based upon the contents of the envelope before the signature has arrived without having to buffer the signature, and where producers can compute the signature in parallel with the transmission of the envelope and payload. The counter-argument advanced by Paul Tarjan of Facebook (in abstentia) is that all languages have a string operation to split a string on the first occurrence of a character.

· Ordering of the signing and encryption operations
How to compose these operations depends upon scenario requirements. Goals identified include Integrity, Confidentiality + Integrity, and Non-Repudiation. Paul Hill identified four sets of relevant operations, which were public key signature, symmetric key MAC, symmetric key confidentiality + MAC, and key wrap/key transport/agreement with Diffie-Hellman. Some took the position that we should define a small set of fixed configurations that are known to safely achieve the intended goals; others argued for general composability of operations. This was the one topic that we had to defer to a follow-on session to be held tomorrow, due to time limitations.

· What can be in an envelope (a small fixed set of things or is it extensible)?
We reached a consensus that the envelope needs to be extensible (but should be extended only with great care).

· What to sign (envelope.payload or just payload)?
Given that the envelope is extensible and therefore may contain security-sensitive information, we reached a consensus (with input from Ben Laurie via IM) that the combination envelope.payload must be signed.

· What can be in the payload (only sets of JSON token claims or arbitrary base64url encoded byte streams)?
By a vote of 9 to 2, the group decided that the spec should support signing/encrypting of arbitrary base64url encoded byte streams. They also decided that the spec should define the syntax and semantics of a set of claims when what is being signed is a set of JSON claims.

· Do we need to support multiple signatures?
The group voted 5 to 2 that it must be possible to support multiple signatures in some manner. Two variants of multiple signatures were discussed: the "gateway case", where additional signatures are added to a token as it is passed between parties, and the parallel case, where multiple parties sign the same contents up front. However the group also decided that it would be overly complicated to support multiple signatures in the compact serialization. Support for multiple signatures was pushed to the JSON serialization (per the next issue).

· Should we specify a JSON serialization as well as a compact serialization?
The group decided by a vote of 11 to 1 that there were use cases for a JSON serialization, and that multiple signatures would be possible in that serialization. The

syntax agreed upon simply uses the three base64url encoded fields, while allowing there to be parallel arrays of envelopes and signatures. Specifically, the syntax agreed upon was:

{"envelope":"["<envelope 1 contents>",…,"<envelope N contents>"],
"payload":"<payload contents>"
"signature":["<signature 1 contents>",…,"<signature N contents>"]
}

and where each signature i is computed on the concatenation of <envelope i contents>.<payload contents>.

I'll follow this note with notes from the planned encryption session tomorrow.

Mobile Social Networking (T3F)

Convener: Monica Lam
Notes-taker(s):
URL: http://iiw.idcommons.net/Mobile_Social_Networking

Tags for the session - technology discussed/ideas considered:

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

OpenID Connect, OAuth Discovery, Webfinger etc. (T3I)

Convener: David Recordon & Kevin Marks
Notes-taker(s): Kevin Marks
URL: http://iiw.idcommons.net/OpenID_Connect_Discovery

Tags for the session - technology discussed/ideas considered:

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

There is a tension between discovering service endpoints for a domain, then applying that for a present user, and looking up information about other users, and getting access to endpoints to connect to them.

WebFinger is focused on user-specific lookup; need to optimize the domain-general lookup too.

Phil's blog post is good notes here:

http://www.windley.com/archives/2010/11/discovery_webfinger_and_openid_connect.shtml

Phil's Blog Post

Discovery: Webfinger and OpenID Connect

I'm sitting in a session on webfinger, OpenID Connect, and discovery session. Discovery is a the process of turning a small piece of information (like a user ID) into the URLs and APIs needed to service some specific request. For example, say I tell you my email address is *windley@gmail.com*, how do you find my profile? Of course, as long as we're talking about one site, like Google, we can just hard code that translation. But how can the discovery problem be generalized?

That's the goal of Webfinger: *WebFinger is about making email addresses more valuable, by letting people attach public metadata to them*. You can try it yourself at webfinger.org (try it with your GMail address, for example).

There's also the related problem of how to know, for some particular host, where to get the webfinger data. That's the job of the host-meta file, a well-known URL proposal.

For example the host-meta data for Google is here:

```
http://gmail.com/.well-known/host-meta
```

and it returns

```
<XRD xmlns='http://docs.oasis-open.org/ns/xri/xrd-1.0'
    xmlns:hm='http://host-meta.net/xrd/1.0'>
  <hm:Host xmlns='http://host-meta.net/xrd/1.0'>gmail.com</hm:Host>
  <Link rel='lrdd'
      template='http://www.google.com/s2/webfinger/?q={uri}'>
    <Title>Resource Descriptor</Title>
  </Link>
</XRD>
```

This tells us that we can get data about a GMail account from the URL

```
http://www.google.com/s2/webfinger/?q={uri}
```

by substituting the GMail address for `{uri}`. So we can get my webfinger data from

```
http://www.google.com/s2/webfinger/?q=windley@gmail.com
```

This URL returns the extensible resource descriptor (XRD) as follows:

```
<XRD xmlns='http://docs.oasis-open.org/ns/xri/xrd-1.0'>
  <Subject>acct:windley@gmail.com</Subject>
  <Alias>http://www.google.com/profiles/windley</Alias>
  <Link rel='http://portablecontacts.net/spec/1.0'
      href='http://www-opensocial.googleusercontent.com/api/people/'/>
  <Link rel='http://portablecontacts.net/spec/1.0#me'
      href='http://www-opensocial.googleusercontent.com/api/people/103887646945247867113/'/>
  <Link rel='http://webfinger.net/rel/profile-page'
      href='http://www.google.com/profiles/windley'
      type='text/html'/>
  <Link rel='http://microformats.org/profile/hcard'
      href='http://www.google.com/profiles/windley'
      type='text/html'/>
  <Link rel='http://gmpg.org/xfn/11'
      href='http://www.google.com/profiles/windley'
      type='text/html'/>
  <Link rel='http://specs.openid.net/auth/2.0/provider'
      href='http://www.google.com/profiles/windley'/>
  <Link rel='describedby'
      href='http://www.google.com/profiles/windley'
      type='text/html'/>
  <Link rel='describedby'
      href='http://www.google.com/s2/webfinger/?q=windley%40gmail.com&fmt=foaf'
      type='application/rdf+xml'/>
</XRD>
```

If you look closely, you'll see that there is a subject, and alias, and a lot of URLs that are tagged in ways that tell you categorically what kind of thing they return about the subject. For example, the entry with

```
rel=http://microformats.org/profile/hcard
```

tells you where to get [HCard data](#) about me.

You might notice that there's a lot of XML here. There are proposals to turn this into JSON, such as [JRD](#), the JSON resource descriptor. Lots of discussion about why this is better, easier, and so on.

One extension is to allow for access tokens to get non-public information. For example, you can get my publicly available information from the profile URL, but what if I've been to your site or app and allowed you access to non-public data? Can you get it using this mechanism. What's the standard for specifying how to pass the OAuth tokens, for example.

So, if I understand correctly, OpenID Connect is a variation on Webfinger that uses JSON, extends it in important ways, and allows OpenID (and other systems) to dynamically put relevant links to services on sites without hard coding them. This allows small players to compete in the NASCAR game. Most service providers won't be big enough to get their button hard coded on a site, discovery allows them to get dynamically added when the site knows that they're relevant.

Session 4

Pseudonyms for Privacy (T4C)

Convener: Jay Unger
Notes-taker(s): Jay Unger
URL: http://iiw.idcommons.net/Pseudonyms_for_Privacy

Tags for the session - technology discussed/ideas considered:

Pseudonyms, OpenID

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

- The meeting was attended by about 20 people.
- Jay Unger gave a short presentation about Pseudonyms. http://www.slideshare.net/JayUnger/iiw-11-pseudonyms-5771938
    - In this context he defined a Pseudonym as being unique value returned from and authentication transaction that was related to the combination of user and relying party.
- There seemed to be general consensus that Pseudonyms are good way to preserve user -privacy / -centricity across many Relying Parties
- Jay suggested that Pseudonym should be the default information returned from an OpenID authentication transaction and the ONLY information returned without specific additional requirement of the Relying party.
    - There seemed to be general consensus for this notion that Pseudonyms should be the default.
    - However there is tension from Identity providers like social networks and portals to do just the opposite. The direction that Identity providers like Google and Yahoo seem to be headed is to return globally unique Pseudonyms that are only related to the Identity provider and user and NOT unique to the combination of user and relying party. This explicitly allows user correlation across Relying parties.
    - The user correlation feature that some Identity and Relying party groups seem to desire could be accomplished using attributes specifically designed for that purpose.

        Such attributes would essentially be Pseudonyms that were only unique to the user and perhaps Identity provider.

        If these attributes were generated and treated separately from Pseudonyms that are Relying Party specific, then users could decide which of the two different types of attributes that wanted an Identity provider to return and thus control the level of "identification" they wished to express with a particular relying party.

- Jay also discussed a use case and requirement to support use of the same Pseudonym presented by different Identity Providers, for the same user's authentication with a particular Relying party. This, for example would allow a user to associate the same profile for that Relying party with both their personal and business userid.
    - This was thought to be a difficult requirement since in this case the Pseudonym generated by one Identity provider would be employed by a second Identity provider.
    - In the absence of attributes (assertions) being digitally signed by the issuer(in this case the Identity provider that created the Pseudonym) many Relying parties are judging the value of a returned id based only on which Identity provider returned it.
    - For example Yahoo and Google presently return a Pseudonym that is related to the combination of the user, Relying party and Identity Provider realm. They do not expect to get a Pseudonym they generated to be presented by any site other then themselves and would not readily trust their own Pseudonym (though I don't necessarily know how they would tell) if it where received from another Identity provider.
    - Jay outlined a method from transferring a Pseudonym related to a particular RP (relying party) from one IdP to another:
        - The user would first authenticate to a site (RP) with either an existing IdP that they had already used to register at the site or a new IdP that the site had not yet seen.
        - That authentication would either present a Pseudonym that either was either already recognized if the user was already "registered" with the site (RP) through that IdP, or not if the user had not used that IdP to register.
        - If the Pseudonym was not recognized by the site (RP) the user would have the option to continue registration with site an generate a new registration (and a different identity) or to try to associate an existing registration with the site from another IdP.
        - If the Pseudonym was recognized the user would be logged in and would be able to request association of their existing registration to another IdP (by selecting an account or profile management function at the RP site.)
        - If the user wished to associate their registration with another IdP The RP site would permit the user to select another IdP (either via URL or NASCAR selection) and then request an authentication from that second IdP. The second IdP would return their Pseudonym.
        - The user would be permitted to select whichever IdP and Pseudonym that the user desired to retain as their identity attribute associated with the Relying Party (either from the first IdP or the second IdP).
        - A request would send the Pseudonym chosen from whichever IdP the user selected to the other IdP to replace the Pseudonym they would respond with for that site (RP) in the future for that user.
        - The user could remain logged into the RP site with either or both IdPs.
        - Assuming that these pseudonyms are essentially attributes (in future OpenID protocols) and that they are digitally signed both by the agency (IdP) that created them and probably by the agency presenting them in response to an authentication request, such pseudonyms would derive

authority both from the IdP that originally created it and from the IdP that was presenting the attribute to the RP.

Rap Leif (It's a Joke?) (T4F)

Convener: Joaquin
Notes-taker(s):
URL:

Tags for the session - technology discussed/ideas considered:

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

Handling Unregistered Clients in OAUTH2 & Open ID Connect (T4I)

Convener: David, Kevin Marks
Notes-taker(s): Kevin Marks
URL: http://iiw.idcommons.net/Handling_Unregistered_Clients

Tags for the session - technology discussed/ideas considered:

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

Currently OAuth 2 in practice requires pre-registered developer information, specifically the callback URL, and obtaining access tokens that are built inot the site.

This has 2 problems:

1) requires up-front work by developers to try things out

2) is problematic for non-web clients (mobile, desktop) as they need to bounce stuff via a website to work.

The advantage for the host site is that they can track and throttle developers calling APIs and have TOS agreement and verified contact address for them.

Other options:
Anonymous
Advantage is that this is very easy for developer to try things out; drawback is that host can't identify by app easily, and potentially leaking user info:

* give public subset of data

* warn strongly in auth dialog

* throttle strongly

Dynamic allocation
Advantage is that the flow is closer to registered flow, and because host can distinguish apps, can apply er-app throttling/monitoring. Above use suggestions may still be useful

Callback endpoint Discovery

by applying WebFinger or other ./.well-known/ based discovery to the callback URL, the host can validate the callback does belong to the site and is not a redirector, and get logo, description and other metadata to show the user. Potentially this could also be used for key discovery and verification between sites, for the University/

Salesforce / Google Apps use cases, though that is currently hard on purpose because of the broad access permissions there.
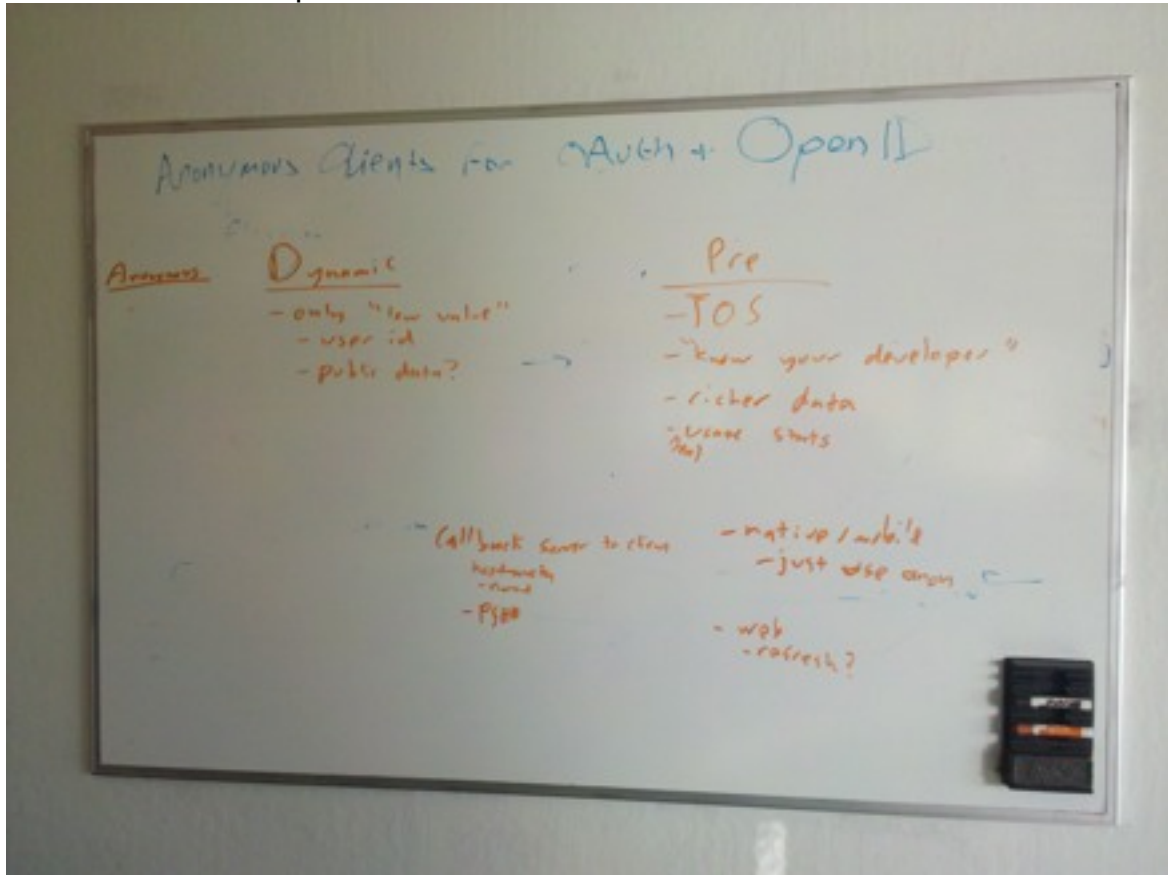
Session 5

Change Notify Proposal (T5A)

Convener: P.Hunt
Notes-taker(s):
URL: http://iiw.idcommons.net/Change_Notify_Proposal

Tags for the session - technology discussed/ideas considered:

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

Link to PDF

File:IIW11 TUE 5A ChangeNotify-IIW.pdf

OAuth Multiple Token (T5B)

Convener: Yusuke Kondo
Notes-taker(s): Yusuke Kondo
URL: http://iiw.idcommons.net/OAuth_Multiple_Token

Tags for the session - technology discussed/ideas considered:

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

      Slides for session can be found here:
http://www.slideshare.net/konfoo/oauth-multiple-lifetime-token

NSTIC Update and Action (T5C)

Convener: Jay Unger
Notes-taker(s): John Fontana and Jay Unger
URL: http://iiw.idcommons.net/NSTIC

Tags for the session - technology discussed/ideas considered:

    NSTIC, US Government, Policy

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

Notes from Jay :

- The meeting was attended by about 20 people.
- NSTIC (pronounce nistick or en-stick) = National Strategy for Trusted Identities in Cyberspace.
- Jay Unger gave a brief presentation (attached) on the history and present status of the NSTIC draft document. http://www.slideshare.net/JayUnger/iiw11-nstic-update
- NSTIC Document first published on the White House Blog by Howard Schmidt http://www.whitehouse.gov/blog/2010/06/25/national-strategy-trusted-identities-cyberspace on June 25th 2010
- Document still available at http://www.dhs.gov/xlibrary/assets/ns_tic.pdf
- Public comments were accepted at http://www.nstic.ideascale.com from June 25th to January 19th 2010.
- High-level document – mostly vision, examples, and goals and objectives. Very little technical detail or technology specifics. No specific implementation plan or schedule.
- Recognizes the need for a general identity mechanism on the internet to support and enhance both public and private interaction between citizens and government, businesses, organizations etc. Also, to reduce risks associated with identity theft and fraud for all citizens.
- Federal government intends to take a leadership role in the specification and exploitation of NSTIC. They say that they recognize the need to work with both the information industry and citizens to define the policy and technology of NSTIC.
- Open Letter to Howard Schmidt at the White House on July 16th 2010 by : Center for Democracy in Technology (CDT), Electronic Frontier Foundation (EFF), Liberty Coalition *http://www.cdt.org/files/pdfs/20100716_nstic_extend_ltr.pdf*
  Requesting:
  - "… that the public comment period be extended for at least 30 days to facilitate more robust public discussion … that subsequent public comment periods on this topic extend for at least 90 days"
  - "… clarification on the agency's proposed timeline and process"
  - "… an opportunity to convene an in-person discussion with an appropriate White House or DHS official to discuss this important matter and engage in further public discussion."
  - Results: No extension of public comment period (IdeaScale was closed to new posts on 7/19/2010). However, CDT personnel have had at least two follow-up meetings with the

cyber-security staff at the White House between mid-July and the present and they have had the opportunity to review and comment on new document drafts being developed including an implementation plan and schedule.

