Internet Identity Workshop comes to DC!

September 9 -10, 2010 Washington DC
Josephine Butler Parks Center

Theme: Open Identity for Open Government

Book of Proceedings

Sponsorship Provided by
Booz Allen Hamilton

Event Production Support Provided by
Wayne Moses Burke & Lucas Cioffi

Table of Contents

Thursday October 9, 2010

Thursday Session 1

Role of Government as Identity Oracle (Attribute Provider) (T1A)

Convener: Anil John
Notes-taker(s): Anil John and Ian Glazer

Tags for the session - technology discussed/ideas considered:

Technorati Tags: #iiw,Attributes,Claims,Identity Oracle,ICAM
del.icio.us Tags: #iiw,Attributes,Claims,Identity Oracle,ICAM

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

My proposal of this session at IIW East was driven by the following context:

- We are moving into an environment where dynamic, contextual, policy driven mechanisms are needed to make real time access control decisions at the moment of need
- The input to these decisions are based on attributes/claims which reside in multiple authoritative sources
- The authoritative-ness/relevance of these attributes are based on the closeness of a relationship that the keeper/data-steward of the source has with the subject. I would highly recommend reading the Burton Group paper (FREE) by Bob Blakley on "A Relationship Layer for the Web . . . and for Enterprises, Too" which provides very cogent and relevant reasoning as to why authoritativeness of attributes is driven by the relationship between the subject and the attribute provider
- There are a set of attributes that the Government maintains thorough its lifecycle, on behalf of citizens, that have significant value in multiple transactions a citizen conducts. As such, is there a need for these attributes to be provided by the government for use and is there a market that could build value on top of what the government can offer?

Some of the vocal folks at this session, in no particular order, included (my apologies to folks I may have missed):

- Dr. Peter Alterman, NIH
- Ian Glazer, Gartner
- Gerry Beuchelt, MITRE
- Nishant Kaushik, Oracle
- Laura Hunter, Microsoft
- Pamela Dingle, Ping Identity
- Mary Ruddy, Meristic
- Me, Citizen 

We started out the session converging on (an aspect of) an Identity Oracle as something that provides an answer to a question but not an attribute. The classic example of this is someone who wishes to buy alcohol which is age restricted in the US. The question that can be asked of an Oracle would be "Is this person old enough to buy alcohol?" and the answer that comes back is "Yes/No" with the Oracle handling all of the heavy lifting on the backend regarding state laws that may differ, preservation of Personally Identifiable Information (PII) etc. Contrast this to an Attribute Provider to whom you would be asking "What is this person's Birthday?" and which releases PII info.

It was noted that the Government (Federal/State/Local/Tribal) is authoritative for only a finite number of attributes such as Passport #, Citizenship, Driver's License, Social Security Number etc and that the issue at present is that there does not exist an "Attribute Infrastructure" within the Government. The Federal ICAM Backend Attribute Exchange (BAE) is seen as a mechanism that will move the Government along on this path, but while there is clarity around the technical implementation, there are still outstanding governance issues that need to be resolved.

There was significant discussion about Attribute Quality, Assurance Levels and Authoritativeness. In my own mind, I split them up into Operational Issues and Governance Principles. On the Operational Issue arena, existing experiences with attribute providers have shown the challenges that exist around the quality of data and service level agreements that need to be worked out and defined as part of a multi-party agreement rather than bi-lateral agreements. On the Governance

Principals side, there are potentially two philosophies for how to deal with authoritativeness:

1. A source is designated as authoritative or not and what needs to be resolved from the perspective of on attribute service is how to show the provenance of that data as coming from the authoritative source
2. There are multiple sources of the same attribute and there needs to be the equivalent of a Level of Assurance that can be associated with each attribute

At this point, I am very much in camp (1) but as pointed out at the session, this does NOT preclude the existence of second party attribute services that add value on top of the services provided by the authoritative sources. An example of this is the desire of an organization to do due diligence checks on potential employees. As part of this process, they may find value in contracting the services of service provider that aggregates attributes from multiple sources (some gov't provided and others not) that are provided by them in an "Attribute Contract" that satisfies their business need. Contrast this to them having to build the infrastructure, capabilities and business agreements with multiple attribute providers. The second party provider may offer higher availability, a more targeted Attribute Contract, but with the caveat that some of the attributes that they provide may be 12-18 hours out-of-date etc. Ultimately, it was noted that all decisions are local and the decisions about factors such as authoritativeness and freshness are driven by the policies of the organization.

In a lot of ways, in this discussion we got away from the perspective of the Government as an Identity Oracle but focused on it more as an Attribute Provider. A path forward seemed to be more around encouraging an eco-system that leveraged attribute providers (Gov't and Others) to offer "Oracle Services" whether from the Cloud or not. As such the Oracle on the one end has a business relationship with the Government which is the authoritative source of attributes (because of its close relationship with the citizen) and on the other end has a close contractual relationship which organizations, such as financial service institutions, to leverage their services. This, I think, makes the relationship one removed from what was originally envisioned as what is meant by an Identity Oracle. This was something that Nishant brought up after the session in a sidebar with Ian and Myself. I hope that there is further conversation on this topic about this.

My take away from this session was that there is value and a business need in the Government being an attribute provider, technical infrastructure is being put into place that could enable this, and while many issues regarding governance and quality of data still remains to be resolved, there is a marketplace and opportunity for Attribute Aggregators/Oracles that would like to participate in this emerging identity eco-system.

Raw notes from the session can be found here courtesy of Ian Glazer.

Notes from the "Government as Identity Oracle" session at IIW East
By Ian Glazer, on September 10th, 2010

These are my raw notes put here for reference purposes.

What is mean by identity oracle?
* An oracle provides an answer to a question but not a specific attribute
** If you ask an Oracle, is Peter over 21 it says yes. It does not hand back an attribute - birthdate

Peter: The Federal Govt is authoritative for very few attributes - State Dept - passport #, citizenship. State govt are authoritative for driver's license number. SSA for SSN.

eVerfify is an example of an oracle, says Gerry.

Peter - what will drive this is the requirement for LOA3 credentials needed to access to medical records.

P - "We do not have an attribute infrastructure." A lot of attributes are simply issued via IdP'

I - our examples so far have shown organizations that are authoritative for identifiers but not attributes

P - raises need for back end attribute exchange

Gerry - Problem with authoritative attribute provides is that the PDP makes a decision as to what is truly authoritative for a given context. Authoritative data source must provide SLA or MOU so that relying party can establish trust.

P - BAE is 1/2 of the equation and attribute provider (market?) is the other half

A - is there a business model for attribute providers?

G - have problems seeing attribute exchange at enterprise scale let alone government scale. Quality and availability are just some of the issues. Access decisions are fairly local and these decisions are not things that known often at the higher enterprise layer. Things are made authoritative by policy decision.

P - Second model for authoritative - a local decision to assign authoritative-ness to something

Nishant - should we get rid of the term authoritative?

Peter for sees multiple attribute providers having say over the same attribute for the same person

If I use an Oracle, do I have to know its sources? No, says Gerry, as you form an agreement with the Oracle ahead of time as to what happens when something goes wrong

P- I am running validation services which services 400 back-end apps. I am standing up a BAE to help. I could build that infrastructure or I could can contract out to an Oracle. The Oracle has to tell me its sources so I can make a decision to use it or not. Gerry comments that you may not want to know the Oracle's source of data.

Returning to the eVerify system - is a person allowed to work? eVerify doesn't disclose sources of info but DHS takes responsibility for its decisions.

Pam asks about redundancy of providers. Redundancy allows same decision to be made via separate paths.

Anil feels that there is a business case for multiple providers.

Mary raises the point that there are organizations who have a lot of data on people. These are often highly regulated organizations because they are related to financial services.

G - uses Health Vault and Google Health as an example of multiple providers of heath information data

A - Talked to financial roundtable - these ors not interested in B2C but very interested in B2B situations. Having the govt offering services to help vet people would be of great service.

Govt business for providing identity information? There are certainly companies that will aggregate public data for a fee. If a service provider helps get me as a business information I need to hire someone (citizenship for example), would I use it? Would I form a business to do this? N raises BT's You Are You service as an example of this.

Pam - talking about building cloud-services in this area. Definitely interest from small business for federation and using Google as authoritative source. Sees consumer-focused needs later down the road.

I ask P about persisting "over 18" information if it is acquitted from Equifax. P says they'd have to issues SORN and protect as PII.

I am curious about Govt as Oracle and the implications with respect to the Privacy Act. Peter wants to facilitate market for Oracles. NIH had MOU with InCommon which included use of attributes and information. This included agreed upon protections for those attributes which was coherent with InCommons users' requirements. Peter acknowledges this doesn't scale but he offers as a counterpoint that NIH is doing this federation to federation. He asserts there won't be that many to federate to.

I many not want to maintain a BAE with hundreds of connections to attribute providers. Likely outsource the work to an Oracle. "It is easier to affiliate with a hubs than it is affiliate with each provider," says Peter A.

Peter says that NIH sees need to handle attributes and thus NIH is setting up BAE. He acknowledges that there needs to be policy and practice around this, which Peter is on the hook to build. FICAM roadmap says that if you are standing up an attribute service it must be a BAE if you want funding.

G - If I am a BAE affiliate and I want to consume other affiliate's data, what is the quality I can expect? Anil says that this is currently being discussed amongst architecture groups. G talked about the quality within his organization. There is no strong commitment to the data that internal data collectors collect. At the end of the day if something goes wrong, is it my fault or someone else's. This is part of the contractual relationship between data consumer and provider.

Hold Harmless clause within MOUs used the by the PKI Bridge. So long as org is acting in accordance with their own policies then they are to be held harmless. G - in certain situations this works, but in others it does not. I might have to run my own infrastructure or shop for another provider who can back up their assertions.

Pam asks if this is govt to govt discussion, would a private group come in an provide services for G2G? Anil says yes and that currently this is happening.

Because there are so many million of high level of assurance credentials, one would think that someone would want to build an ecommerce infrastructure to consume these creds - says Peter.

Peter asserts authentication is a solved problem and next up is authorization, claims, roles, etc.

Every application owner want to maintain control over who comes into the app. But this a way that Peter gets people to plug into the federated SSO environment.

Are people building services to consider risk-based authorization in transaction, asks Pam. Anil mentions the consideration of environmental attributes for initial authorization. G says this is a hot space now. Anil brings up how PayPal takes a low assurance cred and uses it for financial transactions.