- CDT has been informed that work is ongoing, internal agency reviews are being conducted, and no announcements are expected before the beginning of next year.

-

● Jay Unger reported that at a meeting on Cloud Computing on October 19th in Washington D.C., hosted by NSF/NITRD at the National Academy of Public Administration, Vivek Kundra, CIO of the U.S. in the Executive Office of the President (who was the introductory speaker) answered a question regarding NSTIC and said that he expected some sort of announcement this year. Thus we have somewhat conflicting statement from different government officials and we really don't know when further details regarding NSTIC will be made public.

● There was a good deal of discussion regarding the possible value / concerns about government leadership in the area of identity management on the internet but there seemed to be general consensus that the government could at least act as a catalyst to move technical and policy issues forward.

● Jay Unger expressed concern that the IIW community should try to exert some sort of influence and technical advice to the government in this area given the expertise and experience of the community. Several attendees agreed but we were all at somewhat of a loss as to how to approach the government given their present silence.

● Jay Unger asked the attendees to add their e-mail addresses to the sign up sheet if they were willing to join a mailing specifically for communication and action regarding NSTIC that he would try to get the OpenID Foundation or some other body to host. In later conversations with OpenID Foundation it was determined that perhaps the Open Identity Exchange (OIX) might be a better host for the list. Jay will follow up with the leadership of both bodies (and perhaps others) to establish this list and make an initial posting in the second half of November 2010.

Link to John Fontana's below blog post here:

> http://www.pingidentity.com/blogs/pingtalk/index.cfm/2010/11/3/Is-the-US-governments-Identity-Ecosystem-already-polluted.

November 3, 2010 , John Fontana | IdM, Internet

Mountain View, Calif. - Just over four months after the first-draft release of the Obama administration's National Strategy for Trusted Identities in Cyberspace (NSTIC) the proposal is at a major crossroads, says independent consultant Jay Unger, who led a session on NSTIC at Monday's opening of the IIW Conference (formerly known as the Internet Identity Workshop).

"It is already showing signs of burnout," says Unger. "The fact the government is dithering on when it might speak about [NSTIC] again is a concern."

Chief among those concerns is a potential final specification, polluted by politics, that could "blow everything away that the identity community has been doing for the past five years," says Unger.

While that might be the far end of the disaster spectrum, Unger, an ex-IBMer whose IT career spans 40 years, says the government's silent treatment leaves people to wonder what the worst-case scenario just might be.

And public comment on the draft spec shows many of those people are already fearful of strong governement involvement in establishing a digital identity system.

"We need to find a way to get this [identity] community involved," he said about the IIW attendees and others. "The time to start talking with citizens and the identity community is now and not after the government has made a lot of decisions [on its own]."

Unger, who lives just outside of D.C., says he has been going up to Capitol Hill as an ordinary citizen and "pounding on the stell doors as hard as I can."

Back on June 25th when NSTIC went out for public review, the promise was for an "Identity Ecosystem" designed to be "a blueprint to reduce cybersecurity vulnerabilities and improve online privacy protections through the use of trusted digital identities."

But the question now is not the technology to support that goal, says Unger, but "policy, socialization, education and legal liability."

Unger's suggestion is for dialogue to begin now to help finalize NSTIC. The dialogue should take the form of a non-government organization (NGO) similar in design to familiar standards and architecture bodies such as the Internet Engineering Task Force (IETF).

"If [NSTIC] ends up getting shuffled from agency to agency that process could hurt it," said Unger.

This fall, at the IIW-East conference in Washington D.C., Unger said that every federal agency he could think of showed some sign of opposition to NSTIC.

Washington insiders told him that if the government anointed one agency to lead the charge that other agencies would have "an instant allergic reaction" because they did not get the top job.

In addition, there was concern that certain agencies, say the FBI, may not be particularly trusted by the public to lead an effort to create, as the NSTIC Web

[site states](#), "protection of the identity of each party to an online transaction and the identity of the underlying infrastructure that supports it."

Unger believes an NGO could help the process stay on track. He theorizes the NGO would have a few industry luminaries, two or three leading non-partisan politicians, a lawyer specializing in identity, and some educators.

"The government could set this up, give it some seed money and step back and say we are going to participate like everyone else. [They could say] we will make sure it meets use cases for government, health care and others. The government would get it started, but it is not going to do all the work."

Public comment on the draft NSTIC document is closed, but the web site includes this invitation, "Public ideas and recommendations to further refine this Strategy are encouraged."

The original timeline for NSTIC's completion, which called for its release "as soon as practical," now weighs more heavily on "practical" than "soon."

The government had hoped to finalize NSTIC this fall, but next year is the likely target now for anything tangible.

"Sometime between mid-December and mid-March, we'll hear the next shoe drop from the government," says Unger. "The good news is the government is a centipede so there are lots of shoes to drop."

OpenIDConnect Deep Dive (T5E)

Convener: Breno de Medeiros/ David Recordon
Notes-taker(s): Chuck Mortimore
URL: http://iiw.idcommons.net/OpenID_Connect

Tags for the session - technology discussed/ideas considered:

OpenID Connect, OpenID Artifact Binding

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

Comparison and Contrasts between three proposals for a new generation of OpenID protocol based on Oauth2: The OpenID Artifact Binding (AB), The OpenID Connect proposal 1 (OIC1, by David Recordon, Facebook), and OpenID Connect proposal 2 (OIC2, by Breno de Medeiros, Google)

AB characteristics:

−Allow to define request parameters by supplying a reference to a file containing a request descriptor, which allows for fixed URL-length requests
−Provides bindings to all OpenID 2.0 extensions
−Provides backward-compatibility of identifier
−Provides a clear path to higher levels of assurance
−Based on Oauth2 WebServer profile

OIC1/OIC2 characteristics:

−   Provides OpenID Connect flows for multiple Oauth2 profiles (Web Server, User-Agent, Assertion)
−   Support clients that are not capable to perform cryptographic operations
−   Establish a standard Oauth2-protected endpoint, called the UserInfo API endpoint
−   Binding of OpenID extensions TBD
−   Emphasis on new identifier format: binding between old and new identifiers must be provided by a defined account linking step
−   Higher levels of assurance path not described; however, because both OIC1 and OIC2 call for the user of standard JSON tokens to convey assertions, the AB security mechanisms are directly translatable in OIC1/OIC2

In addition, OIC1 describes a mechanism for session management.

Additional discussion on OIC1/OIC2:

- Reconciled token format between OIC1 and OIC2: both now call for a signed JSON blob containing an expiration date, a user_id, and the Oauth2 access token, all signed; and additionally return the Oauth2 token separately for convenience of clients that are not crypto-savvy

Personal Data EcoSystem (T5F)

Convener: Kaliya Young Hamlin
Notes-taker(s): Barbara Bowen
URL: http://iiw.idcommons.net/Personal_Data_Ecosystem

Tags for the session - technology discussed/ideas considered:

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

Kaliya opened the session by reflecting on the past developments and identifying areas to improve:
Mistakes around previous standards and adoption?
Identity commons founder Owen Davis sought to retrieve personal data from service providers
Individuals have many digital devices and data beyond personal devices.

Three points of data aggregation are currently prevailing: Search, Telcos and call logs, and "Cookie land"

How can individuals have a personal data...store, service or cloud where there is a personal copy of data?

User owned ad exchange, how do consumers create personal rfps?

System overview:
Individuals have comprehensive and integrated view and data bank to self-monetize personal information.

Adoption will accelerate with Conversations around individual data service provider lock in and Incentives for service providers to cooperate.

Previous models:
Publisher provides a venue for things to happen, what, where, who, when?
Publisher shapes user experience and aggregates audience.

Key Points:

- New shift... center of universe is wherever you are.

- Marc Davis describes cloverleaf conversion to understand relationships where suddenly the data that can be fused through intent and interaction.

- MyDex in the UK is an asset locked corporation, they are a community interest company to work on behalf of the end users. This is a working model that links to current information, agencies and vendors. Goal is to isolate an immediate form of data
through change of address.

- The core technology should work seemlessly.

-VRM is a homebase to make connections with 3rd and 4th party intermediaries. A specific RFP gives the user control and is given a voice in the marketplace. B-to-B is a huge dimension of VRM as well. Lead generation is personal, with VRM I could become my own qualified and personally verified lead generator

-Business models, service providers, interaction between entities, are key elements.

-Peer to peer linking is very important to build in to the set of services as well as network portability.

-Groups are able to provide authentication and authorization and assert themselves.

-Cloud services apps will be linked to a personal data store to provide interesting services. An example is a wish list, that is implicit to location and inventory.

-Schema interop between databases and data rights is a point of focus in standardization. Currency conversion is an example of data interop is present in monetary systems and markets.

-What lessons have been learned, and what are some of the turning points?

-The federal trade commission has been holding hearings about personal data. "The user has been seen as someone to exploit when services optimize to monetize."

-Scott David suggests privacy as a product placed in a position to gain interest and engagement between business and individuals. Operations and functions that are reliable and can be shaped through services. Parameters for these of economics can scale.

-The issue of greed vs. fear in society.

-Market efficiencies through cohesive needs. Data should flow and the information can be observed. Data flow can have a regulatory level.

Additional follow up sessions about the personal data ecosystem were
suggested: Marketing message, Business Models, Knowledge, roles and
entities, Identity portability..

Next Conversations:

- Commercial incentives that benefit users when they expect things for free.
- How to bring regular old users in
- User Experience
- Relating to the Telco Universe
- Database scehmas and interop - many to many database normalization
- What are the Business models for information assets
- Pooling knowledge on ecosystem rolls
- Current and proposed credit agencies
- Low level technology stuff OAuth related to personal data ecosystem claims
- More data, more correlation, more anonomyization breaks down. What are the terms for derezing data - APIs on resolution. What are ranges and thresholds

Health & VRM (T5G)

Convener: Greg Biggers
Notes-taker(s): Greg
URL: http://iiw.idcommons.net/Health_and_VRM

Tags for the session - technology discussed/ideas considered:

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

Making Security Decisions Disappear (T5I)

Convener: Alan Karp
Notes-taker(s): Alan Karp
URL: http://iiw.idcommons.net/Making_Security_Decisions_Disappear

Tags for the session - technology discussed/ideas considered:

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

A short version of the slides I presented are at http://www.hpl.hp.com/personal/ Alan_Karp/Disappear.pptx.

Day Two – Wednesday November 3rd

Session 1

Value Network Mapping & Analysis for Personal Data Ecosystem…Mapping (W1A)

Convener: Kaliya Hamlin
Notes-taker(s): Kaliya and Susan
URL: http://iiw.idcommons.net/Value_Network_Mapping

Tags for the session - technology discussed/ideas considered:

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

Future Phone Device Authorization (W1D)

Convener: Dick Hardt
Notes-taker(s): Dick Hardt
URL: http://iiw.idcommons.net/Future_Phone_Device_Authorization

Tags for the session - technology discussed/ideas considered:

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

Enterprise OAuth BOF (W 1E + 2E)

Convener: Marius S. Justin R.
Notes-taker(s): Phil Hunt
URL: http://iiw.idcommons.net/Enterprise_OAuth_BOF_Level_Set

Tags for the session - technology discussed/ideas considered:

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

Minutes of the Enterprise OAuth BOF

Apologies if I missed any attendees. These are notes are an attempt to paraphrase the general discussion only. Please let me know of any missing items and edits!

Many thanks for the large group of folks that attended to make this session really work. While I started this with a blog post and provided some loose organization, it was great to have everyone come forward to offer to pick up talks in advance. Special thanks to Patrick Harding of Ping Identity, Thomas Hardjono of MIT, Eric Sachs of Google for the help in setting this up. As in the notes, it is clear we should keep the dialog going. Feedback is appreciated. Should we follow with more IIW sessions, or should we meet more frequently?

Regards, Phil

Use Case Session, Led by Nishant Kaushik

Nishant Kaushik started the discussion with describing the Mint.com web site as an example of usage of uid/pwd and screen scraping of banking information which was something that is of concern to the banking community. One of the issues discussed that in the current status this might help the banks because as unwilling participants they can't be expected to accept liability. Whereas with a potential OAuth solution, they would be seen as supporting 3rd party access.

Patrick Harding indicated that this is a generic case here where businesses have partnered often with 3rd party services but want to deliver convenient SSO enabled service, but then the 3rd party needs access to data from the owner. Rather then opening broad access to the 3rd party, the enterprise actually does prefer a delegated access model as offered by OAuth.

There was some discussion that there may be some variations in scenarios where content providers are offering licensed or metered content.

There was a general discussion that there are lots of enterprise/consumer use cases, some where user consent is required, others where it isn't needed. Bob Blakley pointed out that in many cases, (such as the Banks) they will also want to ascent to a service provider acting on a user's behalf.

The conversation then shifted to one around how operations are initiated, Patrick Harding indicated that the Mint model follows a SP initiated paradigm whereas a bank referring a customer to a 3rd party service provider is an IDP initiated paradigm. The IDP initiated paradigm is certainly more common at present.

Prateek Mishra asked if there is an issue of duration, scope, and granularity of consent? Patrick indicated that Ping sees this as proceeding along strong contractural relations between SPs and IDPs.

Nishant: there is also the app store model. There are enterprise customers that do want to build 3rd party value-add services.

Alan Karp: Commented that Oauth tokens can be used as an enabling technology, bearer tokens that carry limited rights with minimal buy-in.

Prateek: Do you think bearer tokens are enough?

Alan: I don't know if they are enough, but they are a starting point

Bob: If you think they are enough you should go to the firesheep presentation.

Prateek: The issue is whether there is a strong binding to the service provider...so that the token can't be passed around

Alan: You can't stop passing around. They will want to do that.

Eric Sachs: This doesn't have to be solved technically it could be solved in contract law.

Bob: The question becomes is the CP authorizing mint.com or is it authorizing the user to allow mint.com to access.

Alan: The user wants to click on a share button and grab a token that can be passed around to familiy members.

Prateek: Isn't that an extended case where the access token is not bound to the SP, but rather is just bound to the user.

Paul Madsen: Who asks for the token, is it the user, or the application working on behalf of the user?

Bob: You could design it to work either way.

Patrick: Not sure we're hearing that kind of requirement in the enterprise space.

Alan: We have built several UIs where the user doesn't have to worry about the underlying complexity.

General/Prateek: There could be a general policy that states that clicking on a "share" button indicates certain types of consent.

Chuck Mortimore: Mentioned that there are ssos and session management issues to think about.

Bob: OAuth are being used to establish corba-like "associations" to handle the absence of session management. The idea is to remove re-authentications that are occuring because of session management issues rather than a policy requiring re-authentication.

Bob: are we overloading session management on to Oauth

Chuck: OAuth gives the applications an idea of a separate identity from the user...they can make different access decisions about the entity.

Bob: The fact that people are doing this without it being designed to happen may be a good reason to be worried.

Prateek: Do we need some guidance on OAuth+sessions.

Chuck: people seem to be already handling this well. Probaby we need good guidance on refresh, issues and re-authentication issues.

Observations...
1 Questions whether content providers (e.g. banks) will agree to participate in an OAuth delegated system

2. What forms of user consent needed: IDP, Content Provider. Long term vs. Short term (transactional)

3. Token strength and format, bearer, others?

4. Token is bound to a user, should not be bound to a service?

5. User may not have direct relation with the service provider.

6. On subject of contracts or relations:
  CP would have list of SPs
  - static relations
  - user believes they are interacting iwth the content provider?
- CP is the only IDP
- Or, Dynamic - no pre-existing relationship defined. Parties are brought together by the user

7. B2B use-case

8. Methodology to Expose apis on the internet

9. Session management. Need guidance on refresh issues and re-authentication.

Kerberos and OAuth, led by Thomas Hardjono, MIT

Thomas Hardjono - I'm with the MIT Kerberos consortium. When we first heard the news, we felt kerberos had been re-invented again.

We have the same questions with regards to the tokens.

Gartner had some data 60% of enterprises deploy AD and kerberos enabled infrastructure.

For many being able to sell software into the enterpise, being able to work with windows kerberos is a given.

Redhat has a product called FreeIPA which has this challenge.

What we are hearing from financial folks is how can replicate this infrastructure for our own customers. How can we can extend Kerberos service tickets to be used as tokens? Why because this has been looked at for 20 years. TGT is equivalent to refresh token.   Many of the functionality of OAuth has been available in Kerberos for some time.

So customers are asking how kerberos tickets can be used in a federated relationship.

How can we integrate kerberos with OAuth.

One possiblity is to wrap a service ticket so it can be used in OAuth. But the other side would have to know how to unwrap it.

vmware: Some of the hold hierarchical admin models of old systems does not work in the cloud.
The rigidity is not because of the protocol, but rather the implementation.

If you toss out k

Phil: Oauth is working on a cloud architecture where relationships are highly firewalled. Can a Kerberos adapt well to this environment?

Chuck: the oauth ocmmunity is also working from a place of large scale and availability. It isn't necessarily that isn't being ignored.

Thomas: There hasn't been a history that proves the success of oauth

Chuck: Yes, there is an issue that some sites want to deploy relatively lightwieght by intent. Yet if a poorly implemented OAuth situation gets compromised the press won't differentiate it from an enteprise implementation that is secure.

Thomas: there isn't a spec for token in OAuth.

Chuck: That's true, but most web tokens aren't specified or standardized.

Pam: tokens shouldn't be specified, but they should be translatable.

Chuck: The ability to adjust tokens to a standaridized form is difficult. The tokens don't need to be interoperable and there isn't really value in having that way. Changing the session tokens has huge impact. If I need to exchange with a partner I federate and do token translation at that point.

General...there are lots of situations where kerberos is used to authenticate to the IDP which then issues a saml assertion to bootstrap into OAuth. Token exchange isn't a bad thing but probably a requirement.

Alan: one of the issues of Kerberos is the administrative problem can be burdensom, so many enterprises revert back to simple NTLM

Chuck: OAuth takes it to another extreme by forcing responsibility back on the user.

Chuck: is there a good summary about why cross-domain kerberos isn't working?

Vmware: Sharepoint seems to be the only usecase where it has been popular.

Alan: But it is still difficult to run internally.

Alan: I can't issue tokens for rights in mutually distrustful situations (e.g. DOD)

Alan: I'm not against either, but I'd like to make sure OAuth learns from some of the failrues of kerberos.

vmware: we want to move away from on-premise STSs because of the binding to AD. Can we move them to the cloud.

Prateek: OpenId and SAML have been responding to this issue of loose-coupling. OAuthv10 does some of this, but it is still too lightweight on security. But it will be difficult because security impacts rigidity and loose coupling.

Pamela Dingle: Many won't be willing to go through 400 pages of specs, we have to get the knowledgable people to participate in the generation of the OAuth spec.

Prateek: maybe we need to have a group of enterprise folks go off and isolate the key use cases and possibly develop some code.

SAML and OAuth, Lead By Prateek Mishra

Observation:
1. The basic web client profile in oauth is basically the saml artifact profile
2. The security properties of OAuth seem to be very under specified. When I see another implementer of the draft spec, I wonder what have they done to secure the implementation because in SAML the attacks were difficult to get nailed down. Excepting the point that people probably won't want to be told what type of token to use.

Chuck the main problem is that some of the providers don't have the same security posture. There is a broad range of needs. Becuase they are running at very high scale and state replication can be a big issue.

Pam: this sounds like a profiling exercise to identify multiple profiles for different types of requirements.

Chuck: as a practical point we should set up a working group to work on enterprise security issues.

OpenID Connect Session Management (W1I)

Convener: Breno de Medeiros
Notes-taker(s): Breno de Medeiros
URL: http://iiw.idcommons.net/OpenID_Connect_Sessn_Mgmt

Tags for the session - technology discussed/ideas considered:

OpenID Connect Session Management

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

−Discussed the authorization flow for OpenIDConnect
−Discussed the non-crypto authentication mechanism based on UserInfo endpoint
−Discussed the crypto-based authentication relying on signed JSON tokens
−Discussed the session management lifecycle by extending the lifetime of tokens or invalidating them

Topics for further discussion:

−Invalidation and Revalidation of tokens: If and How the Client should signal which session to extend/validate to the Server
−Validity duration of encapsulated Oauth token for API access to APIs other than the UserInfo endpoint
−More detail about how specific Oauth authorization profiles (e.g., User Agent vs. WebServer flow) operate
−Error responses
−Immediate vs. user-interactive modes

Session 2

PDE Why Would Anyone Adopt (W2A)

Convener: Randy Farmer
Notes-taker(s):
URL: http://iiw.idcommons.net/PDE-_Why_would_anyone_adopt%3F

Tags for the session - technology discussed/ideas considered:

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

Prevent Session Jacking (W2B)

Convener: Sam Curren
Notes-taker(s): Sam Curren
URL: http://iiw.idcommons.net/Fix_Session_Mgmt_Jacking

Tags for the session - technology discussed/ideas considered:

>   Session Jacking, firesheep, ssl

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

There is a need to prevent session jacking (firesheep) without requiring SSL for all content. We gathered ideas for a solution that would require slight modifications to both Browsers and Servers.

The Goal: Prevent reuse of hijacked session bearer token for a new attacker chosen request.

This is only to prevent session jacking, not man-in-the-middle attacks for any of the other network related attacks.

Key Ideas:
Leave session cookie/bearer token as-is
Establish a key during initial SSL authentication session.
Add a keyed-hash for the request, and transmit alongside session cookie.
Server checks keyed-hash, validates from original user.

We think the changes to Browsers and Sites would be minimal, following the establishment and verification of a spec.

Key individuals that will be contacted: Colin Jackson, Adam Barth, Ben Laurie.

UMA 201 (W2D)

Convener: Eve Maler & Maciej M.
Notes-taker(s): Maciej
URL: http://iiw.idcommons.net/UMA_201_Q_and_A

Tags for the session - technology discussed/ideas considered:

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

Thanks to Maciej for capturing these! Here are some relevant links that could usefully be added:

Draft minutes of UMA group meeting held two days ago:
http://kantarainitiative.org/confluence/display/uma/UMA+F2F+2010-11-01

Summary of UMA specs and the specs they reference:
http://kantarainitiative.org/confluence/display/uma/Working+Drafts

Info on the Newcastle University SMART project:
http://smartjisc.wordpress.com/

The SMART implementation of OAuth, called "leeloo":
http://leeloo.smartam.net/

UMA group wiki:
http://kantarainitiative.org/confluence/display/uma/Home

UMA Q&A Session

Q) UMA - what is the current state of the protocol?
UMA is OAuth-based. Initially OAuth 1.0a, now OAuth 2.0. UMA is now at the point of reaching UMA 1.0 protocol. Newcastle University (SMART Project) has an implementation of the OAuth protocol and the UMA protocol. OAuth constitutes roughly around 50% of the entire UMA implementation.

OAuth terminology is different from UMA terminology.

OAuth: resource owner, authz server, resource server, client
UMA: authz user, authz manager, host, requester (+requesting party)

Q) UMA Interaction Perspective
The user would start with the resource - when a user would like to share a resource then would go to the resource, click on Share Resource and start associating a policy with that. At the AM, the user would have the option to see all registered applications, all registered resources, all the people that have access to some resources.

Q) How to understand the identifiers of requesting parties
UMA allows different identifiers to be used for defining requesting parties. For example, claims could be used to say "I'll share that resource with somebody who can prove to be bob@gmail.com". Another example is where a user would define a policy that says "I'll share this resource if you say "Hi" to me or if you become my friend on FB". Group management could be integrated with an authorization manager. (see portable contacts).

Q) Resoure/Scope Registration
At the host, the person's job is to say that a resource should be protected/shared. At the AM, the user's job is to say how this resource should be protected/shared (by defiing a policy for a resource)..

Q) AM <-> Host relationshiops
Basically, there is a one-to-many relationship - where multiple hosts would trust a single authorization manager (preferred and chosen by the authorizing user). The Host would ask the AM for the scopes/permssions for which a particular access token received from a requester is valid.

Q) Enterprise Use Cases for UMA
UMA 1.0 is focused on consumer proposition. We will see if there is a interest from the enterprises (e.g. including UMA's Authorization Manager within enteprise infrastructures). This would allow enterprises to have selective sharing.

Q) Integration for existing systems
Necessity to have standard and RESTful (well-known) APIs - because we cannot assume that parties of the UMA protocol will meet statically or will be introduced statically - there is a lot of dynamism and there is a necessity to allow easy integration between parties of the protocol. Standardisation of APIs is important.

Q) UMA Topology
In the basic setting, a user would have a single AM and a bunch of

hosts and a bunch of requesters. This AM would be used for all these nodes. In more advanced setting, for example within the enteprise, the employeer could ask for having an additional AM for the hosts that a user uses.

Q) Would that be possible to chain AMs together?
Yes. For example, the AM could provide an AM,Host and Requester interfaces. And other AMs could subscribe to the Requester interface of another AM.
If you have a lot of ACLs then it might be reallly viable to have these stored and evaluated in multiples AMs and not in a single AM.

Q) How does UMA fit into the current model on the Web?
UMA can be introduced to the current model incrementally. Resources stored at hosts can be private, public, or managed by UMA. AM would be a service and the Host may want to to provide an additional interface to actually use the AM's functionality for this "managed by UMA" part. Examples: every OAuth server, exposing data on the Web (e.b. Facebook Social Graph). The host needs to be able to support local access management while allowing selected resources to be shared using UMA..

OAUTH 2 Extensions (W2F)

Convener: Justin Richer & Marius Scurtescu
Notes-taker(s): Marius
URL: http://iiw.idcommons.net/OAuth2_Exts.

Tags for the session - technology discussed/ideas considered:

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

Hosts (and only participants): Justin Richer & Marius Scurtescu

We talked about several proposed OAuth 2 extensions that we worked on or we thought are important:
- Instance Information
- XML Encoding
- UX
- Unregistered Clients
- Native Clients
- Token Types

Instance Information and Unregistered Clients are somewhat related and we explored if they can be combined. In the end we decided that they are orthogonal and should stay as separate extensions.

For Unregistered Clients the proposal is to specify well known values to two existing parameters and add a required and two optional
parameters:
- client_id=anonymous
- client_secret=anonymous
- client_name - required
- client_description - optional
- client_icon - optional

We explored alternate ways to signal an unregistered client, specifically to omit the client_id and client_secret parameters from the request. The problem with this approach is that these two parameters are required by the core spec so generic libraries that are not aware of this extensions will have problems handling messages like these. Also, a potential benefit in providing these parameters with special values is that some code paths in the authz server implementation can stay agnostic to the client type (by hard coding a fake registration for anonymous/anonymous for example).

The only issue with special values is that a client id of "anonymous"

my collide with a legitimate registered client.
For Instance Information the two proposed new parameters looks fine:
- instance_name
- instance_description

For symmetry we should consider adding a instance_icon, maybe.

For Native Clients we discussed an extension that allows the client to specify that it
does not have a redirect URI, and that the authz server should provide a default one
in this case. The extension also specifies the that default page should add the
response to the <title> tag in a specific way so it shows up in the window title. This
allows clients to implement OS specific window title scraping.
- redirect_uri=oob
- <title>Success code=123&state=abc</title>

We also considered adding an optional parameter called "instructions"
through which the client can provide additional instructions to the end user.

The Token Types extension introduces three new optional request parameters, all are
hints from the client for the authz server. These allow the server to issue only the
tokens that the client really
needs:
- tokens=[access|refresh]
- expires_in - optional
- token_usage=single

tokens tells the authz server what tokens it needs. A web based client may not need a
refresh token, during refresh a client may want a new refresh token, when swapping
an authorization code a client may need only a refresh token.

expires_in allows the authz server to issue access tokens that expire sooner than the
default, this allows lowering the load on the server if some clients are asking for a
large number of tokens in short periods of time.

token_usage allows clients to ask for access tokens that are single use. This allows
reducing load, as before, or reduce the risk if tokens are sent over insecure channels
(think One Time Password). We also considered this parameter to take a number as
value, instead of "single", and this number to represent the number of uses allowed
for the access token, in this case 1 == single.

We noted that expires_in and token_usage can be approximated by using token
revocation endpoint.

XML Encoding should rely on an automatic mapping between the JSON format and the
XML format. We considered generalizing this extension and also allow for form
encoded responses. One possible issue with form encoded is that it allows only name/

value pairs, whereas JSON and XML allow for tree structures. For now all responses are name/value pairs, and maybe it should stay like that, to be similar to requests and in browser responses.

Marius
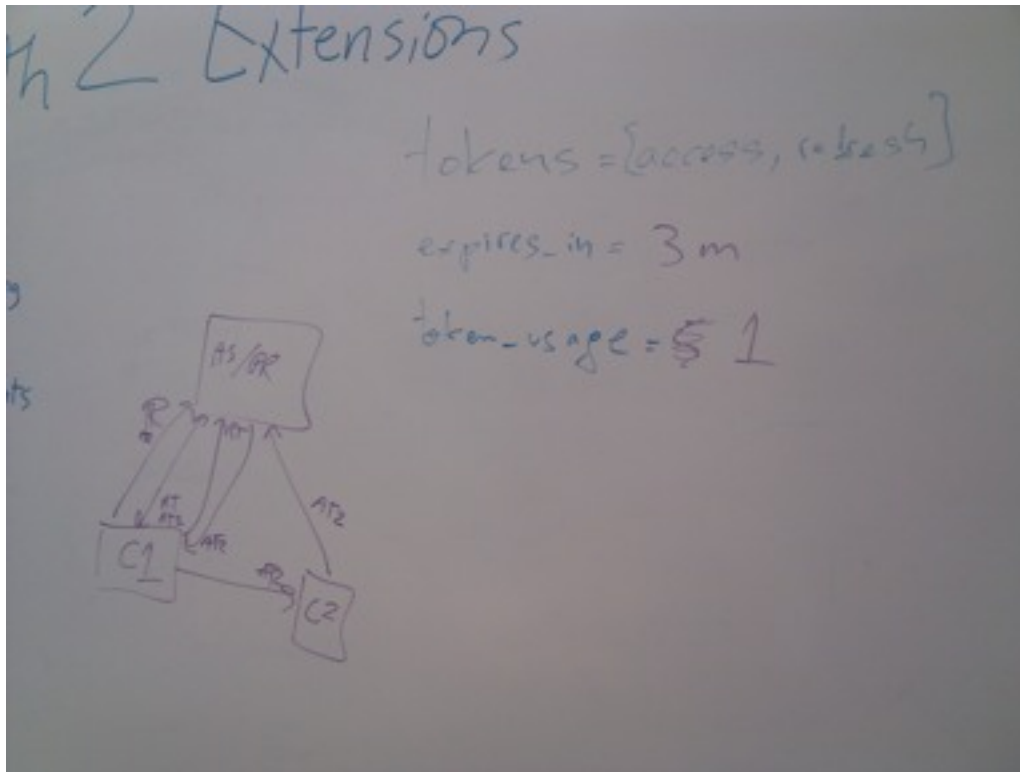
Native Client Extension

An OAuth 2 extension that helps native clients close the loop after the approval page. The extension defines a special value for the redirect URI for the case when the client does not have such a URI and it also defines that the authorization server should provide a default redirect URI for this case and how to format the result on the page generated a this URI.

If a native client does not have a redirect URI then the client can specify the special value `oob` for that parameter.

`redirect_uri=oob` signals to the authorization server that it should use a default redirect URI to show the final result.

In this case the authorization server cannot redirect any kind of messages back to the client, not even error responses.

The default redirect URI should show the authorization code (`code`) and instruct the user to copy to native application.

The default redirect URI should also show both the authorization code (`code`) and the passed through client state (`state`) in the page title, the two parameters should be form-encoded and appear space separated at the end of the normal title

Example page title: <title>Success code=123456&state=qwerty</title>

Browsers will truncate the title at some browser and OS dependent length. Ideally the whole title should be shorter than 100 characters. The Authorization Server should use a short title prefix and it should make the authorization codes as short as possible. Native clients should try to pass very short state strings and only of really needed.

If the authorization server also supports the Unregistered Client extension it should use the client provided name (`client_name`) in the default redirect URI page.

If the user denies, or there are other errors, the default page should similarly display the error code and also put the error message in the title: <title>Denied error=access_denied&state=qwerty</title>

References: ●   Section 6.3.3.2 of draft-hardt-oauth-wrap-01

Additional Parameter

An additional request parameter could be defined that allows the native application to specify wording to be added to the default redirect URI page. This could provide more specific instructions for end users on how to close the loop with the native app.

● `instructions`-optionalrequestparameter

Unregistered Client Extension

An OAuth 2 extension to support unregistered clients.

The extension defines special values for two existing clients and it defines an extra parameter: ● `client_id`=anonymous-existingparameter,definingspecialvaluethatsignalsan

unregistered client ● `client_secret`=anonymous-existingparameter,definingspecialvalue ● `client_name`$_1$ - required, new parameter that allows the client to self assert a client name to be displayed on the approval page

Alternatives No Client Secret

Instead of requiring `client_secret=anonymous` the extension could state that unregistered clients should not send a client secret at all.

More Parameters To Describe The Client

Several other parameters could be defined to describe the client and to help with authorization page rendering:

● `client_description` ● `client_icon`

[1]Equivalent to `xoauth_display_name`

Poor Man's Identity Verification (W2G)

Convener: Jon Webb
Notes-taker(s): Jon Webb, Dan Miller
URL: http://iiw.idcommons.net/Poor_Man_Verified_ID

Tags for the session - technology discussed/ideas considered:

Verified Identity, anonymity, delegated authority

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

Brainstorm format:
What do people want to verify?
- Confirm address
- Employment verification
- Job role verification
- Jon Webb Sony Playstation wants verification that the user is who they claim to be and that it hasn't changed since the last time seen (Playstation has 50mm+ users)

How to prevent account sharing that degrades quality of service for the network and other users?
Q: did people consider delegated authorities?
à People have less need to share account information since they can delegate use appropriately
e.g. edit timesheets on another's behalf, manage parental consent for minors, allow trusted users to conduct banking activities

Noted that systems to implement delegated authority have really only been deployed in the enterprise space, not much in the consumer space. UX in consumer space is a concern.

Pat From Equifax. Studying parental consent issue. Verifying 1.5mm users per day. Community filtering of sex offenders is common.

Allan from HP presented an interesting approach at last year's IIW that had to do with provisioning with an unguessable URL

Need to keep it low friction.

You could put additional challenge response cycle

Pat: You need very little info to verify ID. But it depends on the problem you're trying to solve, what kind of data and what do you need to verify, it comes down to what's the business case

Verification generally happens out of band

Password maps are hard to transfer between users. They are a personalized image where elements of the image are the password

Multifactor to avoid

How to assert ID without promoting a way for them to share the id

Discussed credit cards as an imperfect form of identity

International Presence of OpenID (Strategy Session) (W2H)

Convener: Henrik, Sha-Mayn The, Nat Sakimura
Notes-taker(s): =Nat
URL: http://iiw.idcommons.net/Int%27l_Presence_of_OpenID

Tags for the session - technology discussed/ideas considered:

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

Goal is to discuss the state of OpenID in Europe and Asia and brainstorm strategy of pushing OpenId in the region.

Note from OpenID foundation director: join the foundation and vote so that OpenID can do something for your region.