B2B & B2C: How to Balance the Differences and Challenges of Each Environment (T1B)

Convener: Rainer Hoerbe
Notes-taker(s): Gary Moore

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:

The discussion was based around how to create an environment to handle the complexities of dealing with business-citizen and business-business transactions.

From an Austrian perspective

- Internal govt federation program
- Had a unsuccessful national citizen PKI. Based national identity that is moving towards a SMS based solution but uptake still unknown
- Challenges - privacy
    - B2b privacy less important to ensure audit ability
    - B2c more important for privacy

NIH federation within US govt. starting with PIV. 80% of business is outside govt - currently Incommon to universities. NLM 15000 users - no cross correlation - authorization is delegated to relying party

NIH does not want to be in the business of a credential provider
In Austria centralized data allows higher assurance of identity - legislatively driven with benefit of small population - 8 million

NLM can use multiple LOA (levels of assurance) as well as multiple IDPs

There is a concern with Credential strength versus strength of identity proofing

Stepping up levels of assurance - how to do that?
- Use of organizations like Lexus, Axiom, Equifax for information that can better identify the user

NIH Delegates risk to the companies and universities that they are dealing with

How to manage the separation of attribute definitions - use a common data dictionary or create a mapping service?

Austrian view - NIST is concerned with providing identity to RP - Austrian concern adds on making sure info only goes to the user - European privacy legislation requirement

How do we come up with appropriate definitions of LOA - need better guidelines for the definitions.

Within NIH NLM program In common level 1-2, also using 3 and 4 through PKI as well as OpenID for level 1

How to create international common definitions of LOA? Companies like Paypal are global but definitions of LOA are currently environment specific

TSCP program to issue credentials to the machines that are assured to be trustworthy. In Austria a similar thing for web infrastructure elements. For TSCP they are extending that to leverage trusted platform to ensure long term proper configuration of the environment.

Proofing the Masses (T1C)

Convener: Vikas Mahajan
Notes-taker(s): Justin Tormey

A. Tags for the session - technology discussed/ideas considered:
Proof, verify, physical, trust, notary public, business model, market, audit

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

- Issue: How do we "proof" 300 million+ US Citizens?
    - Daunting task for any identity provider hoping to provide higher level of assurance
    - Some levels require physical inspection of documents
        - Process similar to getting a passport
        - Birth certificate, utility bill, tax information, etc.
- Example: Social Security Administration unable to handle flow of new requests coming in from baby boom generation.
    - Not enough office staff to handle the influx of new claims.
    - Can they off-load some of this to third-party sources?
- What's included in a Level 1 / 2/ 3 proof?
    - There are standards that exist, but they don't specify exact documents or requirements
    - Depends on the level of confidence the issuing party requires.
    - Some government agencies require physical document checks for "Level 2" for example, while the specification doesn't require those checks until "Level 4"
- Concept: Team of trained volunteers, like the AARP, perform certification
    - AARP already doing physical checks for some tax preparation services they provide for free
- Concept: Nearly everyone has a mobile phone, what if carriers could provide an authenticated identity?
    - Should there be a split between Identity Providers & Identity Proofing
    - There are many organizations, groups, companies, etc. that have some identity assets.
    - Companies could provide this data in an open market to Identity Providers
    - Who will consumers trust with their information?
        - Some organizations, like AARP or the Post Office have a perceived high degree of trustworthiness
- What's the business model for proofing?
    - Sell identity attributes and verified identities to Identity Providers

- There needs to be some risk management assessments done
  - Who is liable for bad information?
  - Proofing can be done for free or cheap with no liability implied
  - Pay for some degree of protection
- Audits need to be performed on a regular basis to ensure the proofing is high enough quality

NSTIC 101 (wtf?) (F1D)

Convener: Heather West & Jay Unger
Notes-taker(s): Joshua Gruenspecht

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:

Initial Discussion: Heather, Jay, Aaron Titus describe the process of the creation of the document to date. Created out of a White House policy review, intended to have the force of an executive directive. Authority derives from the executive order that created the review.

<Lots of cross-discussion about the probability that this is placed on the desk of the President and signed – general consensus from the parties to the talks to date that this will be done this year.>

What is the content?

Heather/Jay: Unclear. May include government access using third-party credentials, may include third-party access using government credentials. It's a very objectives-level document.

Will they be continuing to revise the document?

Aaron/Jim/Heather: Yes, although continued comment may not be welcome. They've been burned by the first round of comments through Ideascale. A lot of useless feedback, plus a lot of pushback from civil liberties groups.

Who's responsible for this document (and why aren't they here)?

Aaron/Heather: The Cybersecurity Office in the White House (and we tried!).

What changes can we expect?

Heather/Aaron: Probably fewer questionable examples full of hand-waving. Everything else is unclear.

What agency is likely to end up with the responsibility for this?

<Cross discussion about how none of the obvious choices (Justice, Homeland Security, Defense, the Post Office) look appetizing.>

Jens: I hear three possibilities: Homeland Security, GSA, Commerce (NIST).

Third parties and their responsibility

Aaron: Problem with third-party IdPs and data custodians as well – namely, ensuring that if third parties are used as parties in the transactions between citizens and government, that they don't then sell that data to others.
Jim/Heather: According to NSTIC, players in the ecosystem will be responsible for ensuring some (presumably low) level of privacy protection.

Is this a useful thing? What one change could make this more successful?

Nathan: There isn't one!
Jay: If this is a step toward the government taking an "encouragement" role, then that, at least, is a positive thing.
Heather: If the government is agreeing to be a relying party in transactions, that may be the very best thing that it can do.
Myisha: Just agreeing upon rules of the road to satisfy all the lawyers everywhere would be a big step.
<Cross-talk about liability for breach and allocation of risk>
Jim: Liability doesn't need to be limited, it needs to be allocated in the first place.
<Cross-talk between people who believe that NSTIC is at least a first step toward government reliance on a standardized ID system vs. those who believe that even if it is a first step, government moves so slowly that adoption is, at the least, years away>

More about liability

Jens: One real problem that this doesn't address is reputation loss – FDIC model for identity may not cut it.
<Cross-talk about assigning liaibility within the NSTIC framework>
Myisha: We may need multiple levels of reliability in ID provision so that we can have multiple levels of reliance, risk, and liability.
<Discussion of a "credit services" model (like Equifax, etc.) – liability of IdPs restricted to safe and secure storage and distribution of data – no liability for inaccuracies. This is popular with several attendees, and is proposed as one possibility that should be explored by the NSTIC authors>
<Discussion of what an IdP can do to prevent breach and what its liability would be in the event of breach. IdPs as the equivalent of banks vs. IdPs as credit services>
Jay: In order for this to work, there must be a business model that does not rely on the resale of people's information.
<Discussion of how to get such a model into the NSTIC>

Where is the money going to come from?

Nathan/Myisha/Jim/etc.: The key questions for government money are – Will this get into the 2012 budget? Will all, some, or none of the money requested make it in?

Jim/Jay: Then, we'd need to get into the business model questions – Can we tier by LOA?

What changes should we, the identity-interested community, request?

Jay: A clearer, shorter document with more participation.
Barb: Why don't we act as an advisory group?
Heather/Aaron: We can't, because of ethics rules, and they're receiving so much information anyway that they can't distinguish signal and noise. Plus, we're rushing toward their October deadline.

More Government Employees at IIW Next Time (T1E)

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

Tags for the session - technology discussed/ideas considered:

iiw-east, iiw.gov, branding, marketing, publicity, outreach

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

We started asking what we could do to bring more government employees into IIW-East. One state employee paid his own way and had to take vacation time to attend IIW.

The first tip was to frame IIW as training. Skill acquisition and development is more reimbursable and easier to fit into budgets.

Timing was problematic this time around. We didn't really benefit from O'Reilly's Gov 2.0 Conference attendees staying for a few more days. Labor Day weekend and Rosh Hashanah are real barriers.

We're not sure if IIW-East is a twice-a-year thing since the pace of government is so slow and the focus is on adopting and applying technology, not on defining it.

We considered the event focus. In a way it is too broad: an IIW narrowed to a specific department (DoD, HHS, etc.), or to a community of interest (like criminal justice) might make a series of internet identity workshops a hotter item.

We discussed promoting the next event by reaching out through the media read/seen by government IT/ID employees. We can share trends, themes, findings from this IIW as news/PR, demonstrating IIW is the place to be.

- There are many trade publications for defense, healthcare government IT, privacy, security.
- Dozens of Gov2.0 blogs, like TechPresident and Personal Democracy Forum
- Cybersecurity mailing lists and other mailing lists
- GovLoop – a social network

At the state level, we could be reaching out to IT architects. State legislatures in NY and VT are doing some interesting things.

Last, we talked about reaching out to the US Congress. Staffers will attend short briefings on the Hill but not leave for conversations like this. We'd be lucky to get one

or two and it might be worthwhile to invite the tech and transparency/accountability –minded.

PDX Ecosystem (T1F)

Convener: Austin Faith
Notes-taker(s): Barbara Bowen

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:

Purpose:

The goal of the Personal Data Exchange is to centralize and manage the data that is already being collected by proprietary services into one point of access for customer access and administration.

Points:

Common web api for service providers.
Trust is a fundamental factor.
Variety of choices in providers with common apis Control over real time aggregation with distribution rights management.
Use case model to alleviate and evaluate risk.
Complexity around PDX and link contracts.
Young people share information, they also value trust and privacy.

Problems:

Perception of risk across mesh.
Secure channel that avoids man in the middle attacks Identity online is fragmented.

Platforms:

Real tools exist and are being fully developed with Open Standards Encryption keys that are personally managed.
Terms of service accepted by vendor.
PDX hosted by service provider enabling Data Portability Unique customer identifier and peer to peer connections stay intact.
Higgins stack using rdf as demonstrated in the MyDex pilot XDI stack as shown at personaldatastore.info

High Assurance Consumer Identity (T1G)

Convener and Note-taker: Bob Pinheiro

Tags for the session - technology discussed/ideas considered:

Authentication, credentials, tokens, high assurance, trust frameworks, selectors, active clients, consumer identity

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

High value online services that involve financial transactions or payments, including the establishment of new high value relationships and accounts, are subject to a great deal of fraud. With the advent of electronic patient records and personal data stores, the opportunities for harm to consumers as a result of fraudulent access to sensitive information becomes even greater.

While consumers may not necessarily articulate a "need" to carry around hard tokens or other forms of high assurance identity credentials to deal with these problems, they would almost certainly state a need to prevent others from "stealing their identities" by breaking into their bank accounts, obtaining new credit cards in their name, or accessing other sensitive personal information. These needs can only be met when strong authentication technologies and "open identity" concepts can be combined to create high assurance consumer identity solutions in a way that is easy for consumers to use and understand, and that protects consumer's privacy as well.