Background of the EU situation:
Nov 1 German eID
July 1 Denmark OCES II
(2008) Belgian
2011 Poland
2010/9 wp.pl becomes OpenID provider (largest portal in poland)

Denmark
Banking - 2 factor login: user/password/number on the card (150 numbers at a time)
- tax office is an IDP
- private identity vs government identity

Germany
- state-sponsored identity poofing
- privatized postal service also does manual identity verification
- Microsoft working closely with German govt as a testbed

In Europe, notion of level of assurance is not well known.
Holland has trust framework with 3-4 IDPs and brokers
Certified providers not necessarily state-owned
Belgium is an exception where government provides credentials

For China
- state already knows who you are?
- mainly social networks enabling federated login e.g. tencent (qq), renren. also e-commerce: taobao (IDP), 360buy.com (RP)
- telcos interested but haven't found the business value

- a general strategy is to implement OpenID in open source products (most Chinese sites use open source)
- but need more big IDPs to get big sites interested in becoming RPs. Action item: get AOL, Yahoo, Google etc to write a white paper of why/how it's good to be an IDP

Japan
- trust framework - Japanese govt just recently published public docs about the need for a trust framework
- IDPs: docomo/kddi
- identity proofing by private companies e.g. Yahoo Auctions does door-to-door identity verification.

OAuth for Installed Applications (W2I)

Convener: Dirk Balfanz
Notes-taker(s): Dirk Balfanz
URL: http://iiw.idcommons.net/OAuth_for_Installed_Apps

Tags for the session - technology discussed/ideas considered:

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

Dirk talked through some lessons Google learned from trying to ship installed applications that use OAuth.

- The installed application SHOULD launch an external browser (as opposed to using a WebView) when taking the user through the OAuth dance. It's more likely that the user is logged in already, and has other benefits. Some exceptions to the rule include iPhone O/S and other edge use cases.

- One trick Google found to work across several platforms was for the Service Provider to redirect, after user approval, to a page that puts the OAuth verifier in the title of the HTML document, thus making it show up in the browser application's window's title bar, where it could be picked up by the installed application (thus eliminating the need for manual copy-and-paste by the user).

- Google recommends that developers NOT embed consumer secrets in installed applications. The Service Provider can suppress the scary warning message that usually appears on the user approval page as a result of the Consumer being anonymous _if_ the Consumer chooses a token delivery method that prevents the token from leaking to other web apps. Once such delivery method is to specify the "oob" callback URL.

- In some use cases, the user consent page can be suppressed altogether - in particular if the installed app can "help itself" to OAuth tokens in a secure way. One way that Google is doing this is by providing an endpoint that sets an OAuth token as a cookie (without requiring user approval). Installed applications can read the cookie either by intercepting the HTTP response, or by reaching into the browser's cookie jar. Web applications do not have access to this cookie/OAuth token.

- On certain platforms (such as Android), the device stores the user's credentials, and applications can therefore skip the user authentication step (don't need to ask the user for their username/password). Instead, the app simply asks the O/S to deliver an OAuth token to it, and the O/S does so (after obtaining user consent).

Session 3

VERIFIED IDENTITY CLAIMS – Selectors (W3A)

Convener: Craig Wittenberg (Microsoft)
Notes-taker(s): Ariel Gordon (Microsoft)
URL: http://iiw.idcommons.net/VERIFIED_IDENTITY_CLAIMS_%E2%80%93_Selectors_(W3A)

Tags for the session - technology discussed/ideas considered:
Identity Selectors; Verified Claims; Identity Attributes; Privacy; Privacy Enhancing Technology; User-control.

Participants

Craig Wittenberg	Microsoft
Ariel Gordon	Microsoft
Pat Mangiacotti	Equifax
Mary Ruddy	Meristic
Brian Kissel	Janrain
Greg Hauw	Ohanae
Brad Hill	ISEC Partners
Dale Olds	Novell
Pamela Dingle	Ping Identity
Van Miranda	Socialcast
Diana Smeltas	Google
Naveen Agarwal	Yahoo
Eric Sachs	Google
Paul Trevithick	Azigo
Dave Hebert	Microsoft
George Fletcher	AOL
Lloyd Burch	Novell
Greg Turner	Sierra Systems
Michael Fischer	Stanford
Jeff Hodges	PayPal
Eve Maler	PayPal

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

Verified Identity Claims – How to implement identity/claims selectors

Scoping to the scenarios where privacy requirements mandate a "separation" between claim provider and relying party, e.g. non traceability.
Framing from the perspective of verified claims—adds some requirements. However, the model can be used for any type of claims (verified or self-asserted).
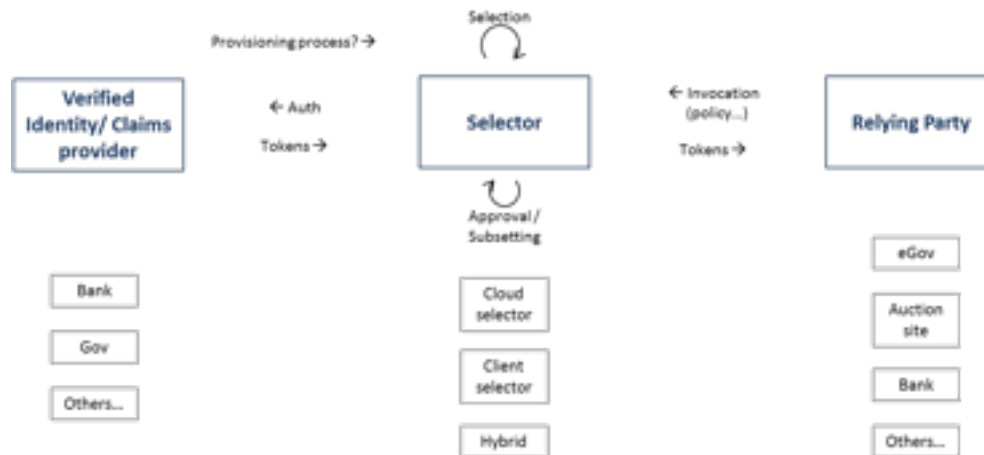
Problems: where should the Selector run?
- If the selector runs on the client, we need to update/manage its lifecycle, enable portability/roaming, etc.
- If the selector runs in the cloud, then one of the major question is who has the keys? (with U-prove tokens, the agent is storing the keys). In this case, the cloud service has the keys and could potentially impersonate the user.

There are many potential UX problems…

We should separate the Login problem from the Exchange of verified claims problem.
Does the user need to authenticate to the cloud-based selector?

Potentially, the user may need to authenticate N+1 times (once to the selector and N times for the N claim sources)…

Paul Trevithick (Azigo): Having the Selector remember my passwords to IdPs/Claims provider is a bad design.
Long-live tokens can address part of the problem because the selector could retrieve a bunch of tokens from the Claims provider to spend later—and not have to save the credentials.

George Fletcher (AOL): the Cloud Selector will now more about what the user is doing than the IdPs and the RPs.
That's true— but if it's operated as a different party from the IdP and is under the user's control, this is already better than the current IdP-centric model.
However, it is true that the cloud selector becomes the center of this relationship knowledge, and this is clearly one of the downside of implementing the selector as a cloud service.
Implementing as a device local service would mitigate that. There might be other, "hybrid" options with limited functions that run on the client.

Pamela Dingle (Ping): think of this as a **User-centric Attribute Broker** (instead of a selector/ agent).
The authentication methods are left to the service providers (outsourced).

Elements that will influence the design process:
- Multiple tokens
- Login to IdP vs. long live tokens; extra auth?
- User preferences
- Nascar
- What drives discovery? Should there be a way to provision the relationship with IdPs/ claims providers to the selector?

Eve Maler (PayPal): Standardizing claims type (building a dictionary?) and referencing valuable claim sources?

Goal: valuable claims need to be available for everyone. Possibly offered my multiple providers.

Paul: This may be the reinvention of user-centric identity and links naturally to the Personal Data Store discussion.
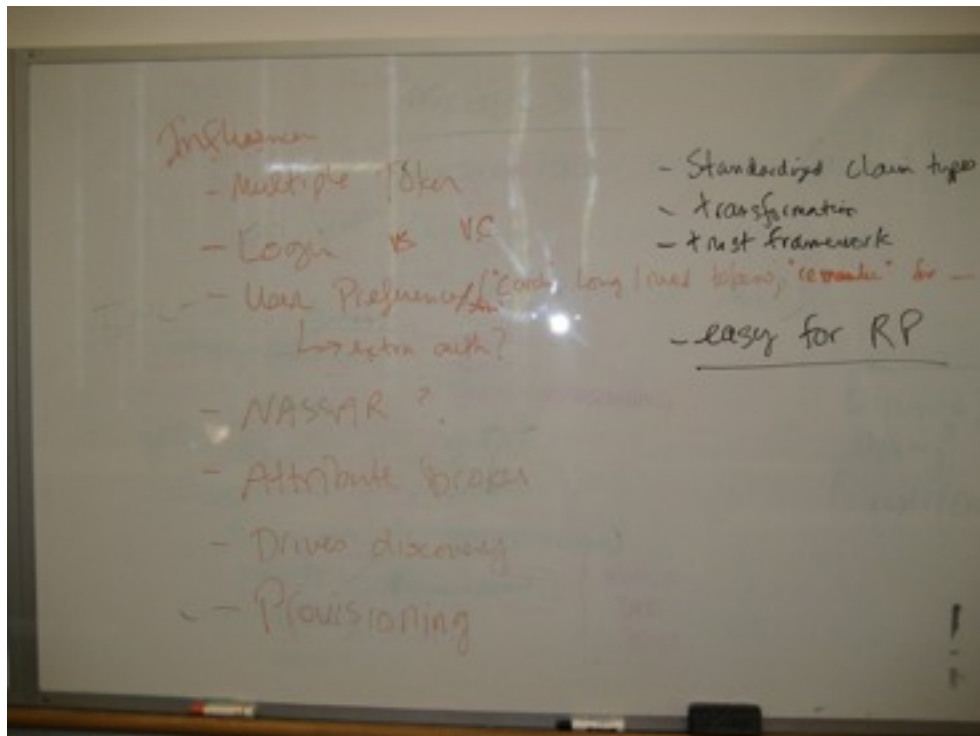
OAUTH 2 for Devices (W3E)

Convener: Marius Scurtexcu
Notes-taker(s): Andrew Wansley
URL: http://iiw.idcommons.net/OAuth2_for_Devices

Tags for the session - technology discussed/ideas considered:

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

What is a device

A device as we're concerned with it here has a display and a limited or painful input. We're explicitly not talking about headless devices, devices with no display and or no input like a refrigerator. These devices as far as we know just run a webserver locally and do the webserver profile.

What's the flow

From the user's perspective, the device displays a URL and code. User goes to URL and enters the code. The device magically works.

From the device's perspective, the device presents AuthZ server with a clientID and gets back a URL a user code which it displays to the user and a device code used for polling. The device then starts polling the AuthZ server which tells it "not yet" for a while then eventually returns yes and a token or no.

AuthZ server has preregistered a device and replies to the device's requests as described above.

The session fixation attack

Trick the user into approving it from a link. Somewhat of a weakness but not a huge threat.

Other sorts of connections

I've already paired my Playstation with my Sony acct. It would be nice if when I add a netflix app it could just pair with Sony's frontend and then that connection could live across devices. In this case we could just do a webserver flow.

Another way to authorize devices is to do bluetooth sharing of credentials. Like I can authorize my photoframe by connecting my android.

c:Client

s:Authz Server

b:User Agent

response_type=device_code*
client_id*
scope

authorization request
{HTTPS, POST,
device endpoint}

device_code*
user_code*
verification_uri*
expires_in
interval

{200, JSON}

instruct end-user
{display}

user_code*
verification_uri*

access token request
{HTTPS, POST,
token endpoint}

grant_type=device_code*
client_id*
device_code*
scope

error
{200, JSON}

error=authorization_pending*

{GET, verification_uri}

authenticate, ask for code, request confirmation

access token request
{HTTPS, POST,
token endpoint}

confirm
{user_code}

access_token*
expires_in
refresh_token
scope

success
{200, JSON}

Building a CAKE Detector (W3G)

Convener: =Joe
Notes-taker(s):
URL: http://iiw.idcommons.net/Building_a_CAKE_Detector

Tags for the session - technology discussed/ideas considered:

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

Shifting the Global Economy Using Identity (W3H)

Convener: Ace Swerling
Notes-taker(s): Didier Perrot (sent in email by Ace)
URL: http://iiw.idcommons.net/Shifting_Global_Economy_w-Identity

Tags for the session - technology discussed/ideas considered:

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

Issues common to large organizations – objectives to reduce costs (IT) and add revenues

Challenge of connecting the IT systems, e.g. cross-organizations, -boundaries, … : among other technical

3rd wave : information based economy (Allan Toffler) – shift in ways of creating wealth

Scenarios : in the supply chain, in the organization … reduce friction

How to do it ??

Fragmentation about representation of identity

Issues of reconciling various sources of identity

Top down vs. bottom up

« Where's the guidance from the (IT) industry »

Chicken & Egg issue
Jumpstarters

Gov. Leadership ?
Private sector ? Financial sector, IT sector …

DNS or Peer2Peer

Easier in developing markets ? (infrastructure white space …)
« System » : technology issues but trust comes from duties
Security as an enabling technology

Open ID ABC – Artifact Binding Working Session (W3I)

Convener:
Notes-taker(s):
URL: http://iiw.idcommons.net/OpenID_ABC_Artifact_Binding

Tags for the session - technology discussed/ideas considered:

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

Session 4

Personal Data Business Models (W4A)

Convener: Kaliya Hamlin
Notes-taker(s): Barbara Bowen
URL: http://iiw.idcommons.net/Personal_Data_Ecosystem_Biz_Models

Tags for the session - technology discussed/ideas considered:

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

Specific case: search

Value Statement: The people who want to create your data and may now aggregate it are aware that our search history over time is more valuable in combination with patterns of behavior. As users we have the option to extend sharing terms beyond the existing terms of service and storage for our own opportunities and goal.

Key Points:

- Lower prices and loyalty programs may incentivize participation.

- The card model could be universal, and trade an aggregate of total data.

- Loyalty cards often do not provide real benefits, frequent flyer models are a better metaphor.

- Application developer may not want to store data, a pds will allow for storage. Cost and risk to developer is reduced. Features may be stored, it gives developers an option.

- VRM and CRM opt in and sharing

- Data by and about each individual brings up the question of joint data ownership of data as in an address book.

- When the system becomes complicated there are issues that bring up more possibility

- Marc illustrates exchange model: with PDS stack. Logical and physical layers are not necessarily contained in a box. Optimization and efficiency are key to adoption.

- Terms of use on the data and ownership rights create friction in sharing.

- 4th party with multiple exchanges. A fourth party can utilize bids. As the sole owner of a data cache users leverage value.

- Verticals will exist in areas that we have not conceived of yet.

- Trusted intermediary with demand fullfillment.

Starbucks is pointed out as a use case in the foursquare offering.

Credit score, reputation, and social currency. Personalization based on data that is not already aggregated. Risk assessment.

- Data validity and authentication are going to be part of the ecosystem

- What is the incentive for the PDS to keep the data portable and build a monetary incentive for service providers.

- A larger cross referenced data set will have value to those who only have access to small data sets.

- Self hosting business model, hosting options with any number of optimization and monetization possibilities.

Anonymized data for exchanges are reflected in the banking model vs a data vault.

Follow up session to follow and expand on pdf use cases and business markets..

Hand Written Notes from Kaliya:

Do we really listen
We think it is logically appropriate
People who make market are not here
Support problem set

"tricking users" - no one joined FB to do web SSO

What is user experience? additional features and functionality
Features and Benifits - what has internet done for me lately.

Give people something valuable include PDS as well

Expose benifirts of PDE people and organizations

Gradually get there
Data in US is free-for-all
give info ---> you get

what do people find valuable - groupon

Marc - driving forces human needs
- Connect
- Feel safe
- Get Recogintion

all from people you trust

Are we solving a problem that doesn't need to be solved?

Groupon "saving money" - we have the worst unemployment in a long time
Benifits them - home safe enough to eat. this feeling people don't have on the web.
Control Self Sufficency

Mobile what is transformative experience
Sarah - Back up your data (Moze & Carbonite)
Make it happen

Sam - look at additional benifits
Solve problems that there are no solutions for yet (without making the existing suboptimal)

Ability build special APIs social data - where is it now

Monica - Things I wouldn't share with everyone. Woman walking home alone at night can share geolocation with spouse at home.
Tracking spending and directing dollars
Only comfortable with self and close people sharing.

Dave msft
Antique Road show - what is it worth

Wendell - all of this is happening
- All big online systems, all events, monetize and change experience
- Compensated
- Better user experience

Asside comment about how to make a lot of money - do a Small industry trade association press - 1,000 of dollars

There are two kinds of stuff people have
1. is that they consciously articulate this is done today with an interest managers
2. the trails that you travel.

These are set up to target adds against
See the semantics of all this

Jay - additional added power of the equals sign

IdM place holder if we add something to it - (IdM + N) * user adoption = ROI

Save money - social event -> participate in & share/relate

Online -> offline

1-2 reports a quarter - on how soup for example was selling on the shelves.
When scanners came in you could get a daily report because the scanners were ubiquitous

Who are these people actually walking into the store?
can we find out in a privacy appropriate way? can we track "conversions" search -> purchase.

if we do this the wrong way we live in a police state.

Google/MSFT health vault -> Start storing other stuff?

Adam Larson - person in the middle and integrate
One company and technology?
Thing - phone, browser "on top of" Phone operating system

Smarter purchasing process

conversation between me and vendor
what my friends bought
Friends and social groups.

Brett.
We are not eyeballs - Holo go through consumer
Behavior me -> yahoo! this data is better then

My Wallet with my permission
Ghostery - sends beacons bugs
Right now there are funnel Advertising

Beacon site - triangle current aggregated raised in quality

Behavior physical world stuff in wallet.