The folllowing presentation outlines some the work undertaken by the Kantara Initiative's Consumer Identity Workgroup towards achieving these goals.

High Assurance Consumer Identity

IIW East, Washington DC

September 9-10, 2010

Consumer Identity Workgroup

Chair: Bob Pinheiro

consumerid@bobpinheiro.com

kantara INITIATIVE

The Problem

- Consumers are harmed if others can impersonate them for various purposes (financial, medical, etc) when sensitive personal information is stolen or misused to
  - establish **high value, identity-dependent services** such as credit cards, loans, cell phone accounts, etc.
  - obtain **unauthorized access to high value online resources** such as financial accounts, medical records, credit reports, etc
- Service providers are harmed and suffer losses (financial, reputational) if they provide high value services to those who claim a false identity.

Some Basic Assumptions

- High value services require (or should require) the Service Provider to have high assurance of a consumer's identity (or authorization status).
- High assurance ➔ FRAUD PREVENTION
  - Otherwise, just use low assurance, self-asserted identity or other claims
- An identity infrastructure should support high asssurance credentials /claims for high value services / transactions WHILE DISCOURAGING their use for low value services / transactions.

High Value Consumer Apps Where Identity Fraud Is Harmful

- Financial Services
  - New account opening
  - Access to existing online accounts
  - Transaction authorizations; ie, move money out of accts
  - Payments; e.g., credit card, debit, commercial payment services
- Healthcare
  - Access to patient health records or other patient-specfic healthcare portals
  - Impersonation of someone else to obtain medical services (Medical ID Theft)
- Government Interactions
  - Payment and reporting of taxes
  - Motor vehicle issues
- Credit Bureaus
  - Access to free online credit report
- Personal Data Stores
  - Access to personal data stores containing sensitive information
  - Authorized permissions for data access

Can Better Control of Personal Information Help?

Maybe, BUT

Service Providers offering high value services should not accept self-asserted personal information as "proof" of anything.

Service Providers really need high assurance of various kinds of consumer claims.

Consumers really need high assurance that false claims made by others using their personal information to obtain high value services will be rejected.

High Assurance of…… a consumer's identity

- Needed by Service Provider to prevent fraud when establishing new high value relationships or enrolling in high value accounts
- Requires identity assertion/verified claim from Identity Provider to Service Provider / Relying Party upon Consumer authentication to IdP

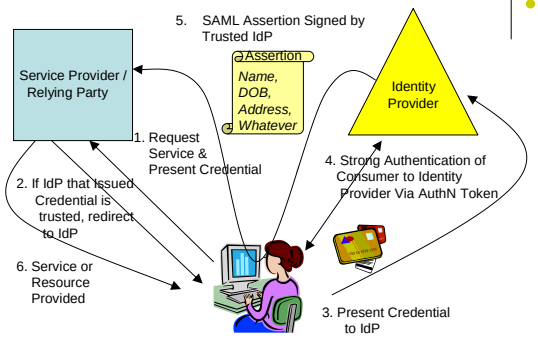
High Assurance of…….
authority to access a protected resource

- Needed by Service Provider to prevent fraudulent access to an online account or resource
- Requires EITHER:
  - Assertion/claim from an IdP verifying authN status
  - Strong credential / authN token bound to the resource; e.g.,
    - PKI cert/private key
    - Self-issued Information Card

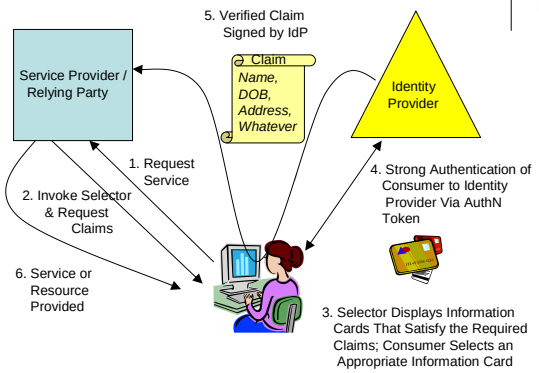
High Assurance of……..
authority to make an online payment

- Needed by online merchants to prevent fraudulent charges to a payment account that can result in a chargeback to merchant. For instance,
  - Credit card / debit card
  - Virtual "one time" credit card
  - Paypal
- Requires:
  - Assertion/claim from a cc issuer to merchant verifying authZ status after consumer authenticates to cc issuer
  - Assertion/claim from cc issuer to merchant containing virtual cc information
  - Strong authN token bound to payment account

Authentication of Consumer Claims
(via SAML Assertions)



Authentication of Consumer Claims
(via Managed Information Card)



National Strategy for Trusted Identities in Cyberspace

- US federal government's NSTIC initiative seeks to facilitate the creation of an identity "ecosystem" that can help to "*raise the level of trust associated with the identities of individuals, organizations, services, and devices involved in certain types of online transactions.*"
- CIWG seeks to help ensure that such an infrastructure can enable high assurance identity or other claims necessary to reduce fraudulent high value consumer transactions, in a way that
  - protects consumer privacy,
  - discourages demand for high assurance identity claims for low value transactions,
  - enables consumers to detect, and prevent, someone else from impersonating them in high value transactions.

Consumer Identity WG Goals

- Investigate open issues and provide specific recommendations to help ensure that an identity infrastructure enables
  - Service Providers / Relying Parties to authenticate, with high assurance, relevant claims about consumers to whom they provide high-value services, while protecting the consumer's privacy
  - Consumers to easily provide the minimal set of verified claims needed by SPs/RPs to enroll in, and use, high-value services
  - Consumers to prevent others from fraudulently impersonating them online in high value transactions
- Determine feasibility and understand what must happen in order to "roll out" this identity infrastructure and achieve widespread adoption by consumers.

Feasibility Depends On

- Whether **Service Providers / Relying Parties** will place a premium on minimizing fraud in connection with high-value services by demanding relevant high assurance consumer claims.
- Whether **Consumers** will perceive digital credentials and authentication methods needed for authentication of high assurance consumer claims as being easy to use.
- Whether **Identity Providers** that provide high assurance consumer claims can develop a business justification for doing so.
- Whether consumer **Privacy** can be protected
- Whether **Liability Issues** can be adequately addressed.

Open Issues in High Assurance Consumer Identity
Definition of "High Assurance"

- Current trust frameworks associate "high assurance" with knowledge of an individual's identity; *identity proofing*
- Need to redefine high assurance in terms of strong authentication coupled with rigorous verification of claims by an IdP.
- "High assurance" should also pertain to claims other than identity; ie, authorization to access a resource, claims based on other attributes such as age, membership, etc.

Open Issues in High Assurance Consumer Identity
Trust Frameworks and Claims

- Will different trust communities require different trust frameworks for supporting high value services offered by service providers in those communities?
  - Open Identity Exchange (OIX) is defining trust frameworks for different "trust communities" such as OCLC library, telecom, personal data stores, PBS public media
  - What about communities such as financial, healthcare, government, where high assurance is also important?
  - How will these trust frameworks be the same/different?
- Will different sets of claims be required by Service Providers operating in different trust communities?

Open Issues in High Assurance Consumer Identity Credentials & Tokens

- Distinguish “credentials” from “authentication tokens”
  - A credential presents a claim made by a consumer; e.g., personally identifiable information, a userID, X.509 certificate, Information Card, OpenID
  - An authentication token authenticates a credential; e.g., a password, shared secret, one-time password, X.509 private key, biometric
- Will separate credentials be needed by consumers for use within different trust communities?
- Who will provide high assurance credentials and tokens to consumers?
  - A consortium within each trust community?
  - Individual Identity Providers within each trust community?
  - State Motor Vehicle Bureaus?
  - Commercial Identity Providers; ie, Yahoo, Paypal, etc?

Open Issues in High Assurance Consumer Identity Digital Wallets / Selectors / Active Clients

- Should selectors / active clients be the default mode of deployment for high assurance online consumer credentials?
- Will consumers be able to keep and manage their various credentials using a single selector / active client?
- What are the issues and tradeoffs determining whether selectors / active clients should be deployed:
  - on the consumer’s PC or laptop or cell phone
  - “in the cloud”
  - on a portable physical device; ie, USB dongle
- Who will provide and setup these selectors / active clients on behalf of consumers?
  - Browser makers (as plug-ins)?
  - Identity Providers?
  - Consumers themselves?

Open Issues in High Assurance Consumer Identity Digital Wallets / Selectors / Active Clients

- What is the trust relationship between cloud-based selectors and Identity Providers?
  - Does the consumer use an authN token to authenticate to the selector for access to a credential, followed by an authentication assertion from the selector to the IdP for issuance of a verified claim,
    => IdP trusts Selector
  - Does the consumer authenticate separately to the selector and to the IdP
    => No trust relationship
- Trust relationship between cloud-based selector and Relying Party?

Open Issues in High Assurance Consumer Identity Portability of Authentication Tokens

- For credentials residing in cloud-based selectors / active clients, or on a consumer-owned device, where will authentication tokens needed to authenticate to Identity Providers reside in order to maintain portability?
  - Also on the mobile device?
  - USB dongle?
  - Somewhere else?

Open Issues in High Assurance Consumer Identity Does a High Assurance Claim Always Involve an Identity Provider?

- Yes, whenever a identity assertion or claim Is needed:
  - Subject is unknown to SP and seeks to establish a new high value, long-term relationship or account
  - Subject is unknown to SP, seeks no long-term relationship but wants a high value, identity-dependent service
- The need for such claims is likely to be infrequent.

Open Issues in High Assurance Consumer Identity Does a High Assurance Claim Always Involve an Identity Provider?

- Once a relationship/account is established, an authorization claim is needed to access or use the service.
  - Authorization claim/assertion from IdP based on authentication of consumer to the IdP via authN token **OR**
  - Localized challenge/response interaction between Service Provider and Consumer to demonstrate control of authN token.
- Since authZ claims are likely to be frequent, can the claim be authenticated without involving an IdP?
  - via PKI certificate or self-issued Information Card

Open Issues in High Assurance Consumer Identity Prevention of Identity Theft Based on Stolen PII

- Previous assumption is that all SP/RPs should rely on a high assurance identity claim/assertion from a trusted IdP when establishing high-value, identity dependent relationships. BUT this won't happen for a while if, ever.
- In the meantime, if an IdP within some trust community has issued you a credential/token, how can you prevent someone who has stolen your PII from claiming your identity?
  - Is there a way to discover if someone is using your PII?
- Possible role for Credit Reporting Agencies to notify credential holders when a SP requests a credit check based on PII for identification.

Open Issues in High Assurance Consumer Identity Privacy

- What are privacy requirements regarding consumer information retained by, or gathered by, entities within the trust framework (IdPs, SPs/RPs)?
- How can high assurance identity assertions be limited to certain types of high value applications involving financial transactions, access to healthcare records, etc?
  - Don't want to create a system whereby every Service Provider demands to know your identity

Open Issues in High Assurance Consumer Identity Stakeholder Roles

Who are the stakeholders and how would they benefit from this?

- Service Providers / Relying Parties
- Financial and healthcare consortia
- Identity theft prevention and assistance organizations, as well as other consumer advocacy organizations
- Identity Providers
- Strong authentication vendors
- US Federal Trade Commission & other government agencies

Thursday Session 2

Certifying Use Location for Politics Governance (T2A)

Convener: Britt Blaser and Lucas Cioffi
Notes-taker(s): Lucas Cioffi

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 difference between constituents and voters in politicians' minds.
- Citizens certified from a location can gain much more attention from a politician than if they are not.
- Advocacy groups want to certify that their members are in a politician's district so they can be heard better.
- Alcatel Lucent provides a way to certify a mobile phone's location
- Trufina has a way to verify a person's identity including their address
- NewGov uses credit card billing address to certify a user's address.
- There would be a need to certify location for each way that citizens contact their representatives, including mobile phones, email, faxes, and land line telephones.

Useability: Addressing the click – click –click problem (T2B)

Convener: Vikas Mahajan
Notes-taker(s): Vikas Mahajan

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

Usability

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

- Discussed the "conditioning" of users to click-through and ignore prompts and security screens. When instructions, warnings, Terms, etc., are constantly prompted for or given to you, they get "tuned out" and ignored because they effectively become a hindrance and stand between you and what it is you are trying to do.

- It's therefore important for user-centric identity solutions to avoid introducing barriers between the user what they are trying to do or the security/privacy protections will get ignored

- Avoid constantly prompting users about what data is to be sent and making them approve it. People EXPECT privacy as part of using the user-centric identity service, but that doesn't mean they want to be constantly asked or told about it and have to make decisions at each transaction.

- The organizations participating in the identity "ecosystem" all need to come up with some "agreement" or "bill-of-rights" or something that states all the orgnazations (ID proofers, IDPs, RPs, APs, etc) agree to data they will by default share or have access to, agree to only get the minimum data they need, and delete the data when asked to or when the user no longer belongs to that ecosystem.

- Consistent User Sign-on experience

- IT will be important to give users a consistent experience when signing in with user-centric idm ecosystems. IDPs must agree to some common and consistent experience so users can get conditioned to expecting that experience and can intuitively sense when something is different so it raises a concern to them (fraud detection).

- When users do need to agree to something, highlight those items in bold and make it in "plain English"

- Use a click box agree system rather than a scroll-through dialogue box since people are likely to blindly scroll through and ignore/bypass the important information.

- There will be important discussions to be had with web designers, marketing and product developers, since they may want to control the "look-and-feel" of the sign-on

process and UI elements, as well as use the user's data in ways that were not clear to the user

- Who can lead/drive the usability charge?
    - There are many people and groups interested in this, but no one seems to have stepped forward to say they will lead this effort
    - With such an impass, can the government step in and facilitate? NIST, maybe?

Leveraging Identity to Enable & Foster Scientific Collaboration (T2D)

Convener: Greg Haverkamp
Notes-taker(s): Greg Haverkamp

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

Saml,opened,vivo

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

3 attendees from 2 organizations.

Discussed LBNL directions and plans. Related those plans to what NIH is doing and has done. Includes a mix of SAML and OpenID, where appropriate; growth of RPs coming from benefits of earlier RP growth; etc.

Briefly discussed goals and state of DOE's Science Identity Federation

Identity & Cross Domain Systems (multilayer security) (T2C)

Convener: Jusin Richer and Gerald Beuchelt
Notes-taker(s): Gary Moore

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:

Mitre driven

Identity in cross-domain systems

Separate systems and networks with possible guards in between - how to go from low to high and vice versa - aka data leakage protection

Use a common low side for sharing info between systems - highly structured systems this may work but what of the environment when the system is unstructured

If on the high side and going down how does one go low and not exposed identity or the fact that they are on the high side

Is there a need to correlate identities on both sides? Maybe for security reasons?

Put mapping of identifiers in guard to allow either correlated mappings or total random IDs to the low end.

One idea is use a GUID at the guard to map identities on both ends to.

Identity is first step - then how to extend to authorization

Should We Create "Ownership Rights" in Law for Personal Data? (T2E)

Convener: Phil Wolff
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:

Personal Data Vision of Future: Video (T2F)

Convener: David Seigel
Notes-taker(s): David Seigel and Barbara Bowen

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:

At the IIW on Sept 8 in Washington, DC, I led a brief session on the vision for the personal data locker. I started by showing my video. We talked about various aspects of the PDL, and I showed on my blog a "bill of rights" for owners of future PDLs. I tried not to get sidetracked with technical issues, as I believe the big problems are in market adoption and trust, not technology. As I pointed out, what we need most at this point are standards for simple things like calendars and contacts. As the standards emerge, we'll be able to build more and more on them. And to whatever degree we need, we can use multiple APIs from companies that keep people's data today.

I'm allowing a small number of people to see my video. I don't want it getting out generally, but the identity community is more than welcome to see it. I make a living giving speeches, so I want it to be fresh for my audiences.

http://vimeo.com/14061238
Password: London (capital L)

It's okay to share with people in your immediate group but only a few people you know and trust.

For the full-screen version, click on the HD logo and then check that "Scaling is off" in the upper right corner.

If the password has changed, email me for the new one.

In addition, my book, Pull, is a guide to everything that's coming along with the personal data locker. My blog has more on recent developments and plans for the personal data store:

http://thepowerofpull.com

Here is the keynote speech I gave to the semantic tech conference in september:

http://vimeo.com/13942000 - feel free to share this link with anyone.

Notes by Barbara Bowen

Purpose:

The goal of the Personal Data Locker is to store personal information in one place, integrate with services, and share with settings. David Siegel is working on a business model to support the ————————————design of Personal Data Lockers.

Points:

Open standards
Ease of use
Cloud based information syndication
Data on cloud, not device
Internet of things
Collection of records with permissions
Move my account button will be in demand by customers.
Calendar, contacts, and groups are early format use cases.
Applications will be highly standardized.

Problems:

What are incentives for vendors to transfer data?
User interface design is challenging.

Platforms and Examples:

CommonApp.org
Mozilla Tab Candy example
Plaxo as model web wide
Do for data what Diaspora does for messaging

Attributes Claims – Identify Attributes LOA (T2G)

Convener: David Wasley
Notes-taker(s): Heather West

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

LOA, attribute, interoperability, credential exchange, federation

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

Levels of assurance are largely applied to identifiers or individual credentials/transactions, but do not translate well to a more complicated vision of identity within context.

Is identity LOA distinct from credential LOA? Should attributes have an LOA? Is there a difference between aggregated data or aquired data from a source of authority?

Is identity the complete picture? Knowing everything about a person at all times?

Is LOA even the right terminology for attributes? Maybe it's LOA that the attribute is coming from a trusted source?

There are three axes based on strenght of each: credential bound to a specific individual, greater privacy, attribute assurance. Where should certain kinds of transactions fall?
What kinds of levels should be necessary for permissions?

A number of example setups were discussed.
Credential LOA is mostyly about tech – what does id proofing add? What part of that is meaningful to an RP?

STORK defines identity – in the levels of assurance. Does 800.63 – only covers the identity elements, not much about proofing otuside preventing fraud.
The bottom line for attributes is what the IdP knows and how well they know it.

Aggreation of data or a source of authority? How do you ensure that IdPs trust SOAs? Certification?

Do we expect RPs to chase down each attribute? It doesn't scale to connect the data provenince and expect everyone to care. You can pass around that signed object, or you can ask everyone to go retrieve it each time.

How can you represent LOA for identity – metric for assertion as a whole? Groups of attrbutes? Weakest assertion? Per-attribute?

TFP doesn't deal with attributes, on purpose. Always been RP's problem, but this is inhibiting the big bang we're looking for.

Data quality is the real challenge in the real world.

Access management decisions aren't made with real names – it's abstract identifiers, personalization decisions, life history, eligibility attributes...
Attribute TF is different than an assurance TF. We don't have a great set of terms for this.

Thursday Session 3

Are Mediation Tools Useful in Authentication? (T3A)

Convener: Phillip Clement
Notes-taker(s): Pamela Dingle

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:

Open Identity for Closed Government: NSTIC the Cybersecurity Answer? (T3B)

Convener: Joshua Gruenspecht
Notes-taker(s): Heather West

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

Security, NSTIC, us-government, cybersecurity

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

NSTIC came out of the national cybersecurity review, in part in order to improve cybersecurity; however, the document that is circulated publically is largely for open governent and for consumer facing transaction. Can this "open identity" be useful for "closed government" – that is, for securing high level targets, etc.

Make this work for secure credentials with strong identity – anonymous, verified online voting? Secure electronic access is the same across sectors. What this example includes is the privacy requirements inherent in our voting system.

How can we solve the security problem? Without solving that, and moving beyond LOA 1, this won't get anywhere. Now, most things are closed and black boxes for the consumers. NSTIC at least presents the challenge and is trying to put together a framework.

How do we manage liability and indemnity for the consumer, the business, the IdP, the government? How do we harmonize security and privacy in a secure, government system?

What is the similar model in government? Security clearances that will be mutually accepted at given LOAs are the key here.

Do we want a DoD credential to sign us into Gmail? There's little hope in the near future of loggin in to secure DoD systems ith a gmail credential – and that's not a bad t hing. Low assurance transactions need to be more friction free, and use that learning process to move towards easiler high level assurance.

What kinds of trust are involved in a transaction where the government is a RP at a high level of assurance?

Implementing agency shoudl ensur that NSTIC is not just about creating a universal set of credentials with the government as a viable RP, in soe cases the governmnet should

be accepting third party credentials even at higher LOAs. This will seed third party LOA world with people that are doing this.

Also encourage more gov R&D – or SOME R&D - at the creation of hardware for use in abstracting identity from individuals. This needs to be trusted by government, but not necessarily government run/sponsored.