Using A Personal Data Store (W4G)

Convener: Phil Windley
Notes-taker(s): Phil Windley
URL: http://iiw.idcommons.net/Using_a_Personal_Data_Store

Tags for the session - technology discussed/ideas considered:

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:
To read the complete blog post with content that this session is based on go here: :http://

www.windley.com/archives/2010/10/kynetx_and_personal_data_services_project_neck_pain.shtml

One of the technologies that seems to be picking up steam lately is the PDS or personal data service. The PDS goes by other names as well. David Siegel calls it a "personal data locker" in his book Pull. Drummond Reed has determined the right name is personal data service rather than "store." I talked about the problem with the name and enumerated some principles for personal data services after IIW DC. I'm certain that the PDS will be a significant topic of conversation at the upcoming Internet Identity Workshop XI in Mountain View, CA (register here).

Why all the fuss? I believe it's because the PDS is the centerpiece in a new kind of Internet; one where the individual sees significant increased utility from the use of their personal data in their behalf instead of having it used against them. At the same time, the PDS offers increased privacy over the current regime.

That said, I think a PDS might be more of a pain than a help if a PDS doesn't come with accompanying automation. If it's just one more thing to manage, then I don't need it. On the other hand, if the PDS helps me by making mundane tasks less onerous and focuses my attention on the decisions that I really must make, then it's a win.

Of course, if you've been following along, you've probably already guessed that I'm thinking the Kynetx Rule Language, or KRL, is the perfect way to automate PDS tasks.

So, without further ado, here's a five minute video that shows a conceptual demonstration of how a PDS and KRL can work together. This conceptual demo illustrates the opportunities that are available for automating the contextual activities that people undertake every day. At the heart of the demo is a personal data store and Kynetx. The interactions are all done using real Kynetx applications that are plumbed in a realistic manner. The scenario uses 5 different APIs and a dozen individual rulesets in the Kynetx system. In the scenario, Scott Phillips gets bad news from his radiologist: he needs surgery. You'll see that a personal data store and a collection of loosely coupled Kynetx apps automate the frustratingly disjointed activities associated with Scott's bad news and focused his attention so he can complete the tasks with the least amount of effort. **Go to link above to see video**

Project Neck Pain

I commissioned this demo in mid August in preparation for [Doc Searls'](#) [VRM+CRM workshop on August 25, 2010](#). We called if **Project Neck Pain** (PNP) and it involved much of the company. The goals were

1. Create a compelling demo of what Kynetx could to to make a PDS useful and worthwhile

2. Produce a large application comprising multiple cooperating rulesets

3. Find out where the Kynetx Network Service lacked features in support of goals (1) and (2)

I couldn't have been happier with the result as it achieve all three goals. The video is proof of (1). I'll talk about (2) below. We extended and polished the platform in some significant ways in support of (3). My recent post on [building event intermediaries](#) is one small piece of that.

In what follows, I'll describe the various pieces that went into PNP.

Endpoints

To understand what happened behind the scenes in this video, you need to understand a little of the architecture of Kynetx. In the Kynetx Network Service, or KNS, active clients, called "endpoints," raise events. Rules inside the Kynetx Rules Engine respond to those events to cause an action. When an event is raised one or more rulesets might respond to that event on the user's behalf. In the case of the demo, there were four different endpoints involved:

- a web endpoint in the form of a browser extension,

- an email endpoint that uses IMAP to watch a mailbox,

- a telephony endpoint that uses [Twilio](#) to make phone calls and respond to user input, and

- the PDS itself.

The idea that a personal data service be not simply a repository of personal data, but an active participant in coordinating activities in behalf of the user is a key piece of the Kynetx vision for how personal data will transform what we think the Internet is

and how it works. In the demo, the PDS is a key actor that not only responds to API requests, but also raises events.

As outlined in our free white paper: [The Kynetx Rule Language - The First Internet Application Platform](#) (PDF), there is a vital link between events raised by endpoints and rules. For example, the following rule fires off the phone confirmation when the PDS signals that the appointment has been chosen:

```
rule start_confirm is active {
  select when kpds update_event key "chosenappt"
        or kpds create_event key "chosenappt"
  pre {
    phoneNum = (datasource:pds({"key":"phone"}))
                    .pick("$.value.number");
    appt = datasource:pds({"key":"chosenappt"})
                    .pick("$.value");
    confirmed = appt.pick("$.confirmed");
  }
  if((confirmed neq "") && (confirmed == 0)) then {
    http:post("https://secrets:here@api.twilio.com/Calls.json")
     with params =
      {"Called":phoneNum,"Caller":"8018954878",
        "Url":"http://webhooks.kynetx.com/h/a8x54/outboundcnct"};
    send_directive("log") with
      app = "PhoneConfirm" and
      desc = "Confirmation Call Started";
  }
}
```

This rule is selected when the PDS signals that the appointment has been chosen. Note that there are two different ways that might happen and the select statement takes both into account. It gets Scott Phillips' phone number, the appointment data, and doctor information from the PDS in the rule prelude (pre) and then initiates the phone call with Twilio using an HTTP POST if specific conditions are met. One key feature of the event model is that the PDS doesn't have any idea what will happen when it signals that the appointment is set. The PDS simply raises the event. What happens depends on what apps the user has installed and what rules are in those apps.

APIs

In addition to the various endpoints involved in the demo, it also uses multiple APIs, including the follow:

- **PDS** - the PDS has an API as you can see in the preceding rule. Not only does the PDS allow data to be queried in a permissioned way (right now using OAuth), but it also allows values to be updated or created. At present our prototype PDS doesn't have a generalized schema beyond what is needed for this demo.

- **Twilio** - as already noted above, the Twilio API is used to make phone calls and gather responses from the user.

- **Google Calendar** - we are readying Scott Phillips' schedule from his Google calendar using their API.

- **Flickr** - the pictures painted on Scott Phillips' dashboard are coming from his FLickr account via the API.

- **Weather** - the weather data is coming from the Yahoo! weather API

The ability to freely use APIs makes the demo very powerful because of the data that can be pulled in. If the demo were real, there would likely be a dozen more APIs that would be useful in helping choose a doctor and schedule an appointment.

Rulesets

Our vision entails multiple coordinating rulesets cooperating in a loosely coupled manner to help the user. Events allow the system to be loosely coupled because, as mentioned above, the raiser of an event does not know who may be listening or what action might be taken because an event is raised. Multiple rulesets may be listening to and event without being aware of each other.

Our goal in creating the demo was to create apps that we thought might actually exist. We wanted apps that had a good backstory, even if they were demo apps. I'll describe the primary rulesets in this demo and how we envision they may really exist.

- **Dashboard** - the dashboard in the demo is painted by a ruleset. There's no real web page to speak of. Just a blank page with a few divs for structure. Everything on it from the banner, to the weather and time, are painted on the page by a Kynetx ruleset. This app might be provided by the PDS manufacturer.

- **TODO List** - the TODO list and its management are a separate app that might be provided by the PDS manufacturer or be a standalone component that the user installs according to their own preference.

- **PDS Activity Stream** - again this is a standard component for the PDS that shows detailed logging data

- **Flickr** - reads the Flickr feed of the user and shows pictures. This might come with the dashboard or be something the user has found and installed to work with the dashboard.

- **Healthcare Action Items** - watches the user's email for messages from the health care provider and adds relevant TODO items to the TODO list in the PDS. You can imagine that the radiologist is using a patient management system (PMS) to communicate with the user and has provided a PDS app to the user that is watching specifically for messages from the PMS. The app might be doing other things as well such as proactively reminding users of medical alerts, looking for appointment reminders, and so on. In the demo, we just looked for text patterns, but RDFa or microformats in a HTML message would provide more opportunity to grab meaningful, structured data from the email.

- **Doctor Choices** - responds to the TODO item about choosing a surgeon by showing the user some choices and annotating the doctors who are in the user's insurance network. This app might come from the user's health care network or an independent provider.

- **Select Doctor** - overlays the doctor's professional "about" pages with relevant data, augmenting what's there with recommendations from the user's social network, showing data from other Web sites, and any relevant ratings and reviews. In our scenario, we've imagined this app came from [Angie's List](#) or a similar service provider ranking site.

- **Set Appointment** - compares the user's calendar (Google in this case) with the doctor's free-busy schedule so find the intersection and display three choices for the appointment. The app also sets the appointment in the user's calendar and transmits it to the doctor. Currently we know of no standard way to discover calendar data for a service provider. Such a capability would be critical to an app like this working seamlessly.

- **Phone Confirmation** - called the user with relevant appointment data and asked for confirmation. Note that this app was calling on behalf of the personal data store. This app might be part of the appointment scheduling system or a more general "confirmation" app that the user has installed to confirm certain changes to PDS data using a secondary channel.

- **Medical Information Transfer** - responds to requests from medical providers for information from the PDS. This might be specific medical information or part of a more general information request system that requests and records the user's authorizations and data transfer preferences.

- **Global Configuration** - while it wasn't part of the demo that you saw, there's also a separate app that is used to configure the PDS and reset certain fields for demo purposes.

This set of eleven rulesets cooperate to deliver the experience that we saw in the demo. They are independently using the PDS and working with whatever APIs are relevant to their function. The PDS is the centerpiece of the demo since all the apps and functionality revolve around it. The individual rulesets know nothing of each other for the most part. They just do their piece and use events to message other components.

Events enable loose coupling, but they're not magic. While we've avoided it through design in this demo, loosely coupled apps may interfere with each other and give non deterministic performance in real life. For example, two apps may need to write the same field in the PDS. The PDS will need to incorporate appropriate data isolation techniques and, where ordering is important, apps will need to find ways to serialize themselves. Events can do this, but it's not automatic.

Life Events: Helping Users Achieve Purpose

Back in 2001, when we were envisioning how egovernment would work at the State of Utah, we came up with a concept called "life events." The idea was that most people interacted with government when something happened in their life that compelled them to. Further, those events almost never cleaved along departmental lines. A typical life event, like "moving to Utah" involved multiple interactions with many different government *and non-government* entities at all sorts of levels.

At the time, we envisioned that we'd build out tools on the Utah.gov portal that would help constituents walk through the various steps. The only one that ever got built out, as far as I know, is the one-stop business registration application. I've used it and it works surprisingly well. The reason that more didn't get built was that a server-side portal is just the wrong technology for coordinating all this.

One reason why a server is the wrong place to do this is that the server is missing all the help that active clients provide—specifically the ability to raise relevant events and respond to directives. As a consequence, the server has to simulate this by requiring the user to enter data, click buttons, and select things. That is, a server turns the user into the active client.

Another reason the server is wrong for this is that it's too tightly coupled. In a way, the whole Web services play was a complicated way of trying to create interactions between APIs on the server side. You could make this all work with Web services but it would be quite brittle. Of course, there are Web services technologies for creating more loosely coupled systems, but they're still working on the server away from the user.

In 2010, I think we're a lot closer to actually being able to help people with the tasks and activities that matter to them—their purpose for being online at any given time. The demo shown above is an example of this.

The answer isn't a big, one-size-fits-all, server-side, portal-based application, but a set of loosely-coupled, cooperating apps coordinating around a personal data service. The overall experience is infinitely customizable because any of the components can be traded out by the user. Further, the experience is incremental, meaning that I don't need all of the apps. I see incremental benefit as I incrementally install apps. The experience grows and changes as I customize my environment to suit my needs. What's more, changing out an app for another one doesn't require upgrading or changing the other apps.

Conclusion

There are several important ideas for me in Project Neck Pain that bear emphasis

- The experience focuses the user's attention on the things that matter, critical decisions, rather than making the user fuss with instigating every interaction and manage the details.

- There was no Web site involved in delivering this experiece except for a very simple Web page served with a few divs for structural purposes. Everything else was painted on the page using a Kynetx app.

- You can write event-driven applications that knit together multiple domains like Web, email, and phone. This is a powerful idea that is difficult without the concepts of an active client and events.

- Developers program loosely coupled applications that are event-driven. KNS with a PDS gives developers a very flexible platform for building all or just pieces of any given experience.

- KRL provides significant help in creating apps that use multiple APIs and interact using events. KRL was designed from the ground up with the idea of making writing such apps easier. Having a domain specific language adds significant mental leverage.

- You can build large applications in Kynetx using multiple cooperating rulesets. We've further tested this with another large app that we built for a customer in the last few weeks.

- A PDS without an accompanying automation system is going to be a pain in the neck. A PDS will be just one more huge, complicated thing to manage if it's not a participant in an app ecosystem.

- The demo shown in the video isn't really about health care, but rather, more abstractly, about picking a service provider and scheduling the service.

If any of this is interesting to you, I invite you to signup for a free Kynetx developer account and start playing around. We're happy to help—remotely or in person—and will gladly share the techniques and even the code we used to create this demo.

JSON Token Spec Work Encryption (W4E)

Convener: Mike Jones
Notes-taker(s): Mike Jones
URL: http://iiw.idcommons.net/JSON_Token_Spec_-_Encryption

Tags for the session – technology discussed/ideas considered:

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

We held a session on encryption for JSON Web Tokens at IIW (Wednesday after lunch in space E), building upon the results from the JSON Tokens and No Base String sessions on Tuesday. Once again, substantial consensus emerged, which is described in the notes below.

These consensus decisions were in place by the start of the session:
- Some use cases for JSON tokens require encryption
- (plus all the decisions from the sessions on Tuesday)

It was agreed that these sets of high-level goals need to be achievable by application of signing and/or encryption:
- Integrity
- Confidentiality + Integrity
- Non-Repudiation (which also implies Integrity)
- Non-Repudiation + Confidentiality

Open issues identified at the start of the session were:
- Should encryption and signing be accomplished via (1) separate but composable encryption and signing operations, (2) use of a small set of recommended composite operations that achieve the high-level goals, or (3) allowing for both possibilities?
- Data format and how data formats affect streaming operations
- Order of signing and encryption operations
- Compress before encrypt?
- What are we encrypting (payload or payload + signature)?

The primary consensus in the room was to **invent as little as possible by reusing work** that other experts have done in the space, while adapting their work to a JSON context. Participants provided the following references to work to borrow from:
- Cryptographic Message Syntax (CMS): http://tools.ietf.org/html/rfc5652

- Table of Algorithm Suites from WS-SecurityPolicy 1.2, section 6.1: http://docs.oasis-open.org/ws-sx/ws-securitypolicy/200702/ws-securitypolicy-1.2-spec-os.html#_Toc161826547
- XML Signature Syntax and Processing (Second Edition): http://www.w3.org/TR/xmldsig-core/
- XML Encryption Syntax and Processing: http://www.w3.org/TR/xmlenc-core/
- Defective Sign and Encrypt analysis: http://world.std.com/~dtd/sign_encrypt/sign_encrypt7.PDF
- The TLS Protocol Version 1.0: http://tools.ietf.org/html/rfc2246
- Transport Layer Security Protocol Compression Methods: http://tools.ietf.org/html/rfc3749
- Compressed Data Content Type for Cryptographic Message Syntax (CMS): http://tools.ietf.org/html/rfc3274
- DEFLATE Compressed Data Format Specification version 1.3: http://tools.ietf.org/html/rfc1951

Specific issues were resolved as follows:

- **Should encryption and signing be accomplished via (1) separate but composable encryption and signing operations, (2) use of a small set of recommended composite operations that achieve the high-level goals, or (3) allowing for both possibilities?**

The consensus was for (3) – that we should specify a small set of composite operations that will meet the needs of common use cases, while also enabling applications to compose encryption and signing operations in a general fashion, should the composite operations prove insufficient for their use cases. A subset of the composite algorithm suites in WS-SecurityPolicy 1.2 was suggested as an appropriate starting point. Paul Tarjan of Facebook had also suggested during the OpenID Summit on Monday that descriptive composite algorithm values be used, such as "AES-256-CBC HMAC-SHA-256".

- **Data format and how data formats affect streaming operations**

For the same reasons as discussed during the signing session, the group reaffirmed that the order of the fields should be envelope.payload.signature, with the envelope containing sufficient information to determine the nature of the contents of the remaining fields. This order enables streaming operations, where content is created or analyzed in parallel with its transmission or reception, to the maximum extent possible, and also potentially minimizes buffering requirements imposed upon implementations.

- **Order of signing and encryption operations**

It was recognized that no one-size-fits-all solution applies here and that different sets of operations are needed for different use cases. For instance, if non-repudiation is required, a signature of the plan text using public key cryptography must be present,

which therefore must precede any other operations. Again, the group reaffirmed that we should reuse other work in this area to the extent possible.

- **Compress before encrypt?**

Several participants pointed out existing practice in this area, including the use of the DEFLATE compression algorithm prior to encryption by TLS and CMS. It was agreed that we should similarly document how to optionally perform compression before encryption for those use cases where it makes sense.

- **What are we encrypting (payload or payload + signature)?**

This was another area were the participants felt that we should reuse existing practice that has already been vetted by experts.

Special thanks go to Breno de Medeiros, whose crypto expertise was invaluable during this session, as well as Brad Hill, Diana Smetters and several other Googlers, John Bradley, Nat Sakimura, Joseph Holsten, Thomas Hardjono, Terry Hayes, Dick Hardt, Tony Nadalin, and others who contributed to this productive session.

VERIFIED IDENTITY CLAIMS – *User Experience Challenges (W4H)*

Convener: Ariel Gordon (Microsoft)
Notes-taker(s): Ariel Gordon (Microsoft)
URL: http://iiw.idcommons.net/Verified_Identity_Claims_-_UX

Tags for the session - technology discussed/ideas considered:

Identity Selectors; Verified Claims; Identity Attributes; Privacy; Privacy Enhancing Technology; User-control.

Participants

Craig Wittenberg	Microsoft
Ariel Gordon	Microsoft
Mary Ruddy	Meristic
Henrik Biering	Peer Craft
Greg Turner	Sierra Systems
John Engler	Webroot
James Reffell	Webroot
Mike Min	Booz
Adam Dawes	Google
Charles Andacs	PBB
Phil Hunt	Oracle
Nishant Kaushik	Oracle
Mike Ozburn	Booz Allen
Tom Leon	AOL

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

Verified Identity Claims – UX (User Experience) challenges

Policy could be driven by the RP, the user/user's agent, or the Claims provider
UX gets even more complicated when we add N claim sources (orchestration scenarios)

How to mitigate UX complexity: add a "always consent" option on the agent
Friction when things went well: the user has to take many actions (and stop reading)
Friction when something goes wrong (error handling)

James Reffell (Webroot):
I have to go get data from 3 different, independent sources: present the UX as a ToDo list while keeping the RP's context in the background.
The UX could look like a ToDo list, showing the steps that the user has to complete before continuing:
Go get Claim 1 [go]
Go get Claim 2 [go]
Go get Claim 3 [go]

The user can do them in different order. Say he goes to do #1. Now the UX refreshes to:
Claim 1 R
Go get Claim 2 [go]
Go get Claim 3 [go]
-Or-
Claim 1 [!]did work/here's why... Go again
Go get Claim 2 [go]
Go get Claim 3 [go]

The RP will offer a list of potential claim providers
We'll need some sort of an auditable standard so that the RP can say "I'll accept claims from any source that's auditable at level X".