What Does 'Protect Your Privacy' Mean? In Government – Industry – Retail vs Wholesale Privacy (T3C)

Convener: Aaron Titus
Notes-taker(s): Aaron Titus

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:

The meeting was relatively short because we were outside in the sun. The question, "What does 'we will do [something] in a manner that protects your privacy'" has no universal answer, except that the enterprise writing the privacy policy will reserve all available rights for themselves. In the United States, this means that privacy policies can become little more than a placebo, and give users a false sense of security.

Building Standards for "Trustable" ID Providers (T3D)

Session: Day – Number - Space Location Thu 9/9 - 3 - D

Convener: Jay Unger
Notes-taker(s): Jay Unger

Attendees:

Name	Affiliation
Ty Stahl	Oracle
Barb Flanagan	Trufina
Jay Unger	Independent Consultant

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

OpenID, Identity Provider, Trust, Limited Authority Stroage, Trusted Computing

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

There being only 3 attendees including the facilitator this session was more of discussion about various "trust" issues associated with identity.

The session was opened with a discussion by the facilitator of his desire to find a technical means for building an ID Provider that could be trusted by users with their identity attributes because the mechanisms used to store, maintain and present those attributes fundamentally protected the attribute data from disclosure to anyone (even the IdP) without expressed permission from the user.

The facilitator asserted that mechanism like "least authority" storage systems and "trusted computing" could be used to create an implementation where stored attributes could only be accessed by a relying party that the user designated and only then with appropriate decryption keys supplied by the user.

The representative from Trufina described that systems role as both an attribute provider and attribute proofing service that uses third party data and means to verify and vet attributes originally asserted by the user. We also briefly discussed the "liability" model associated with an attribute provider and proofing service attesting that attributes "vetted" using third party data carried.

Liability and Financial models for Identity Providers, Attribute Providers and Identity Proofers (T3E)

Convener: Brian Kelly
Notes-taker(s): Brian Kelly

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:

- Who is responsible?
- Who pays?
- How much?

About a dozen people gathered to discuss the "L" word that has been omitted from many of the NSTIC and Trust Framework Provider documents and discussions – Liability. The first point raised was that we need to define what type of liability we are discussing and between whom.
Liability between

1. Identity Provider (IdP) and Relying Party (RP)?
2. User and IdP?
3. User and RP?
4. Trust Framework Provider (TFP) and IdP?
5. TFP and RP?

Attribute Providers and Identity Proofers also belong in this mix, but we lumped them into IdP for sake of the discussion.
These are all areas where liability may be carried. Liability and risk current shift around from user to RP to IDP to TFPs. But who is really responsible?
The concept of an "Identity FDIC" was raised, but not tackled.
The conversation then shifted to the question of "who polices the system?"
e.g. During an audit, an IdP gets kicked off the TFP whitelist for behaving badly.

- How does this affect users of that IdP?
- And more importantly, how does it affect the RPs that those users expect to access?

We also discussed how some RPs may **require** an IdP or a set of IdPs to access the RPs resources. There would be no alternative way to access the RP (e.g. StackOverflow **requires** an OpenID to sign-up; Airlines **require** a credit card to pay for food/drink while in flight).
This raises the trust that RPs and users are putting into an IdP and magnifies the liability on that IdP. There is one area where this will be protected: Citizen to Government – Government must always provide another way to access their services – even offline. Maybe government will always offer a username and password option. It's debatable.
The conversation then shifted into the financial discussion.

- RP pays the IdP
- User pays the IdP
- IdP offers a substantial cost savings / convenience to the user or IdP

Think about a bank as an IdP or Attribute Provider (AP) that could offer its service as a value-add to its existing (vetted) customers.
Someone mentioned that putting a “Fair Credit Reporting Act” in place for IdPs before critical mass of RPs is achieved might kill the “Identity Big Bang”.
** RP adoption driver: **lower fraud by outsourcing account sign-up / identity vetting**
- RP can take away risk from themselves by outsourcing to IdP

RP growth drives the market -> Not IdPs or TFPs or APs.
Government has the capability to bootstrap the RP adoption process and get the ball rolling.

Personal Data Stores and Context Automation (T3F)

Convener: Phil Windley
Notes-taker(s): Phil Windley – Blog Post

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

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

http://www.windley.com/archives/2010/09/pdx_principles.shtml

There was a lot of discussion around Personal Data Stores (PDS) and Personal Data Lockers at IIW East. Every time slot on both days had at least one and sometimes two sessions on the subject. (As an aside, if you're not familiar with IIW, the agenda is created in real time, by the participants, not months in advance by a program committee, so it represents more fully the interests of the participants than a normal conference aganda might.) I'm confident that this will also be a major theme at the upcoming IIW in Mountain View CA in November.

The term itself is a problem. When you say "store" or "locker" people assume that this is a place to put things (not surprisingly). While there will certainly be data stored in the PDS, that really misses it's primary purposes: acting as a broker for all the data you've got stored all over the place and managing the metadata about that data. That is, it ***is a single place***, but a place of indirection not storage. The PDS is the place where services that need access to your data will come for permission, metadata, and location. Similarly for services that need to give you data. Consequently, some have taken to calling it a PDX, where "x" stands for the "variable x." That is, we don't know what to call the last thing, so we'll say "x" and leave it at that.

In the discussions, I started to tease out a few principles that define the PDX and make it something different from just a database where my stuff is. We all have lots of places where data about us is stored and since it's personal data, we might think of them as "personal data stores" but when people at IIW (and elsewhere) use the term, they're talking about something larger and more capable that just a passive database. Here's a list of a few things that I think distinguish a PDX from just places where your personal data is stored:

- **user-controlled** - the user needs to be in control of the data, who has access, and how it is used. Once that data is in my PDX, I make decisions about it. That doesn't mean the data might not also be somewhere else. For example, data about my purchases from Amazon will certainly be stored at Amazon and not

under my control. But I might also be emailing the receipts to a service that parses them and puts the data in my PDX for my use.

- **federated** - there isn't one place where your data is stored, but multiple places that the data needs to be able to flow between, in a permissioned way. There's no center, just a lot of cooperating system with my PDX orchestrating the interactions. While Amazon might not give my PDX access to and control over my transactions, my phone company might provide a PDX-capable contact service where I choose to store my contact information.
- **interoperable** - various PDX services and brokers have to be able to operate together according to standards to perform their roles. When I take money out of my account at Wells Fargo and deposit it at Chase, I don't lose part of the value because Chase doesn't know how to handle some part of the transaction. The monetary system is interoperable with standards and, sometimes, shims that connect it all together.
- **semantic** - a PDX knows more about the data that it holds than existing data stores do. Consider Dropbox. I can put all kinds of things in my Dropbox, but it's syntactic, not semantic. By that I mean that if I want to put healthcare data in Dropbox and control who uses it, I create a folder and put the data in it with specific permissions. The fact that there is a folder with a certain name located at a particular place in the folder hierarchy is purely syntactic. In a semantic world, the data itself is tagged as healthcare data and no matter where it is, it's protected according to the policies I've put in place.
- **portability** - a PDX doesn't trap data in proprietary formats. If my phone company is storing my contact data in the cloud and I decide that I want to move it to my own server or another service, I can—from a technical as well as a policy standpoint. Note that this doesn't mean we have to wait until thousands upon thousands of data format specification get hammered out. Semantic metadata can provide a means of translating from one format to another.
- **metadata management** - one of the primary roles of the PDX is managing data about my data. What are the roles I've created? What permissions have I granted as exceptions to the defaults? What semantics surround the various data fields? What data sharing, encoding, and encrypting policies have I created? All of this has to be kept and managed in my behalf in the PDX.
- **broker services** - the PDX is a place where the user manages a federated network of data stores. As an example of why this is important, consider the shortcomings of OAuth. If I use an application that needs access to four OAuth mediated APIs, I have to go through the OAuth ceremnoy with each API provider separately. Now consider that I might have dozens of apps that use a popular API. I have to go through the OAuth ceremony for each of them separately. In short a broker saves us from the N x M explosion of permissioning ceremonies. Similarly for various data services.
- **discoverable** - a PDX should provide discoverability for its APIs and schemas so that any application I'm interested in knows how to interact with it. Discoverability protects users from having to completely specify addresses, mappings, and schemas to every application that comes along.

- **automatable and scriptable** - a PDX without automation is worse than no PDX at all because it burdens the user rather than saving effort. A PDX will be a player in a larger ecosystem of services. I don't see is as a mere API that allows services and applications to GET and PUT data—it's not WEBDAV on steoids. The PDX is an active participant in the greater ecosystem of services that are cooperating on the user's behalf.

Surely I've missed some, but this list is a good start. What would you add?

Update: Kaliya wrote up a vision and principles document for personal data stores a month ago. Not surprising to people who know us both, they differ radically in perspective, but are coherent in spirit.

Patient Centric Medical Record Federation – Securing HData (T3D)

Convener: Justin Richter & Gerald Beuchelt
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:

How to Make HTTP Authentication Useful Again? (T3H)

Convener: Yutaka Oiwa
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:

Thursday Session 4

PRIVACY – Did We Solve Privacy for Web Identity Systems (technically already?) (T4A)

Convener: HannesTschofenig
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:

Personal Data Store/Archive (T4C)

Convener: Terrell Russell
Notes-taker(s): Barbara Bowen

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:

Purpose:

Personal Data Stores exchange and aggregate attributes with persistent systems and terms of service. Realigns difficult questions around privacy and consent.

Points:

Vendor neutral packaging
Structural leverage with portable data and rights through link contracts.
Profiles, facets, and roles are established within a container.
Groups create context.
Authentication with an attribute store.
Aggregation and merging of data from several sources is a problem which requires relying providers.

Platforms and Examples:

XRI is a standardized graph model that establishes structure and context through dictionaries.
Inames are identifiers that are a format for the construction of privacy.
The Mine project and XDI examples.
Telcos may offer data stores with replication in the cloud.

Service Chaining and Trust (T4D)

Convener: Gerald Beuchelt
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:

Extending OpenID Assertions with SAML+ (T4E)

Convener: Jay Unger
Notes-taker(s): Jay Unger

Attendees:

Greg Haverkamp	LBNL
Justin Richer	Mitre
Michael Barnes	PWC
David Dove	Judicial / CT
Zhihong Zhang	AOL
Nishant Kausmik	Oracle
Pamela Dingle	Ping Identity
Joel Schnee	AOL
Jay Unger	Independent Consultant

Tags for the session - technology discussed/ideas considered:

Attributes, SAML, OpenID extensions, OAuth extensions

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

The session was scheduled to discuss what is being or might be done to provide a more comprehensive and robust attribute capability for OpenID.

Began with a statement of requirement for more comprehensive capabilities than are now included in OpenID Attribute Exchange Extension which currently supports a simple gets/sets model for textual attribute/value pairs.