Authenticate to the Claim Provider:
- U/P
- KBA
- Using the phone as a second factor -- see Google's Strong Auth initiative with iPhones
- Anakam (recently purchased by Equifax)--phone approach rather than Equifax's traditional KBA
- Using a device-based Agent to participate in the authentication ceremony to the Claims provider, and simplify this for future use.

Installing an App on all of my device : painful. What about users without a smartphone?

Session 5

7 Deadly Sins of Distributed Authentication (W5A)

Convener: Brad Hill
Notes-taker(s): Brad Hill
URL: http://iiw.idcommons.net/Deadly_Sins_Distributed_Authentication

Tags for the session - technology discussed/ideas considered:

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

7 Deadly Sins of Identity and Authentication Systems The "OWASP Top 10" of what we do at IIW. IANAC High school calculus was my last math class

I am an engineer/nerd who understands the properties of some crypto primitives, and a little bit about how they combine and compose.

I've seen a lot of mistakes and read about even more. Focus on protocol / artifact flaws Not governance, policy, key management, ecosystem issues

These are universal and unavoidable challenges, not flaws Background Reading: Classics Prudent Engineering Practice for Cryptographic Protocols Abadi and Needham, 1995 Robustness Principles for Public Key Protocols Anderson and Needham, 1995 Programming Satan's Computer Anderson and Needham, 1995 Authentication in Distributed Systems: Theory and Practice Lampson, Abadi, Burrows and Wobbler, 1992

Background Reading: Post WWW Ten Risks of PKI: What You're not Being Told about Public Key Infrastructure Ellison and Schneier, 2000 Ceremony Design and Analysis Ellison, 2008 Defective Sign & Encrypt in S/MIME, �PKCS#7, MOSS, PEM, PGP, and XML Don Davis, 2001

Background Reading: �Higher notation tolerance necessary Using encryption for authentication in large networks of computers Needham and Schroeder, 1978 Trust Relationships in Secure Systems – A Distributed Authentication Perspective Yahalom, Klein and Beth, 1993 A taxonomy of Replay Attacks Syverson, 1994 Some New Attacks upon Security Protocols Lowe, 1996 Federated Identity-Management Protocols (Transcript of Discussion) Pfitzmann, 2005 Background Reading: Books Cryptography Engineering: Design Principles and Practical Applications Ferguson, Schneier and Kohno, 2010 Security Engineering: A Guide to Building Dependable Distributed Systems Anderson, 2008 Network Security: Private Communications in a Public World (2nd edition) Kaufman, Perlman and Speciner, 2002 More formal papers of special interest New Proofs for NMAC sand HMAC: Security without Collision-Resistance Bellare, 2006 On the Security of Joint Signature and Encryption An, Dodis and Rabin, 2002 Authenticated Encryption: Relations among notions and analysis of the generic

composition paradigm Bellare and Namprempre, 2007 The 7 Deadly Sins Unconstrained Delegation Unbound Composition of Transport and Message Security Un-Scoped or Over-Scoped Authority PKI, PKIX and SSL/TLS Dependencies Impedance Mismatch in Identity Contexts DoS and Confused Deputies in Revocation and Key Retrieval False Dilemmas in Adoption vs. Assurance 1. Unconstrained Delegation Failure of least privilege Username / Password Don't just replace it with a "token" with mostly equivalent properties. Specify a target set against which the credential is valid Delegate privileges or capabilities, not identities Identify and audit delegate as well as delegating principal Accommodate attributed re-delegation Prefer holder-of-key proof to bearer tokens

2: Unbound Composition of Transport and Message Security "Mixed-mode" or "Message Credential with Transport Security" Server Auth TLS + a client token

"While encryption guarantees confidentiality and authenticity, it also serves in binding together the parts of a message: receiving {X, Y}K is not always the same as receiving {X}K and {Y}K." - Abadi & Needham, '95 Forwarding attacks possible TLS validation is incorrect or absent Mismatched scope NTLM over HTTPS X.509 tokens without an AppliesTo Multiple server identities Kerberos SPN specified in WSDL Renegotiation attacks with client certs in TLS

Example Forwarding Attack:�WS-Security Kerberos Tokens over TLS Scoped to a particular server, negotiates key material, requires holder-of-key proof by client Still vulnerable…

Alice retrieves WSDL from Mallory Mallory's WSDL says her SPN is Bob Alice gets Kerberos ticket for Bob Alice verifies Mallory's TLS server cert, sends ticket with signature over a timestamp Mallory connects as a client to Bob, forwards ticket with signature and new message body Forwarding Attack Solutions Service Binding AppliesTo header – copy the TLS subject name here Use for both symmetric and symmetric credentials as per our Kerberos example AudienceRestriction Other indication in token of intended target Channel Binding Include a property of the outer channel as a signed attribute of the inner token ([RFC 5056](#)) 3: Un-Scoped or Over-Scoped Authority Not often a problem in Internet-scale systems PKIX is the BIG exception. Global CAs have terrible name-collision properties. Certs for non-unique names, IP addresses, etc. Any authority valid for every name Often a problem in enterprise and federation Can the Boeing.com STS assert identities in "@airforce.mil"? What about "@airbus.com"? What about server names? Solutions: SID Filtering in Active Directory Apply a scope or bailiwick for every counterparty Make this a mandatory part of establishing a trust

Language: Configuring a "trusted partner" implies too much I prefer "federation counterparty"

4. PKI, PKIX and SSL/TLS Dependencies We all hate it here at IIW. But it is the one universal Internet-scale identity system, and one that is also widespread at big organizations Interop is a tempting target But it is more complex… OID extensions, constraints, KU, EKU And less trustworthy than you think Non unique names Negligent and Bad actors No assurance for client certs 4. PKI, PKIX and SSL/TLS Dependencies

Problems with Production / Non-Production systems We don't want to spend the money for certs for our development, test and acceptance environment We don't want to or don't know how to set up our own authority (Wrong) Solutions? Turn off validation (and forget to turn it back on) Use same keys for all environments (no separation of duties) 5. Impedance Mismatch in Identity Contexts How granular is an identity?

When you interoperate or cross-contexts with different scopes, how do you normalize this?

6. Denial-of-Service and Confused Deputy Attacks with Revocation and Key Retrieval Good: My key is the entire content of a resource at this anonymously accessible HTTPS URL

Bad: My key is the result of the following XSLT transformation at \\192.168.1.99\c$ \foo\bar 7. False Dilemmas in Adoption vs. Assurance Bearer Tokens vs. Holder-of-Key

Because having to "find, install and configure libraries" is too hard for developers, compared to "the convenience and ease offered by simply using passwords." (from the intro to OAuth 2 page)

Is crypto "too hard"? Not too hard then... Too hard now? Canonicalization and Transformation is Hard, Basic Signature Ops Aren't Canonicalization was what made XML DSIG and OAuth 1.0 difficult, not hashing and crypto Strange but true – building a lenient parser seems to be easier than building a strict serializer. See, e.g. "the Web".

The "See what is seen" idea in XML DSIG that led to XSLT and related functionality is also a misplaced responsibility Canonicalize as little as necessary Extreme C14N is often a layering violation. Cryptographic primitives can provide confidentiality, guarantee authenticity, bind together the parts of a message and serve in producing random numbers

Ensuring that every well-formed message has an unambiguous meaning is the responsibility of the protocol or message layer, not of the cryptographic primitive. The elements of the crypto protocol itself may require careful treatment to avoid type flaws. But the payload should be opaque.

7. False Dilemmas in Adoption vs Assurance, continued The ideal: "There is one mode, and it is secure." – Ian Grigg

The reality: "Something's gotta give." (and guess which one will)

Solution: Build Two Protocols and Incentivize Low friction protocol for easy onboarding

Encourage self sorting of higher value clients to the higher assurance protocol Provide higher value services or assertions Set different price points Examples: SXIP, Google Checkout

TWO protocols, not one protocol with complex options or NegOtiated security

Extra Time: Implementation Foibles Poor 3rd-party token storage (cookies, GET urls, unencrypted at rest) Decrypting tokens but not verifying signatures. Common for encrypted SAML messages HMAC verification timing brute-force Encryption without integrity Mentioned last time – now padding oracle attacks have gone mainstream

http://groups.google.com/group/iiw-common-problems-dist-authN brad@isecpartners.com

Model Personal Data Ecosystem continued (W5B)

Convener: Kaliya Hamlin
Notes-taker(s): Kaliya Hamlin
URL: http://iiw.idcommons.net/Personal_Data_Ecosystem_Model_2

Tags for the session - technology discussed/ideas considered:

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

We outlined things we could talk about.

- Transfer for Risk
- Individual Incentive
- Beyond one time use
- Data Schema
- Long Data -> preservation
- Long History
- Economies of Scale - Quality and Size
- Commercial value of Data
- Auction -> Bidding
- Insight isn't Data
- Analytics - Data -> Info -> Knowledge
- Self Asserted & Validated (credit card transactions) 4th Party
- Companies NEED info
- "go to Market"

Barbara put forward a map of what she was seeing as a ecosystem landscape.

Use cases - Can you ask your friend network - about questions and get back answers without reveling who.

Willing to share in network - example given of last FM friend music similarity in your neighborhood.

Image of a Groker - linked to many PDS's. Today the customers don't know what each other buys.

This was in the context of the amout of information flow that is driving retail sales and how if people had their own ability to link and share data.

Share with my PDS - Things I don't want to show up on the internet. "Your pants won't fall down on you any more"

You should EDU own PDS

Data Assets you have others don't - Highly sensitive highly valuable - keep going back to and permissioning - recommendation services.

Silhouette Service by PDS provider

Data Curation - organization for data at rest.

Most of my life isn't commercial or "social"

Civil Society and Neighborhoods

Identity Integrity

Front Door lock - how are indivdiauls personally responsible

Privacy -> Property frame - Digital Society.

Higher value Quality

What to talk about tomorrow

- Civil Society and Personal Data
- Funness
- Problem Recap - what needs to be solved
- Dating and Relationships and the PDS
- Political Aspects -> Opportunities (NSTIC), Bill of Rights
- Adoption Drives
- Quality going up and information and knowledge.

Cloud Directory Standards (W5C)

Convener: Eric Sachs, Patrick H., Chuck M.
Notes-taker(s): Eric Sachs
URL: http://iiw.idcommons.net/Cloud_Directory_Standards

Tags for the session - technology discussed/ideas considered:

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

Overview of the Cloud LDAP problem:
* https://sites.google.com/site/oauthgoog/cloudldap

* Pressure from customers that are using increased number of SaaS providers

* Provisioning process often involves HR sending a spreadsheet every week

* Want providers to have a simple and consistent mechanism to work with all of these different companies

Some conversation between a few of the vendors around a technical solution:
* REST + OAuth

* Market not ready for a specific format

* SAML Assertion, batch push, run time pull, notifications on state change

Data schema

* Looked at six cloud apps (box.net, google apps, sfdc, webex, travel app, HR app)

* High disparity

* Nearly ubiquitous across providers: username (email for some, not others), first name, last name

* Questions about display name, internationalization. Most providers have optimized naming conventions for their home markets

* Beyond above, huge disparity in required and optional fields across providers

* Contact info, many don't care, others allow these fields as optional

* timezone, locale, language required by sfdc

Next steps

* match these fields against InetOrg and EduPerson persons

* Lots of subtle difference in the use of attributes

* mapping attribute names to providers is really hard

* Assertion that lowest common denominator doesn't meet the needs of any service

- Every app needs its own attributes and many definitions for common attributes overloaded

Infrastructure: Focus on Relationships Among Things (W5D)

Convener: Bob Frankston
Notes-taker(s):
URL: http://iiw.idcommons.net/Infrastructure_Focus_-_Relationships_Among_Things

Tags for the session - technology discussed/ideas considered:

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

For more about this topic you can go here:

http://frankston.com/public/?n=MakerDisconnect

http://frankston.com/public/?n=AmbientConnectivity

JSON Token Spec Work – Claim Names (W5E)

Convener: Mike Jones
Notes-taker(s): Mike Jones
URL: http://iiw.idcommons.net/JSON_Token_Spec_-_Claim_Names

Tags for the session - technology discussed/ideas considered:

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

We held a session on naming for JSON Web Tokens (JWTs) at IIW (Wednesday during Session 5 in space E), building upon the results from the JSON Tokens and No Base String sessions on Tuesday and the JSON Token Encryption session on Wednesday. Like the previous sessions, there was a clear consensus for the decisions the group made.

Names are needed for these specification elements:
   * Envelope parameters (such as the name of the signature parameter)
   * Claim names (such as the name of the issuer claim)
   * Algorithm names (such as the names representing the HMAC SHA-256 and AES-256-CBC algorithms)

The first issue tacked by the participants was whether short names should be used in order to keep tokens concise (and in particular, in order to have them be potentially usable in query strings for mobile phone browsers with 512-character URL limits), or whether to use longer, descriptive names. For instance, the name of an algorithm parameter could be either "alg" or "algorithm". By a 7-2 vote, the participants opted for short names.

We next used the names in the current JWT spec to drive discussion on specific names in each category. In keeping with the decision to employ short names, Nat Sakimura suggested that the few names over three characters in length – specifically "keyid" and "curi" also be shortened to three-character names. The other participants concurred with this suggestion.

A discussion was held on behalf of Paul Tarjan of Facebook on defining a standard time-issued-at claim (which together with the expires claim, bounds the token lifetime). There was consensus that this claim should be defined by the specification.

George Fletcher led a discussion on whether an issued-to claim distinct from the audience claim should be defined. The group didn't feel strongly about this, but voted 3-1 against including it. The participants noted that any claims meaningful to both parties can be defined as needed, so all claims need not be pre-defined in the specification.

The group discussed what algorithm names should be used. It was agreed that while each software package uses specific names for algorithms, because they tend to differ by software package, there is no compelling reason to choose one set over another. And indeed, given the group's over-arching decision to use short names, people felt that employing short names such as "HS256" imposed no more burden on implementers that using longer names like "HMAC-SHA-256" or "http://www.w3.org/ 2001/04/xmldsig-more#hmac-sha256". Thus, the short names in the current JWT spec were endorsed, with the understanding that additional names will be needed for encryption algorithm names and names of recommended algorithm combinations.

To help implementers, the group suggested that the specification include a table cross-referencing the algorithm name strings used in standard software packages and specifications. Breno de Medeiros supplied a link to the JCE algorithm names for inclusion in this table.

While not strictly on the topic of naming, the group held a discussion of how to factor the JWT specification or specifications so as to maximize its acceptance and adoption. The choices discussed were (1) a single specification, (2) a part one specification covering signing and claims and a part two specification covering encryption, and (3) three related specifications – one for signing, one for claims, and one for encryption. The consensus was for (2), since the normal use case will always include signed sets of claims, whereas people should only need to pay the price to understand encryption if they actually need to employ it.

Finally, Nat Sakimura asked if we wanted the branding of the specification or specifications to be more general than JSON Web Token (JWT), since the scope of the work is actually broader – encompassing JSON encodings for claims, signing, and encryption. Mike Jones took the position that, given that this is a composite spec including JWT claims, that we're better off branding it in a way that matches the common use case, and therefore and keeping the name JWT as the overall brand. The participants concurred.

OAuth LEELOO (W5F)

Convener: Lucas Z & Maciej M
Notes-taker(s):
URL: http://iiw.idcommons.net/OAuth_LEELOO

Tags for the session - technology discussed/ideas considered:

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

What Do USERS Really Want (W5G)

Convener: Brian Schmidt
Notes-taker(s): Brian Schmidt
URL: http://iiw.idcommons.net/What_do_USERS_want%3F

Tags for the session - technology discussed/ideas considered:

Multiple personas, user experience

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

- Users are asking for fewer credentials but to have multiple personas online.

- Users place different levels of trust in different personas.

- Identity = Actual Person; Personas = how you want to be known to an application

- Facebook, Twitter, Google, Yahoo all give you personas to be used across internet

- Over time, trust in the personas can change.

- Critical personas (banking, health, etc). Social personas (facebook stuff).

- Most users are "reactive" to privacy issues; they're largely unaware of issues until they start hearing about things in the press, from friends (even happens to them).

- Which identities to people use depends on what they're doing.
  Gigya data support this: http://info.gigya.com/Identity.html

- Advisable that PDS (or other trust systems) should allow for multiple personas because users demand this type of flexibility.

- PDS systems should support real-world behavior with regards to multiple personas

- PDS user interfaces should make mapping to personas dirt simple.

- Don't overcomplicate PDS for users; focus on the few really impactful ideas and discard the other ideas until proven to be needed (Apple approach).