Discussed required additional attribute capabilities including: content rules, typing, usage restrictions and some sort of attribute provenance and dependency information carried along with the attribute expression. Provenance information should include information about both the source of the information (attribute provider) and the methods used for proofing/vetting the accuracy and authority of the assertion. Dependency information should explicit call out what other attributes were depended upon as pre-cursor to an attribute.

The use of SAML Attribute assertions (with extensions to support provenance and dependency information) was briefly discussed in the context of possible extensions to OpenID.

Several participants offered that there are a few other mechanisms that can be integrated with OpenID Authentication that provide some additional functionality:

Another OpenID extension called Artifact Binding (http://wiki.openid.net/OpenIDwithArtifactBinding) was mentioned as means for supporting a attribute exchange that contains a large set (perhaps all) of the attribute associate with an authenticated claimant.

OAuth 2.0 was also mentioned as a means for extending OpenID and was cited as a general direction for extension of OpenID. OAuth provides a mechanism for out-of-band site to site authorization and data access using bearer tokens.

UMA – User Managed Access (part of the Kantara initiative) was also referenced as protocol for user-centric management of attribute (and services) access.

Webfinger was also mentioned as a means for discovering the IdP (or perhaps other service provider) that a users has affiliated with.

In addition to these discussions there was a conversation about why several of the larger OpenID providers like AOL, Yahoo, Google etc. were presently not also operating as relying parties (RP) and allowing users to authenticate to their primary services (like AOL or Google mail) using another Identity Provider. The primary reason given was lack of any business incentive for these services to do this as it would in some way be viewed as ceding “ownership” of the user to another competing service. A representative from AOL stated that the technical means to do this had been implemented but not offered (at least not easily visible) because of this business concern. Others opined that some of the larger OpenID providers certain DID or were planning to act as RPs and permit “foreign” authentication transactions.

The discussion was a generally useful information and idea exchange.

NSTIC – "Identity Ecosystem" (T4F)

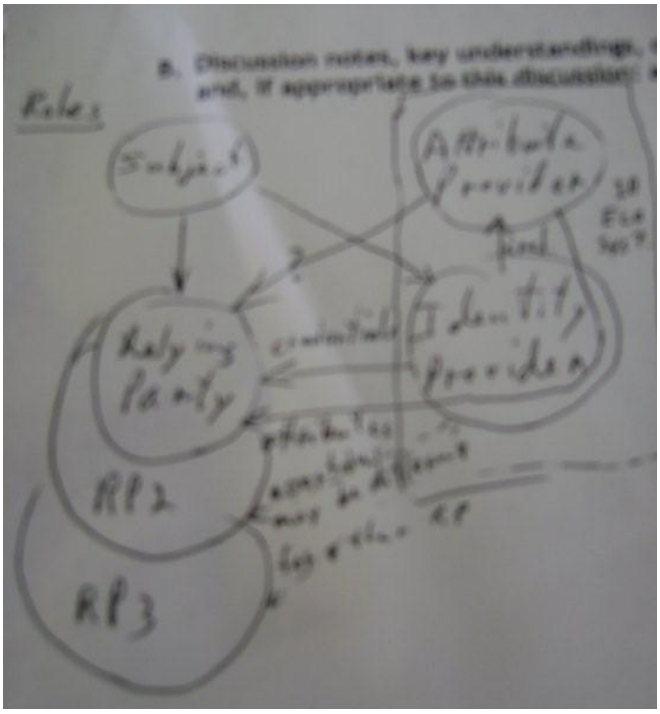
Convener: Jim Fenton
Notes-taker(s): Bill Braithwaite

Tags for the session - technology discussed/ideas considered:

NSTIC, Identity Ecosystem, Identity Provider, Attribute Provider

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

Jim described his concept of what was meant by the "Identity Ecosystem" in the June 2010 report on a "National Strategy for Trusted Identities in Cyberspace (NSTIC)". He drew this diagram of the roles and their relationships:



The box in the diagram represents the identity ecosystem and includes APs and IdPs. The assertions of attributes about the subject required by the RP may be delivered through the IdP or in some cases directly from the AP. Different RPs may require different assertions about the same subject.

The discussion revolved around the trust relationships necessary for this system to work. Attribute Providers (AP) must be trusted by Identity Providers (IdP). Examples of trusted APs included Bank, College, Credit Bureau, and Employer.

Identity Providers must be trusted by the subject, and in at least some cases by the Relying Party (RP). Examples of trusted IdPs included: Credit Bureau, Post Office, Fedex/SPS, PayPal, AARP, and Banks.

Cross Federation Trust w/Meta Data(T4G)

Convener: John Bradley
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:

Friday September 10,2010

Friday Session 1

OAUTH – What Topics Should We Focus on Next? (F1A)

Convener: HannesTschofenig
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:

Liability for Idps, APs, RPs… Continued (F1D)

Convener: Brian Kelly <brian_kelly@symantec.com>
Notes-taker(s): Myisha Frazier-McElveen <myisha.frazier-mcelveen@truestonefed.com>

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 grabbed a larger room this morning to continue our discussion on liability and financial models for IdPs and RPs. We were fortunate to have a number of lawyers joining the conversation as we all learned about how to get to the root of solving the liability issue. Scott David (K+L Gates) took us all through a whirlwind applied law lesson that was very helpful in giving this mixed audience a new way of thinking about the real legal problems.

Session Highlights

- The American Bar Association (ABA) has started a workgroup that is addressing Liability issues (Led by Tom Smedinghoff)
  - Scott David wrote a draft document to help define how to think about the **duties** of the various parties (IdP, RP, User, 4th party–AP) in the identity ecosystem so that we can accomplish the goal:
  - **Curb discretion to make the entire system more reliable and more interoperable.**
    ("program people" to act in the best way that benefits everyone in the system.)
  - The biggest risks are on the edge of the system. E.g. Credit Card companies put a $50 liability on the consumers on the edges.
  - **Tools & Rules: It's a 50/50 split** to have a successful system.
- ABA draft materials
  - Similar to the terms sheet but a three way agreements
    - The agreements are not bi-lateral but rather multi party in nature.
  - Find the low hanging fruit of duties to standardize in a legal spec. **Defining the duties of each party in the system is the key place to start.**
    - **Level Of Assurance (LoA)** – Based on NIST SP 800-63 and OMB M-04-04 (1-4)
    - **Level Of Protection (LoP)** – Third party data theft (e.g. leaky pipes) – Protection of data (e.g. HIPAA)
      - Where this falls on the four parties is TBD
      - Identifying duties associated with preventing third parties from getting access to the data is currently being defined.
      - Data duty: transfer of data, holding of data

- **Level Of Control (LoC)** – Provides protection for 1st party unauthorized use.
  - Use fair information practice principles (FIPPs)

- **There are different sets of duties for different trust communities.**
- Source of duties: Law, Contracts
- Start with *background law* and work to achieve *contract law*.
- The Trust Frameworks fill in the gaps from the duties identified from the legal spec.
  - Creating the legal spec floor upon which trust frameworks can build based on specific requirements of each trust framework.
  - Attribute Providers would fall under the scope of the trust frameworks as part of the gaps from the duties.
- The goal is to curb human discretion to increase reliability and interoperability.
- Other terms: causation, duty, breach, damage

Notes from earlier in the session

- NSTIC references that liability needs to be addressed potentially utilizing insurance to mitigate the liability issue – but doesn't go any further than that (today).
- Is the FDIC Model for liability applicable to identity?
  - Would Trust Framework Providers put the money into the identity FDIC
  - Utilizing this model includes and underlying assumption that there is government regulation over the identity space (as what is done in the financial space).
  - This model may not be able to deal with redress for end user
    - If the IDP goes down (like with a bank) how do you deal with the end users loss
    - Model may be good for catastrophic system failure but not good for individual end user re-dress
- Issues that could arise
  - Data breach
  - ID provider hands out misleading attributes
  - ID Theft
  - Liability of a relying party transferring information outside the transaction
  - RP reveals information to the wrong end user.
- Claimed ID Portability
  - What happens if an IDP goes down:
    - How portable are those identities?
    - Or should they even be portable?
- In order to address liability, we need to examine each entity in the transaction and understand their drivers.
- Liability – a duty that's breached, with causation and damage.
  - What do we want these systems to do?
  - What do we want to have happen?
  - Identify the duty
    - How was the duty breached?

- Who caused it?
- What are the damages?
- Liability is the end result.

❖ Are there other models that would work?
  - ➢ E.g. No Fault Auto Insurance

Getting More .gov @ IIW (F1E)

Convener: Phil Wolff
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:

Identity Commons "3.0" Big Tent Creation (F1F)

Convener: Kaliya Hamlin
Notes-taker(s): Drummond Reed

Tags for the session - technology discussed/ideas considered:

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

ATTENDING

Julie Fung
Don Thibeau - OpenID Foundation and Open Identity Exchange
Joni Brennan - Kantara
David Wasley - InCommon
Paul Trevithick - Interested in the cross-tribe conversation
John Bradley - Co-chair of one of the current IC workgroups (OSIS)
Barbara Bowen - Designer/developer/marketing - interested in the big tent
Mary Ruddy - Current chair of Identity Commons
Austin Fath - Interested in clearer picture of the space
Ian Glaser - Gartner, wants to see what the new scorecard will look like
Trent Adams - ISOC - wants to learn about 3.0
Ankit Kapasi - Consultant, working with fed/state/local governments, wants to give them the best options about how to get citizens on their networks
Bill Braithwaite - Physician, also known as "Dr. HIPPA", working with a
Phil Windley - Wants to see IC stop suffering and grow to the next level
Drummond Reed - ICF, OASIS XRI and XDI, wants to see what third generation looks like
Kaliya - has been working with IC for a long time, wants to see how IC can be more effective
Lark Allen - Wave Systems, wants to see how level 2 and 3 authentication fit into open identity
Rainer - interested in how existing federations fit into a larger picture
Charles Andres - wants to see how the next generation will work
Tony Nadalin

Identity Commons (IC) today is a loose affiliation of different organizations and workgroups.

Mary summarized the impetus for this conversation:

1. ÂÂÂÂ Some of its member groups/orgs or prospective member groups/orgs are at inflection points.

2. Some of the funders of those groups/orgs are interested in simpler funding model, lower overhead, and greater cooperation/synergy.
3. There is a desire for a more comprehensive international involvement/coverage.
4. There is a desire to simplify messaging and confusion in the market.