OpenID Attributes – Beyond Attribute Exchange (W5I)

Convener: Jay Unger
Notes-taker(s): Jay Unger
URL: http://iiw.idcommons.net/OpenID_Attrib_-_Beyond_AX-SREG

Tags for the session - technology discussed/ideas considered:

OpenID, Attributes, Signed Claims, Attribute Exchange

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

- The meeting was attended by about 5 people
- Jay Unger presented a small set of slides regarding his ideas about identity attributes. http://www.slideshare.net/JayUnger/iiw11-beyond-attribute-exchange
- He re-iterated a concept from his earlier session that a pseudonym related to user and the relying party requesting identity information was the only "Attribute" that should be presented to relying party without an additional request of the relying party and permission of the subject (user).
- He also discussed the concept that the "identity triangle" was really a "rectangle or diamond" that included all of: the subject, the identity provider (IdP), the Relying Party (RP) and possibly one or more Attribute Providers (AP). He mentioned that the NSTIC (National Strategy for Trusted Identities in Cyberspace) draft also described eluded to this concept.
- He discussed the role of Attribute providers as brokers of verified, certified or vetted assertions (claims) about the identity of the subject including things like age or date of birth, citizenship, address or other contact information, employment, credit rating etc. There was a good deal of discussion about this role and the overlap with existing business or organizations like governments, credit reporting agencies, insurance companies, motor vehicle bureaus etc.
- In Jay's presentation he discussed the need for Attributes to have a richer data model than is presently supported by OpenID including things like: conditions of use, duration (valid / expires), confidence level or strength of assurance of the assertion, dependency on other attributes or external information etc. He also discussed the requirement that such attribute assertion be digitally signed by the Attribute provider to insure provenance and integrity. He pointed out that SAML XML Assertion markup can include much (but not all) of this information.
- There was a discussion of whether such attributes should be stored (or cached) by IdPs. There was agreement that in many cases storage of the attributes by an IdP was valuable to provide economy in the request -response protocol between an IdP and Relying Party, but we agreed there might be cases where a Relying Party would want to interact directly with the Attribute Provider to close any revocation window and also for trust chaining.
- We discussed briefly how these ideas might mesh with the work being done on the next revision of OpenID including both the OpenID Connect proposal and the Artifact Binding proposal or a convergence of both. It seems that as these proposals mature there is opportunity to get some of these concepts adopted.

Day Three - Thursday November 4th

Session 1

Go To Market PDE (TH3A)

Convener: Kaliya Hamlin
Notes-taker(s): Kaliya Hamlin
URL: http://iiw.idcommons.net/Go_To_Market_-_PDE

Tags for the session - technology discussed/ideas considered:

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

This session was a conversation with people considering options and ideas. These were from hand written notes.

Do we really listen

We think it is logically appropriate

People who make market are not here

Support problem set

"tricking users" - no one joined FB to do web SSO

What is user experience? additional features and functionality Features and Benifits - what has internet done for me lately.

Give people something valuable include PDS as well

Expose benifirts of PDE people and organizations

Gradually get there

Data in US is free-for-all

give info ---> you get

what do people find valuable - groupon

Marc - driving forces human needs

- Connect
- Feel safe
- Get Recogintion

all from people you trust

Are we solving a problem that doesn't need to be solved?

Groupon "saving money" - we have the worst unemployment in a long time

Benifits them - home safe enough to eat. this feeling people don't have on the web. Control Self Sufficency

Mobile what is transformative experience

Sarah - Back up your data (Moze & Carbonite) Make it happen

Sam - look at additional benefits, Solve problems that there are no solutions for yet (without making the existing suboptimal)

Ability build special APIs social data - where is it now

Monica - Things I wouldn't share with everyone. Woman walking home alone at night can share geolocation with spouse at home. Tracking spending and directing dollars. Only comfortable with self and close people sharing.

Dave - msft

- Antique Road show - what is it worth

Wendell - all of this is happening

- All big online systems, all events, monetize and change experience
- Compensated
- Better user experience

Asside comment about how to make a lot of money - do a Small industry trade association press - 1,000 of dollars

There are two kinds of stuff people have

1. is that they consciously articulate this is done today with an interest managers
2. the trails that you travel.

These are set up to target adds against

See the semantics of all this

Jay - additional added power of the equals sign

- IdM place holder if we add something to it - (IdM + N) * user adoption = ROI

Save money - social event -> participate in & share/relate

Online -> offline

Cambells Soup: 1-2 reports a quarter - on how soup for example was selling on the shelves.

When scanners came in you could get a daily report because the scanners were ubiquitous

Who are these people actually walking into the store?

can we find out in a privacy appropriate way? can we track "conversions" search -> purchase.

if we do this the wrong way we live in a police state.

Google/MSFT health vault -> Start storing other stuff?

Adam Larson - person in the middle and integrate

One company and technology?

Thing - phone, browser "on top of" Phone operating system

-- Smarter purchasing process

conversation between me and vendor

what my friends bought

Friends and social groups.

Brett.- We are not eyeballs - Holo go through consumer. Behavior me -> yahoo! this data is better then

My Wallet with my permission Ghostery - sends beacons bugs Right now there are funnel Advertising

Beacon site - triangle current aggregated raised in quality Behavior physical world stuff in wallet.

Google's Sample Open IDRP & RP Best Practices (TH1C)

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

Tags for the session - technology discussed/ideas considered:

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

We used the session to go through this document:
https://sites.google.com/site/oauthgoog/Home/openidsamplesite

Overview of OpenIDSampleStore
The website at openidsamplestore.com was built to demonstrate how a website that already allows users to login can help those users (and new users) leverage OpenID to login. Â This provides a number of advantages for website owners such as:

- Higher signup rates for new users and higher return/login rates by existing users
- Lower customer support costs for handling problems with accounts
- Improved account security by leveraging the security features and scale of large identity providers like Yahoo, Google, Microsoft, AOL, etc.

Users obviously also benefit from the improved user experience that can be achieved with OpenID.

The Challenges
Larger websites that have experimented with OpenID have found that it can cause confusion among some of their users who already have logins on the site. Â That confusion can lead to customer support requests that are expensive to handle. Â This RP (relying party) best practices article provides details on many of those challenges. Google built the openidsamplestore.com site to demonstrate how to combine those RP best practices with our latest research for how a website with a large set of existing user accounts can start to migrate to OpenID.

In addition to the sample site, we have provide a collection of videos (see below) to show how the site handles some of the trickier issues with OpenID, or you can experiment with the website directly.

We hope that website owners will experiment with this sample site so that they can see how they might add OpenID support to their own site. Â We also hope that the owners of existing OpenID enabled sites will evaluate whether the features and user-interface of the sample site would avoid some of the user confusion and customer support costs that they have encountered. Â A large part of the design of the sample

Public Key Certificates as JASON Web Tokens (TH1E)

Convener: Mike Jones, Microsoft
Notes-taker(s): Breno de Medeiros
URL: http://iiw.idcommons.net/JSON_Spec_Work_continued

Tags for the session - technology discussed/ideas considered:

If and how to represent public key certificates as Jason Web Tokens

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

The final session at IIW related to JSON Web Tokens (JWTs) explored whether and how to represent public key information as JWTs or other JSON structures as an alternative to X.509 certificates. Thanks to Breno de Medeiros for taking notes, which I've pasted in below:

- Certificate installation a difficult and core technical obstacle in configuring security
- Not all cases require PKI validation; motivation examples given by J. Panzer et. al., drove the proposal for the Magic Signatures specs
- In the absence of PKI certificates, it's not possible to 'preserve' the security context around fetching the certificate
- Is there a need to invent another type of JSON-based certificate? De we have a need for certificates in addition to bare keys
- Why re-invent X.509? Create a JSON binding for the subset of KeyInfo from X.509 that is needed to advertise keys
- After reviewing the KeyInfo, decided that the part of it of interest is trivially small and already described in competing proposals
- Even a JWT is too complex, only need to create a simple descriptor for the key in JSON
- Key_id needed

  Decision: Go with simple approach

  Keep this mini-spec separate from JWT and cross-reference? Or include this in the expanded spec of JWT to include encryption?
  –
  Decision: Keep specs separate
  Need to allow this to have a URL-safe representation such as compact JWT?

From Mike:

Examples of what these representations might look like are as follows:

```
{"keyvalues":
  [
    {"alg":"ECDSA",
     "x":"MKBCTNIcKUSDii11ySs3526iDZ8AiTo7Tu6KPAqv7D4",
     "y":"4Etl6SRW2YiLUrN5vfvVHuhp7x8PxltmWWlbbM4IFyM",
     "keyid":"1"},

    {"alg":"RSA",
     "modulus":
"0vx7agoebGcQSuuPiLJXZptN9nndrQmbXEps2aiAFbWhM78LhWx4cbbfAAtVT86
zwu1RK7aPFFxuhDR1L6tSoc_BJECPebWKRXjBZCiFV4n3oknjhMstn64tZ_2W-5J
sGY4Hc5n9yBXArwl93lqt7_RN5w6Cf0h4QyQ5v-65YGjQR0_FDW2QvzqY368QQMi
cAtaSqzs8KJZgnYb9c7d0zgdAZHzu6qMQvRL5hajrn1n91CbOpbISD08qNLyrdkt
-bFTWhAI4vMQFh6WeZu0fM4lFd2NcRwr3XPksINHaQ-G_xBniIqbw0Ls1jF44-
csFCur-kEgU8awapJzKnqDKgw",
     "exponent":"AQAB",
     "keyid":"2"}
  ]
}
```

Near the end of the discussion, it was pointed out that what we are proposing is much closer to the XMLDSIG KeyValue element than the KeyInfo element.

The participants recognize that the security of these raw keys is dependent upon the security of the mechanisms for distributing them – in most cases TLS.

References:
- XML Signature Syntax and Processing (Second Edition): http://www.w3.org/TR/xmldsig-core/
- Using the Elliptic Curve Signature Algorithm (ECDSA) for XML Digital Signatures: http://tools.ietf.org/html/rfc4050
- Additional XML Security Uniform Resource Identifiers (URIs): http://tools.ietf.org/html/rfc4051
- Magic Signatures: http://salmon-protocol.googlecode.com/svn/trunk/draft-panzer-magicsig-experimental-00.html

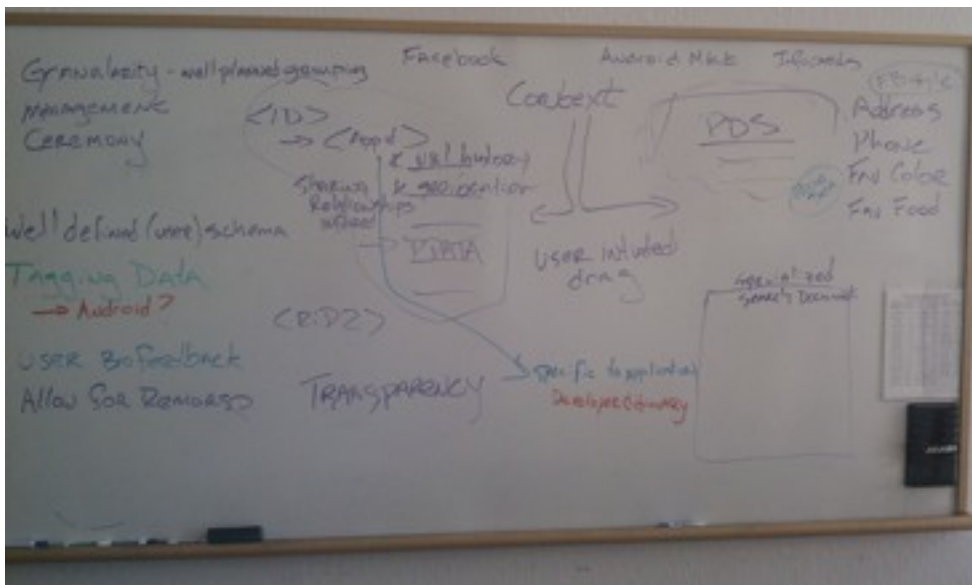-- Mike

User Managed Permissions (TH1F)

Convener: Mark
Notes-taker(s): Joe Andrieu
URL: http://iiw.idcommons.net/User_Managed_Permission_Interface

Tags for the session - technology discussed/ideas considered:

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

Granularity
Management
Ceremony

Facebook
Android Market
Infocards

Kynetx Data Model (KDM & PDS)
<ID> (internal user id for tracking activity)
  <RID1> (ID unique per user per app)
    stuff1 (URL History)

```
     stuff2 (geolocation)
  <RID2>
     stuff3
     stuff4
```

PDS (starting with XRI/XDI dictionary)

What's the boundary between KDM & PDS?

KDM is application-limited
PDS is available for sharing via permissioned access

So, how do we manage permissions for access to the PDS?

You can use application-specific gestures that make it obvious which
permissions are granted. For example, dragging a GEO location onto a
picture can be constructed to /mean/ that the subjects of the photo are
permissioned to know that geolocation information.

In a link contract, the permissions define addressable entries in the
graph

At a minimum, you need a gesture to indicate what is being permissioned

Voluntary Oblivious Compliance
I have a bunch of things I can share, but I don't know the rules for
sharing, e.g., corporate rules about data releases. But there is a
background policy protecting the user from breaking those rules.

There may be a role for "policy" providers and a distinguishable role
for automated tagging, which tags the data for use by policies.

Note: the PDS must keep track of permissions and data access /and/ the
user should be given tools to view & manage their permissions based on
actual basis

Groups v individual permissions in an ACL

Default verses specific versus override = inherently complex.

Must supply an "oops" button to revoke, fix, errors in permissions..

Session 2

Your Terms of Use – Privacy Policy (TH2E)

Convener: Doc Searls
Notes-taker(s):
URL: http://iiw.idcommons.net/Terms_of_Use_Privacy_Policy

Tags for the session - technology discussed/ideas considered:

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

Look Up By Phone Number (TH2G)

Convener: Kevin Marks
Notes-taker(s):
URL: http://iiw.idcommons.net/Look_Up_by_Phone_Number

Tags for the session - technology discussed/ideas considered:

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

Kitties Are Fluffy (TH21)

Convener: Justin R.
Notes-taker(s): Sean Cashin
URL: http://iiw.idcommons.net/Kitties_are_Fluffy

Tags for the session - technology discussed/ideas considered:

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

How to deal with employees mistakenly saying personal things in the company light.

OpenID and "Handshake" available to employees.

Employee takes company OpenID and says Kitties are fluffy on Blog. Does that mean company now supports kitties being fluffy?

Legal, Policy, sociology what is the issue here?

Passive disseminating of information in Social Networks can be interpreted poorly by companies.

Social Media so new, so have to trust people and accept that mistakes are made. Company now just makes sure they cover themselves.

Don't restrict peoples speech, according to one companies legal department. You don't want to go there.

Monitoring tools are important. Can't blindly trust.

Want to make sure employees have access to the data they need to be productive, but you also can't be so open that your data is out.

Disclaimers are normal company policy. Bringing some idea of official company accounts to services to provide automated disclaimers. Allows people to give company approved statements.

Reputation with your online identity is a determining factor of how people interpret things you say in the public forum.

It all comes down to trust of employees. You can't have policies for every condition.

You don't have to be around a journalist to be on the record anymore. With social media everyone has their soapbox.

Benefit in enterprise with OpenID is that when someone does something wrong the company knows exactly who to tell. They can do company reprimand, reminder, etc.

Go To Market For PDE? Part 2 (TH2M)

Convener: Kaliya Hamlin
Notes-taker(s): Kaliya Hamlin
URL: http://iiw.idcommons.net/Go_To_Market_PDE_2

Tags for the session - technology discussed/ideas considered:

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

iOS	Safari
Android	Chrome
Windows	Explorer
_____	Mozilila

Facebook SSO environment across everything

Talking about new Chrome OS - you login to the computer and it brings all your stuff from the cloud down into the system and knows who you are.

Hold Users REal IDentity in master directory.

ChromeOS you sign into book marks etc.

Back into very fabric the OS knows who you are.

PDS - personal data store

- Hard drive of iPhone - I have control

User-Adoption use phone and browser

Version of the truth - per roll

"Anonymous user" - Dependent / Indpendent

- A quote from facebook - We believe that data wants to be unified.

EMR

Silhouette and Pattern Detection - Permissioned Research.

PDS is an abstraction - collection of data across many things

- How do you connect and have control.

Start with easily collectable things

- Calendar
- Transaction graph - credit cards - member/customer
- Things I own and buy

Services I use

Social graph "I know this person"

- Where I go
- Who I know
- Where i go

Transaction graph - I connect to each of the things I am a customer of

Not enough to make graph

- Portable and Private
- Social & Interest
- Transactional - things I own and services

Display Advertising ecosystem because none of this data is surfaced to the user.

Session 3

Go to Market and Community Strategy for PDE? (TH3A)

Convener: Kaliya Hamlin
Notes-taker(s): Kaliya Hamlin
URL: http://iiw.idcommons.net/PDE_-_Go_to_Market_and_Community_Strategy

Tags for the session – technology discussed/ideas considered:

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

What are the use cases for initial got to market?

What is the value proposition for those who have capital?

Monetization is key

Don't make a guess

Pitch is conversation

Let us tell you (across multiple domains)

Refine conversation model

User -> "Intent to purchase" explicit declaration -> Existing Data Exchange?

Key Models/Features outlined

- Social Address Book
- Alternative Social Graph (owned by people in it)
- Groups
- Better Targeting
- VRM B->C
- Core Services - Backup, DeDupe, Sync

Question: What do we "have to have" for data.

Interop how does this actually happen

Who is solving this? Where is it being solved?

Do defacto standards emerge

One could go at this with a chart

Across the top the different groups

- Telco's
- Webco's
- Apps/Developers/Startups
- Standards Stuff/ Interop
- Legal Regulatory Advocacy
- End User Citizens People
- B-C Businesses
- B-B Businesses
- Organizations, NGO's, NPO's (churches, activism groups, schools)
- Informal Groups/Classes
- Education
- Standards/Industry Organizations

on the other axis - Today, Unanswered Questions, Can do soon, long term

Go to Market Paths:

- Telco's adopt PDS + give to consumer
- Facebook/MSFT/Google/Yahoo! gives data control to user
- 3rd Party creates PdS for users, advocates with users for integration with services (Statz, Buynamite, Epass)
- Laws & Regulation make more money by complying. Potential for new regulation in US and EU existing law.

R Button Session (TH3E)

Convener: Doc
Notes-taker(s): Alan Karp
URL: http://iiw.idcommons.net/R_Button_Affordamies

Tags for the session - technology discussed/ideas considered:

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

Left button represents user's policy

Right button represents seller's policy

Buttons merge if policies are compatible

Seller (and user?) are informed of what doesn't match

User clicks right button if no agreement and can change user's policy
 for this seller, sellers want to avoid this friction so they use
 policies likely to be accepted by most users

User clicks left button to change policy for all sellers

Adopting OAuth 2 – Open ID Connect (TH3F)

Convener: Travis Spencer
Notes-taker(s):
URL: http://iiw.idcommons.net/Adopting_OAuth_2_OpenID_Connect

Tags for the session - technology discussed/ideas considered:

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

We talked about the following (among other things) during this session:

- The timetable for finalization of the OpenID Artifact Binding (AB). According to John Bradley, the spec would be finalized in a month or so.

- John told us the OpenID AB would not directly depend on OAuth 2 because it isn't finalized but that OpenID AB would make migration to the final spec as simple as possible.

- The Leeloo development team said that they are not concerned w/ the state of the OAuth spec and are taking a dependency on it for UMA. They did say in another session that there are things in the spec that they didn't implement because there has been talk on the mailing list about changes in that area (not sure which exactly)

- A employee of Oracle said that the current flux in the OAuth spec coupled w/ some security issues are the reasons that they are advising all of their clients not to use the protocol ATM.
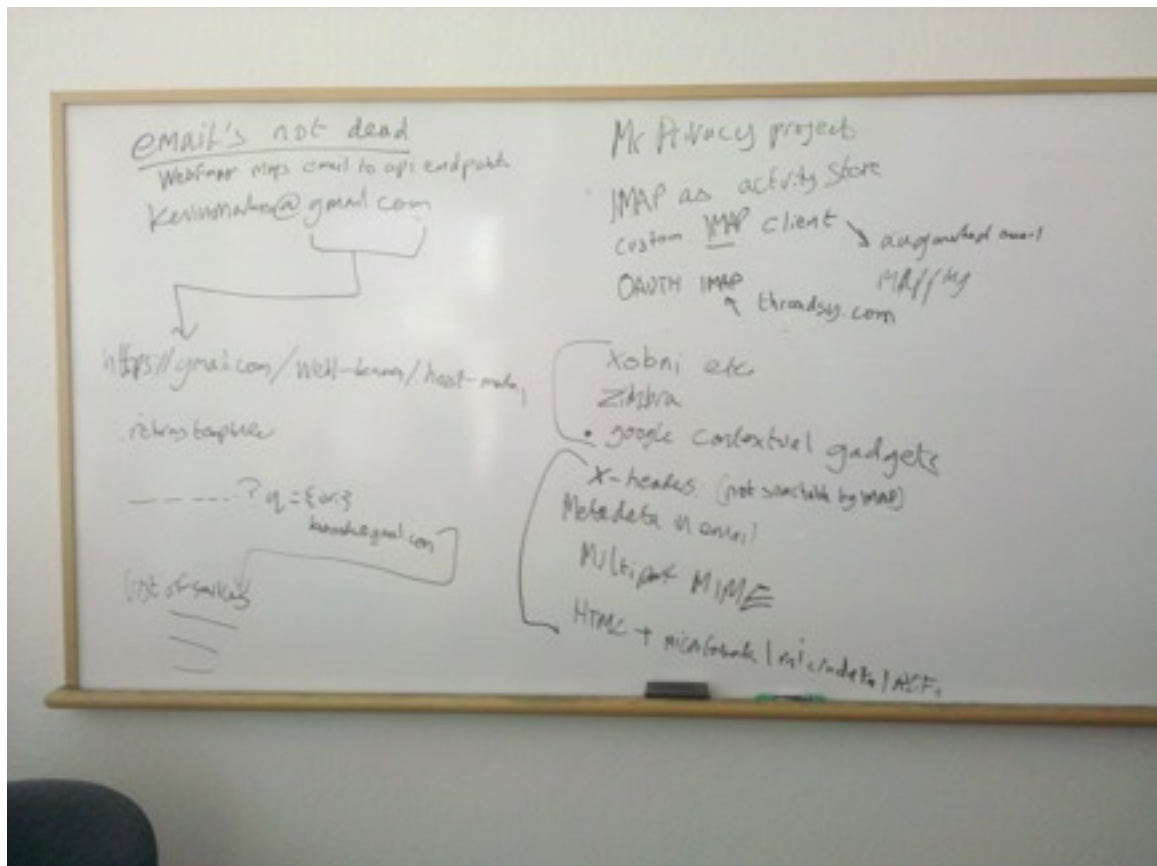
Email Is Not Dead (TH3G)

Convener: Kevin Marks
Notes-taker(s):
URL: http://iiw.idcommons.net/Email_is_not_Dead_Yet

Tags for the session - technology discussed/ideas considered:

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

Privacy Framework (TH2L & 3L)

Convener: Jeff Stollman
Notes-taker(s): Jeff Stollman
URL: http://iiw.idcommons.net/Policy_Framework

Tags for the session - technology discussed/ideas considered:

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

Attendees: Joni Brennan, Jay Unger, Peter Capek, Alan Zhao, Max Beman

One effective way of creating an identity ecosystem that provides both trust and privacy is through a Trust Framework. The Kantara Initiative has created one of the first trust frameworks which has been certified by the US Federal Government through the Identity, Credential, & Access Management committee (ICAM). Kantara is now garnering support for the development of a Privacy Framework that will document auditable Service Assessment Criteria (SACs) that will allow for the certification of the personal information handling practices of Identity Providers and Relying Parties. The session sought to solicit both ideas and ongoing participants in the Privacy Framework development effort.

Background
In the traditional three-party internet transaction model, there are Subjects, Identity Providers (IdPs) and Relying Parties (RPs). To create trust among all three parties, a Trust Framework establishes a three-legged stool that provides (1) Assurance, (2) Protection, and (3) Control.

Assurance is the trust a Relying Party can have in the ability of the Identity Provider to accurately represent the Subject when the Identity Provider assigns an ID to the Subject.

Protection is the ability of the Subject to trust that his personal information is being handled "as advertised" by both the IdP and the RP.

Control is the ability of the Subject to correct errors in the information about him/ her as well as the ability specify when and how this information is disseminated.
[NOTE: In our discussion we also noted that a fourth part is likely to exist for many transactions: the attribute provider. But we did not digress into this area, reserving it for future discussion.]
The US National Institute of Standards and Technology (NIST) has defined a hierarchy four Levels of Assurance and prescribed information proofing practices necessary to provide increasing levels of assurance for transactions that require them. At Level 1,

an identity can be self-asserted for simple transactions such as managing one's Facebook account. Additional assurance is typically required for higher value transactions that might involve the transfer of money or confidential information. The Kantara Initiative has already created an Identity Assurance Framework (IAF). This Framework describes auditable Service Assessment Criteria (SACs) that can be used to vet an Identity Provider's ability to provide identities at different Levels of Assurance. The IAF establishes these broad rules and also includes profiles that allow for variations as needed to address unique requirements that exist for different trust frameworks (typically defined by either national jurisdiction or industry sector). A profile has been created for the US government's ICAM program. The IAF provides an RP with the necessary level of trust to conduct business at various Levels of Assurance.

Privacy Framework
The next step needed in this process is to create a Privacy Framework that afford Subjects the trust they need in how their personal information will be treated to induce them to use the Trust Framework.
In the session we discussed various issues regarding a Privacy Framework. For example, we discussed whether it is practical to establish Levels of Protection in the same way the the Identity Assurance Framework establishes Levels of Assurance. We also discussed the viability of combining Levels of Control with Levels of Assurance, but the group's initial inclination was to keep these separate.

Next Steps
One of the goals of the discussion was to enlist ongoing contributors to the creation of the Privacy Framework. Several of the participants recognized the criticality and high visibility of this effort and were enthusiastic to participate. Participation will begin via one-hour, bi-weekly telecons to be held every other Thursday at 08:00 Pacific Time to gather the team and layout the work streams.

Others interested in participating or with questions about the effort should contact Jeff Stollman (stollman.j at gmail.com).

Thank you. Jeff

Session 4

Best Way to Connect People to Content That is Relevant (TH4E)

Convener: Kevin and Monica
Notes-taker(s):
URL: http://iiw.idcommons.net/Best_Ways_to_Connect_People_to_Content

Tags for the session - technology discussed/ideas considered:

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

Personal Data Ecosystem ORG Role (TH4F + TH 5F)

Convener: Kaliya Hamlin
Notes-taker(s): Kaliya Hamlin
URL: http://iiw.idcommons.net/Personal_Data_Ecosystem_Org_Role

Tags for the session - technology discussed/ideas considered:

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

Notes for last two sessions of IIW -

Translator between main points of activity -- visit the neighboring industries to move along to market

- Professional Associations
- Health
- Finance
- Real Estate
- Edu
- CISSP
- ISC2

The existing advertising world

Translator between main points of activity

- Glossary - Terms
- Directory
  - People
  - Companies
  - Projects (open source, standards)

Clinical Trials (get users involved)

Foster Incubation of new Framework

Business Value Found (who are participants & what are they getting out of it)

- Value Network Analysis
- Scenario Futures
- Data Flow $

Main point of Contact for Larger Companies
- Executive Information Complexity Reduction
- Aggregation Curation Function (GigaOM Pro $75)
- Thought Leadership Bring it Together
- Fit different aspects in
- Analyze different players
- Sanity Check Internationally

Data Flow's Internationally - heat map or privacy

Frame/Map stage discussion

Much is happening in this area but removed from this community

They are "terrified" of Government and Public Perception Poisoned Well.
- Ad Exchange.com
- Mediapost.com
- AdAge

The conferences are NY & SF

They are all in the business of Audience Selling.

Companies Mentioned
- better advertising
- statz
- oneword
- Telco-Webco Collaboration
- Telco as IdP for Kids
- Telco - Accenture, IBM
- Utility Company roll
  - Higher value
  - "more personal"
  - Set top box for storage
  - What spend $

Subscription Model - Industry Segment

Privacy - Biz Model
- Reduce Risk Complexity
- Protection Harm - Benifit
- CISSP
- ISC2 -> certification

Potential Models

- Volunteers
- Kickstart

(Aside Comments) Rebels take over the deathstar? did it happen is it possible

Executive Convincing
- Magazines
- Book
- Talks
- Reports
    - simplifying diagram
    - media machine
- Consulting
- Events
- Produce summary of hot button things coming out of IIW
- Editor/Interest & Passion - contribute by someone else

Core Asset - Development

Lineup - roster

TEDx about identity?

IIW is a compost Bin

Aggregate create good soil and grow good food

Economically Sustainable

Home for Community

$4000/Head - Executives

Marketing Business - IIW assets
- "Personal Information Econ/Ecosystem" - PIE
- "communicate to execs"
- "Digital Bill of Rights" UN

The Transactional Graph (TH4G)

Convener: Adam Carson
Notes-taker(s):
URL: http://iiw.idcommons.net/The_Transactional_Graph

Tags for the session - technology discussed/ideas considered:

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

None...just a small discussion with two people.

Session 5

Googles Usability (TH5C)

Convener: Eric Sachs
Notes-taker(s): Sha-Mayn The
URL: http://iiw.idcommons.net/Google_Usability

Tags for the session - technology discussed/ideas considered:

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

Overview (Eric):
- demo of the two-tab approach
- demo of the identity selector
- discussion of multiple identities

Benefits:
 * Higher signup rates for new users and higher return/login rates
by existing users
 * Lower customer support costs for handling problems with accounts
 * Improved account security by leveraging the security features
and scale of large identity providers like Yahoo, Google, Microsoft,
AOL, etc.
- Users obviously also benefit from the improved user experience that can be achieved
with OpenID.
Audiences recognize the demo is a long-awaited activity by the OpenID community.

Q: If a gmail user input his email address and password as in legacy
way, can the user login successfully via openid?
A: Yes, and we provide a training page to notify the user that next
time he can simply choose the second login tab.

Q: Can the order of the listed nascar icons change?
A: Yes, each RP site will customize its desired list.

Q: How was the website built, and how much lines of code were needed?
A: The website was built by taking a popular e-commerce website
package, OpenCart, and then extending the login system with a new
login-box to support OpenID, as well as adding the necessary backend
support. Several thousand lines of code.

Q: Will Google be making the code open source?

A: The current code was written for research purposes, and is not in a form we could open source. However we plan to continue our research in this area based on feedback from website owners, and we may provide some parts of the site as Open Source. For example, the login box user-interface is built in JavaScript and so we are evaluating how we might provide that as a stand alone component.

Q: Will this work for non-listed IDPs?
A: Yes, end users can input email or openid of non-listed IDPs.

Q: Have you tried css history for remembering accounts?

Multiple identities (Chris Messina)
- How a user can identify in a way that is meaningful to themselves
- Email/password works fine, but when they take creddentials to other sites
- Using photos works well in browsers and mobile devices
- Concept of incognito window - could you also have identity windows?
- how to work well with multiple accounts?

Mozilla demo:
- Browser takes over OS. user selects accounts and authorizes the browser to take over for this session
- Identity at browser level: incognito mode or use one of multiple identities

Quora:
- Different profile photo shown on login page when you type in the email
- Shows account picker on signed out page

Branding of the Plus sign
- Is it sufficient to have a plus sign for users to know that they should add an account if there are none yet? No better icon so far.
- If there is just one text box people think it's a newsletter signup, but people blindly respond to two text boxes (user/password)

Comment
- add mouseover to the plus sign "add a new account"
- Express login will become a competitive advantage

Q: How about showing both tabs on the same page?
A: We've tried many permutations (email, password/no password, buttons). People don't read, they get confused and do nothing

Q: Comment on passpack: tool that will fill in the password field for you. Why not do something similar?
A: Login box should work for IE5 with no plugins

Training page
- shows you what you should be clicking, so you notice the 2nd tab
tested against people who never used a google account
30% of users noticed the tab and recognized the yahoo and aol buttons

Q: Reducing Nascar buttons
A: Using xAuth
- if you go to a site that you've never visited and something shows up about them, it scares them (facebook does it anyway)

Q: Clicking plus button on one website
- how to make it work across sites?
- enterprises want to make it easy for their employees to log in in many places

Comments:
- Single log out is a hard problem. Make it an advantage/feature
- Removing the box should mean i want to clear myself

Q: How do people react to training?
- 60% need 1 training, 30% need 2, 10% need 3. Generally positive response.

Q: What about non-openid accounts in the selector?
A: There's nothing in the UI is specific to openid

Q: What about personalized bookmarks? Drag your identity from the browser into the site

Q: What about making 2nd tab the default?
A: from the sites that tested it: all sites switched to first tab until 70%
With 3 idps (AOL, Yahoo, Google) looks like they can easily reach 70%
Hard to do AB testing on same site.

Personal Data Ecosystem ORG Role (TH4F + TH 5F)

Convener: Kaliya Hamlin
Notes-taker(s): Kaliya Hamlin
URL: http://iiw.idcommons.net/Personal_Data_Ecosystem_Org_Role

Tags for the session - technology discussed/ideas considered:

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

Notes for last two sessions of IIW -

Translator between main points of activity -- visit the neighboring industries to move along to market

- Professional Associations
- Health
- Finance
- Real Estate
- Edu
- CISSP
- ISC2

The existing advertising world

Translator between main points of activity

- Glossary - Terms
- Directory
    - People
    - Companies
    - Projects (open source, standards)

Clinical Trials (get users involved)

Foster Incubation of new Framework

Business Value Found (who are participants & what are they getting out of it)

- Value Network Analysis
- Scenario Futures
- Data Flow $

Main point of Contact for Larger Companies

- Executive Information Complexity Reduction
- Aggregation Curation Function (GigaOM Pro $75)
- Thought Leadership Bring it Together
- Fit different aspects in
- Analyze different players
- Sanity Check Internationally

Data Flow's Internationally - heat map or privacy

Frame/Map stage discussion

Much is happening in this area but removed from this community

They are "terrified" of Government and Public Perception Poisoned Well.

- Ad Exchange.com
- Mediapost.com
- AdAge

The conferences are NY & SF

They are all in the business of Audience Selling.

Companies Mentioned

- better advertising
- statz
- oneword
- Telco-Webco Collaboration
- Telco as IdP for Kids
- Telco - Accenture, IBM
- Utility Company roll
  - Higher value
  - "more personal"
  - Set top box for storage
  - What spend $

Subscription Model - Industry Segment

Privacy - Biz Model
- Reduce Risk Complexity
- Protection Harm - Benifit
- CISSP
- ISC2 -> certification

Potential Models

- Volunteers
- Kickstart

(Aside Comments) Rebels take over the deathstar? did it happen is it possible

Executive Convincing

- Magazines
- Book
- Talks
- Reports
    - simplifying diagram
    - media machine
- Consulting
- Events
- Produce summary of hot button things coming out of IIW
- Editor/Interest & Passion - contribute by someone else

Core Asset - Development

Lineup - roster

TEDx about identity?

IIW is a compost Bin

Aggregate create good soil and grow good food

Economically Sustainable

Home for Community

$4000/Head - Executives

Marketing Business - IIW assets

- "Personal Information Econ/Ecosystem" - PIE
- "communicate to execs"
- "Digital Bill of Rights" UN

About IIW Events

The Internet Identity Workshop (IIW) was founded in the fall of 2005 by Phil Windley, Doc Searls and Kaliya Hamlin. IIW is a working group of Identity Commons The event has been a leading space of innovation and collaboration amongst the diverse community working on user-centric identity. The spring of 2011 event will be the 12th workshop held in California.

It has been one of the most effective venues for promoting and developing Web-site independent identity systems like OpenID, OAuth, and Information Cards. Past IIW events have proven to be an effective tool for building community in the Internet identity space as well as to get actual work accomplished. The event has a unique format – the agenda is created live the day of the event. This allows for the discussion of key issues, projects and a lot of interactive opportunities with key industry leaders.

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

To read the Values of IIW as articulated by attendees of the 11th event held in November of 2010, you can go here:
http://www.internetidentityworkshop.com/iiw-values/
To read descriptions of 'what IIW is' as articulated by attendees of the 11th event held in November of 2010, you can go here:
http://www.internetidentityworkshop.com/what-is-iiw/

We are considering doing more events outside the Bay Area branded "Identity Open Spaces" once we get feedback from attendees at IIW East and IIW Europe we will know more about when and where they will be and what themes they will have. If you want to share thoughts with us on this please e-mail kaliya (at) mac.com and Phil (at) Windley.org.

To check on Upcoming Events you can go here: http://www.internetidentityworkshop.com/

IIW Events would not be possible without the community that gathers or the sponsors that make the gathering feasible. Below are the sponsors that supported IIW XI. The Notes Collection Center and collection, compiling of notes including producing this book and getting notes onto the Wiki was supported specifically by Google.

Facebook – Gigya – Google – Kynetx
Microsoft – OpenID Foundation – PingID – Yahoo!

Thank you to all our sponsors!