Other observations about motivations:

- Consolidated/coordinated messaging.
- Eliminate duplication
- Expand coverage to other groups/bodies that are not currently touched upon/coordinated with
- Have a clearer answer about who should talk to who about what
- More curation

Joni observed that Kantara has also evolved a long ways.

Tony observed that there has not been much "action" coming out of some of the orgs, i.e., actual specs and real positive initiatives. So right now they are not perceived as being a good return on investment.

Tony used the analogy of a "hotel" where there is a known set of facilities for supporting collaboration, but each group can set up their own particular meeting space and agenda.

Tony does not believe it should become a standards body -- there are already enough of those. Joni pointed out that Kantara agrees with this and that Kantara WGs are not intended to be SDOs.

Don believes that the IC3 proposal has merit -- it needs to be fleshed out. But he wants to find out who are the other companies who are interested, and how interested, i.e., at one level of funding.

Trent's perspective from an ISOC standpoint is to ask more questions about the hotel concept, and drill down into the specifics about issues like IPR. Is it really just about "paint, power, pipe"? Optics are important.

Kaliya feels there are some core functions that IC3 needs to offer that at its "core" that are should not be optional functions.

Kaliya said another key concept is to have Focus Areas that allow groups to cluster. Ian agreed, pointing out areas like health care, smart grid, etc.

Trent mentioned that IC3 might want to consider becoming a grant funding target as that would attract different groups that either are seeking funding or that want to provide funding.

Lark offered the analogy of it becoming the "United Way for identity".

Drummond suggested it would be ideal to do a bullet point of the deltas between IC2 and IC3.

We discussed the following concrete next steps:

1. Write up a specific proposal for IC3: Mary, Kaliya, Drummond.
2. Determine the actual companies who are interested in funding: Mary, Kaliya, Drummond.
3. Have a discussion with ISOC about cooperationâ€”Trent will be point.
4. Have a discussion with Kantara about cooperationâ€”Joni will be point.
5. Have a discussion with Gartnerâ€”Ian Glazer will be point.
6. Determine if there are funders willing to fund the legal/accounting work necessary for the transitionâ€”Mary and Kaliya.
7. Put the proposal to IC2 Stewards for approval actionâ€”Mary and Kaliya.
8. Open the new entity to funders and participating WGs.

Friday Session 2

Government Relationship Management (F2A)

Convener: Britt Blaser, Lucas Cioffi, Zack Brisson
Notes-taker(s): Lucan Cioffi

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:

- Government agencies often collect feedback from the public; usually when they take comments to comply with a regulatory requirement.
- Most opportunities for commenting are highly technical and are not interesting to the average citizen, however there are many more capable citizens that would want to comment if the knew there was an opportunity for them to do so. Lobbyists are often the ones who participate most in these commenting opportunities.
- Commenting would be more useful to politicians if they knew a citizen was certified as their constituent.
- Commenting would be more useful to government agencies if the agency could track a persistent pseudonym and see the quality of the citizen's comments over time.
- Often there are comments left across the social web that would inform agencies decisions, but it's neither easy for agencies to find most of these comments or to make sense of them.
- iTrust at NIH fits squarely in this space and offers promise as a solution.
- NewGov.us is working to create a place

Enterprise Open ID (F2E)

Convener: Justin Richer
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:

Identity in the Browser (F2C)

Convener: Paul Trevithick
Notes-taker(s): Charles Andres
attendees: Phil Windley
Jay Unger
Barbara Trufia
David Wolsey
Phil Wolff
Austin Fath
Rainer
8 others

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:

set of ID solns with lots of real world analogies to anonymous wallet
- credentials
- digital cash
etc.
necessary part of constellation:
- addressy
-money
- group affil

how to shift th max power to the control of the indiv.

zero knowledge proof tech
vapor trail
cookie trail

active client
smarter browser
endless digital baptism

form fillng
password

openID
SAML
ICF
- dif challenges - RP site - pick from
NASCAR popups

Dave Recordon of FBook
- tests state that if advice that some popup would release info, open to FB?
FB level of consumer trust in the cecision is fairly low.
a statement by your browser is highly trusted...

takeaway: role of infastructure that completely control
browser is the agent for the user

FB: consider the source.

selecors: AIR, etc.
popups - use notice of consent tranpsarenc

2 windows become annoyance.

a barier with what we are trying to do.

the UX must become much more sophisticated.

credit card analogy -- compelling
a 4 party agreement
lots of protection are happening behind your back

we were naive how people interact with computer systems

you don't think about airbag technology

signals have to be simple
uptake in EV signals because it is simple.
green bar;
simple signal, simple behavior.

radio button, checkbox is beyond simple signals and simple behavior.
Google also has similar studies -- UN/PW is as complex as people can deal with.

Browser, tc. is a great place to make simple secure private work.

how to do this in an inclusive way?
it has to embrace every protocol with traction
the consumer don't care
prtocols must disappear

How does a human login to a website across protocols?

pick an IdP.

design can't be implemented tech doesn't exist.

browser is not on phones but there is a user agent

user agent determines look and feeluilt in standard response
don't do it with questionable javascript
identiriers are a kind of claim.
10 years ago browsers b

basic authentication came from IETF
little progress since then

could start with ID Commons, but need to connect with IETF
and how about W3C
the ID space is so balkanized. but if there were one place --html, browsers, & ID

Jay: aftarid of constitutional monarchy

IETF more like a

if std and practice appear perhaps the IE logjam can be broken.

health care -- lot of info going into this 45K per doctor, $22B

could gov + healthcare drive this?

Federate authentication would help-

Dont forget your role as a procurement

$20M invested in ID space
real customer
real use case
real money

best bet = Mozilla
size of Firefox and IE are huge
tag candy was even worse.

can we put info in the communication stack?
- smaller certifable trustable

should we fix https at the same time?

tinest change in the broswer; do the service elsewhere.

similar to STSou what Dale did for Mac for i-cards
running process in theuser space has security probs.
Windiows did it outside user space
or in the hardware.

yyou canif't experss simple signals without chagnig user interaction.

if the production comes from depths of comm stack, its a lot harder to screw up
anti-virus software - keep me safe, don't talk to me about it.

M$, Androic, Firefox
- devolving to open components

always have the issue of dumb environment, kiosk, school computer, etc.
gotta get in and do something.

another mistake: work in a non modified airport kiosk.

red laser id scan???

openID knew a tiny bit of broswers (and tell the RP)
set the home page to the iGoogle page, and login.

Friday Session 3

“Today Geekdom, Tomorrow the World” (F3B)

Convener: Wayne Burke
Notes-taker(s): Wayne Burke

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:

Background:

Putting together an association of vendors & developers in the citizen engagement space. Nobody knows what to do with Identity - voter registration, constitnuent Identification, etc.

Identity has its own language and acronyms, etc., how do we describe the problems, the products, the solutions, to people who are not "in the know".

Vendors who sell to congressional offices, sell to advocacy groups, growing market for "citizenspace" products, ways for citizens to connect to elected officials, advocacy groups, etc.

What problem are we trying to solve? Identifying messages from constituents, because these are relevant/valuable, verification of Identity might amplify the message. They "get" that this is important, but they don't know how to solve the problem.

Trying to help the adoption curve.

Describing Identity in terms that "normal" people will understand. Drivers license/passport analogy, versus using lots of acronyms that make MEGO.

Okay, we understand the problem. What's the next step? People know that there's a need and a problem in this space, but they don't know how to begin looking for a solution. What are the key components that need to be determined? What are the top-level things that ppl need to understand? Start at a high level start to drill down.

Identity is simple. It's not easy, but it's simple.

Break down AuthN, AuthZ, Auditing

Two-part problem: how do we communicate clearly in a language that they understand? How do we express the problem in a way that a BDM will care?

Has there ever been a talk about common terms of service for an IdP, RP? What are "citizen-centric" term of service for a site/app?

Do organizations need to be "convinced" of the need for user-centric identity?

Identity systems need to have ease of use, usability baked in, or they won't be adopted to any scale.

Identity systems should shield the inner workings of the IAM system where possible - my mom doesn't care about LOA.

Education also matters - users need to be taught what is "normal" and what is a possible sign of trouble.

The UX of the IdP/RP will inevitably reflect on the reputation of the app utilizing them, even though decoupled. #iiw

We are not looking for understanding at a certain point, we are looking for adoption. My mom doesn't need to understand SAML.

Is there really value prop for the user to understand the technology? Or do we just need to educate them that its usable?

If you want mass adoption of a standard, it helps if it comes with additional benefits. OpenID vs Facebook.

Laura E. Hunter
Principal Technology Architect
MSIT ICS – Identity & Access Management

Personal Data Locker? What is it and Why? (F3D)

Convener: Jim Fenton
Notes-taker(s): Justin Tormey

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:

Ownership Rights in Data Pt2 (F3E)

Convener: Phil Wolf
Notes-taker(s): Joshua Gruenspecht

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:

Phil: Review of yesterday – Started with a discussion of the idea that "if data feels like it's yours, it should be owned by you." However, the ultimate resolution of that discussion was that property law was not the right frame in which to consider these issues. Instead, perhaps we want to consider something more similar to a European-style moral rights regime.

Heather: What about a "common pooled resource" model a la Scott Davis – water pools, fisheries – for identifying information? Guarantees levels of protection/control without regard to the nature of the information or its availability in non-pooled forums.

<Discussion of the problems of trying to put genies back in the bottle – if information is already available outside of such a regime, how would we get people to participate within the regime without the carrot of that information's availability? Commercial regulations? Law? Something else?>

Heather: We do this kind of top-down control of commercial information transactions already – any transaction involving a user and an aggregator approved by the user is covered by the Fair Credit Reporting Act. Consider this precedential.

<Discussion of the de-identifying requirements within the Freedom of Information Act>

Phil: In our future, I'd like to have some sense of control over my own online identity. My problem with doing this under contract law is that it doesn't give sufficient control to users.

Heather: No, contracts are really the only way to ensure, through law, that users can have individual control.

Steve: I do not believe that you can completely describe people's preferences in a preexisting contract, and that contracts will be insufficient for those reasons.

Joshua: So if we don't like property or contract, what's in between the two?

Jay: Scott's suggestion could be helpful. European privacy laws and the moral rights framework may also be helpful.

Phil/Heather: If we get people's assumptions and beliefs about privacy online, that would serve as a useful basis for determining what the "rights floor" ought to be.

Phil: What we're discussing here is all the information that constitutes people's "onlife" – everything that you do and are online.

Jay: The key to any such regime is that policy is great, but you also need a mechanism with which to ensure that said policy is enforced.

<Lots of talk about the possibilities of/problems with an insurance model>

Steve: But the problem with that model is that insurance assumes an acceptable level of failure, and there may not be an acceptable level of failure in this case.

Heather: We can work that problem, and we can't let the perfect be the enemy of the good.

Heather: The assorted FIPSs covering various different kinds of data distributions under US law demonstrate how much of a patchwork things currently are.

Mary Ann: I think there have been a lot of unstated assumptions about data which have gone into this conversation to this point – for example, the assumption that data needs to be protected.

<Discussion of the reasons to believe that some data might need to protected; general agreement about the lack of decided scope for such protections.>

Jay: One key information practice – making it clear to users what information you're asking for because you need it to provide the service in question (including the financing of that service) vs. what you're asking for with other uses in mind.

Phil: Assuming we want to take action on this, who should be in on the discussion?

<Discussion of possibilities: national congressional leaders in the case of privacy lawmaking, legal negotiators for various companies in the case of trustmarking (alongside marketers), privacy engineers in the case of privacy design policies.>

Information Security Standards and "Levels of Protection" (F3F)

Convener: Ankit Kapasi
Notes-taker(s): Ankit Kapasi

Tags for the session - technology discussed/ideas considered:

Information Security, Privacy, Level of Protection, LOP, Level of Assurance, LOA, Legal, Liability, NIST SP 800, ISO 27001/27002

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

Discussion:
There are 4 levels of protection. These levels of protection are mentioned but not defined. Levels of protection are complimentary to levels of assurance and as higher levels of assurance are implemented, levels of protection become more important. The levels of protection concept are drawn from legal requirements surrounding data protection policies.

- ➔ Level of assurance is focused on trust in credentialing. Within NIST it is the identification and authentication security control families.
- ➔ Level of protection is related to the remaining 15 NIST security control families
- ➔ A levels of protection paper will be presented at the ISO Privacy Standards Conference in October 2010.

As frameworks are developed, each framework is responsible to establish the requirements for levels of protection based on the legal and business needs. Levels of protection can be used as a product/service differentiator.
A level of protection is a service provider's obligation to the consumer that should follow data security and privacy legal and business requirements.
There are several information security standards, including NIST SP 800 series and ISO 27001/27002.

- ➔ The NIST framework is a US standard and the required framework for US Federal Government systems. It is based on a FIPS 199 system categorization of low, moderate, or high. Security controls are then selected from NIST SP 800-53 to manage risk to the information assets processed and stored by the system.
- ➔ NIST SP 800-63 covers levels of assurance and addresses the risk of a false positive. There is no NIST publication that speaks to levels of protection.

- ➔ ISO 27001/27002 is an international standard and can also be used to secure an information system and in general is more organizationally focused than system focused.

There is an opportunity for the National Strategy for Trusted Identities in Cyberspace to address liability and the insurance infrastructure. Currently, many industries (e.g., healthcare) view security as an impediment. The focus needs to shift to that of a business enabler such that trust with consumers can be established for high value, sensitive transactions in cyberspace.

Certification Coordination – OIX, Kantara, ID Commons (F3G)

Convener: ?
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:

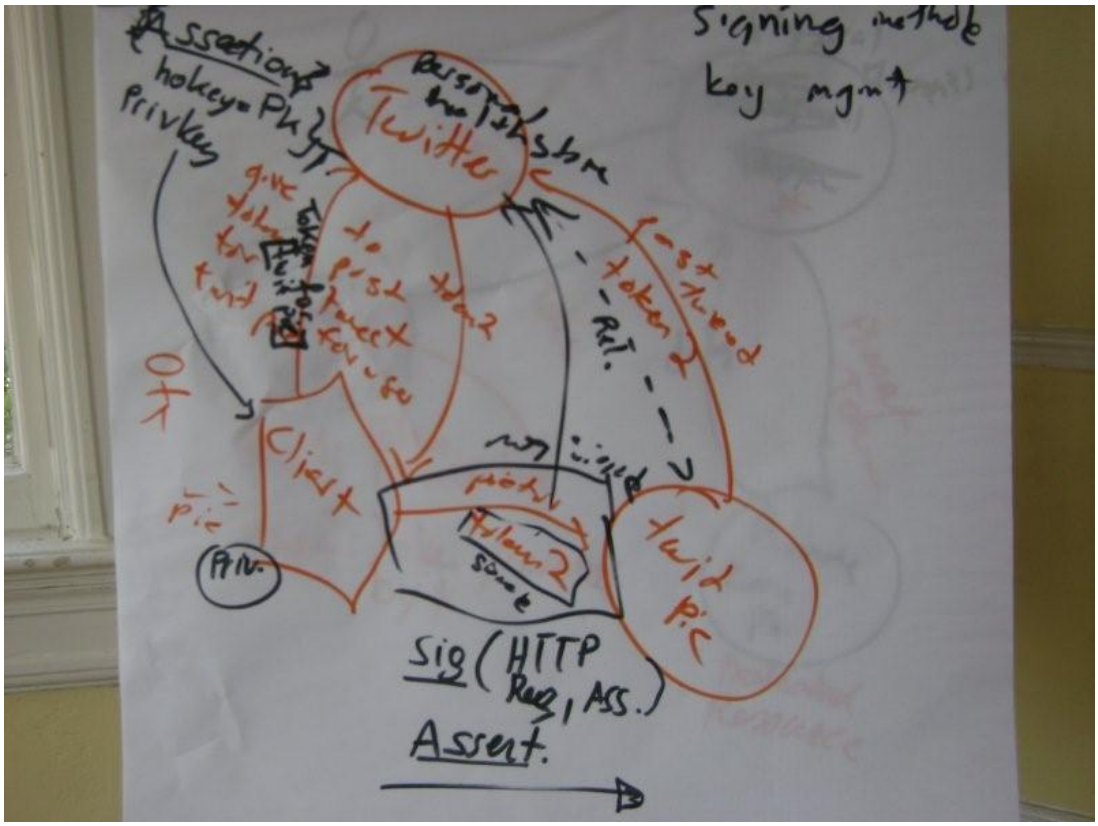
Friday Session 4

OAUTH Signing #2

Convener: Hannes Tschofenig
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:



Making NST IC Open/Making NST IC Happen (F4D)

Convener: Heather West & Jay Unger
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:

Hybrid Online/Offline Debate: BYO Issue (F4E)

Convener: Lucas Coiffi
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:

Roadmap for Personal Data Store Ecology: Let's Make One (F4F)

Convener: Kaliya Hamlin
Notes-taker(s): Barbara Bowen

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:

Demo (F4G)

Convener: **Wayne Burke**
Notes-taker(s): **Barb Flanagan**

Tags for the session - technology discussed/ideas considered:

Demo

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

2 Demos presented.

Barb Flanagan provided a demo of the "identity verification" service in use today by Trufina. Sharing verified identity data between user-user, and between business-user was shown. Service currently in use with mentoring sites, auction sites, job hiring/contracting sites, dating sites, and social networking sites.

Justin Tormey provided a demo of "cell phone location finder" service available today by Alcatel-Lucent. Input any Sprint cell phone number and receive the current latitude and longitude position of the cell phone. Plan to expand the service to use all carriers.

End of Event Reflection – As a Result of today…

... I have advanced multiple goals, have had with issues of identity and policy. Success.

... I learned about high assurance which helped in understanding its role as service providers and consumers.

...Importance of personal data storage for consumers

...I suspect that future IIW's should focus on the personal data store ecosystem?

...I will write a blog entry about Attribute and Identity Providers" regarding separate roles and list some use cases.

.... I was able to find other who were interested in addressing the non-technical aspects of user-centric identity.

....I'm happy to listen various themes for identity.

....I would like to hear " the use case" of trusted framework and attribute data exchanges.

....(language, tech, protocol, Auth, Authz) barrier is very high. but interesting!!

....more involved in personal data locker activities

...I have more questions than I showed up with although several ones have been answered.

...I have learned more about the IdM community and issues others are experiencing. Tomorrow would like to learn more about the implementation of 4 assurance levels (especially for level 3 and 4)

....I will look in to the pds.info project and examine XDI service descriptors.

....I am more aware of un-conference format, aware of some thoughts of future personal data, on the web.

...I'm happier to have learned there are people much smarter then me working on the issues...but glad to have been able to contribute in some way!

... I have more contacts in the identity space

....I have shared my companies vision with others in space

.... gained knowledge on interesting aspects of identity

....I am going to look up the blog posts about "data ownership"

.... I learned about 3 interesting projects that I never would have heard of, and heard the presepctive of people that I otherwise would not have spoken to.

....I have realized how many alteratives I need to research in order to resolve some of my (previously unresolved) use cases

.... more academic approaches

....i'm looking forward to tomorrow.

... I have a better understanding of obstacles involved with productive structuring of identity.

.... i have some new perspectives on identity and NSTIC in particular.

....I have a lot of extra repentance on Yom Kippur -- L'shana Tovah! Happy New Year, IIW! 5771

....it i the first time for me (us) to attend IIW. At first, I wonder because i don't know how to participate in the discussion. Next time, on November, we will attend again with our session, to introduce our issue and our proposals.

....I'm ready for these [personal data stores] to exist so I can take control of my stuff.

....I appreciate more that the government's weird problems are not necessarily unique.

....I will follow up with new contacts I made

....I learned about another layer of complexity under the policy assumptions regarding ID

....I will communicate my learning’s to my colleagues.

....I have met new people and learned new things. And I don't think that personal information should be treated as property.

....I will put on a workshop bringing together ID Providers with developers and readers of citizen engagement software to make significant progress on the problem of voter/constituent online identity.

....I now have a seed list of technologies to bug about nettlesome policy questions. Look out technologists!

...And despite the high level Intro, I didn't see a great interest in attendees in busienss approach around Identity and new tools that are built for. Maybe its not the event for that?

...I've met a doze important people in the identity space that I didn't previously know.

...there are still no answers

...I have gained a higher interest in various levels of assurance

....I met people I worked with for years but previously only know by voice.

....I am less ignorant and more confused

...I gained a better understanding of government policy and open questions. Would like more discussion on possible answers and how we can help drive those to resolution.

....I have taken a strong public position on the importance of encoding the meta-data in the same format as the data.

...I'm more convinced than ever that OAuth needs message signing.

...I am more concerned than ever about the looming Uber Furher of identity. The Gov looks to push this into private industry and the industry is responding with enthusiasm. Maybe this would be what the next gen wants; I hope they like it when the get it.

... New atmosphere, new people, with a lot of interesting discussion!

... Technology and framework/policy is the wheels of vehicle, looking forward for tomorrow and next west-coast IIW! Next step is more technology forward!!