ID COLLABORATION DAY

Across User-Centric, Enterprise and Government Identity Initiatives
Monday February 14th, prior to RSA North America

Book of Proceedings

February 14, 2011
San Francisco, California

Jointly produced by the Kantara Initiative and IIW Producers
(Doc Searls, Phil Windley and Kaliya Hamlin) - Identity Commons.

Table of Contents

Table of Contents 2

Session 1 4

Identity Commons Claims Agent Working Group (1A) 4

How Will the Enterprise do Identity In The Cloud? (1C) 6

UK Government ID For Digital Public Service (1E) 7

Why (Identity, Privacy, Turst) Frameworks are Failing (1G) 8

Session 2 9

Identity In The Browser (2B) 9

ID Adoption Discussions: Compliance + Service Certification Requirements for Cross-Domain IDM Deployments – Govt, Financial etc… (2C) 10

Personal Data Ecosystem Personal Data Stores & Services Emerging. What is Happening, How To Be Involved, What To Do Next (2D) 11

Architecture for A Personal Data Ecosystem (2G) 12

Session 3 13

Organizations and Their Individual Affiliates (retirees, contractors, etc…) Bringing Their "Own Identity" to the Organizations Services (3C) 13

Measuring ID Assurance Through Complex Supply Chains – "The Weakest Link Breaks the Chain" + Is There a Market for Assurance? (3D) 14

U-Prove CTP RZ (3G) 15

Session 4 16

ANSI / NASPO – ID-V Standards Workgroup Update (4A) 16

Machine Readable Policies => Informed Consent (4B) 17

NIH Seeks Higher LOA (4D) 18

Personal Data Management (part2) Practical Applications and Market Considerations (4G). 19

Session 5 20

NSTIC.US (5C) 20

Use Cases for User Centric + Communicating Them On The Web – "Identity Labs?" (5E) 21

Kantara Universal Login Experience (5G) 22

Session 6 23

Open ID ABC – High LOA Secure Discovery (6A) 23

User Managed Access & SMART (6E) 24

5 Minute Higgins 2.0 Personal Data Service Demo(6G) 25

About IIW Events 26

Identity Collaboration Day 2011 had over 90 attendees and 22 different sessions were posted for the day!

The wide audience of Government, Industry, and User-Centric advocates enabled interesting and interactive participatory groups. We had a good day collaborating and connecting the big enterprise resources with individual contributors (large and small). The event was a great success and we look forward to creating collaborative events in the near future.

Session 1

Identity Commons Claims Agent Working Group (1A)

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

Session Topic: Identity Commons Claims Agent Working Group

Convener: Paul Trevithick

Notes-taker(s): Mike Hanson & Patricia Wiebe

Tags for the session - technology discussed/ideas considered:

A link to the Claims Agent
charter: http://wiki.idcommons.net/ Claims_Agent_Charter.

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

Intro: A Claims Agent is a piece of software that conveys claims from some set of Claim Providers to some set of Relying Parties. A new Claims Agent Working Group is being setup that talks about how do we build this; focusing on eGoverment initially, skipping the question of how to log in.

For example, an RP asks, "are you over 21" or "do you have health insurance". eGovernment is interesting because it is privacy sensitive and, in many governments, sometimes has an interest in not being seen as Big Brotherish.

Sal D'Agostino: Relation to UMA?

Paul T: CAWG is more focused in privacy, more interested in augmentation of UI.

Paul Bryan: No browser or user-centricity in the model; transaction usually doesn't have a person in it. Lots of backchannel flow.

X: If the Claims Agent were an UMA Access Manager, it could provide tokens for person-present and person-not-present claims.

Paul T: The goal of the WG is to not invent anything, but to put together the technology that we've got. Facebook has demonstrated a way of providing a non-distributed, closed implementation of this. Let's try to narrowly focus on a small number of use cases, but also think broadly about existing technologies, e.g. OAuth, OpenID ABC, UMA. Emphasis on working code, less on specs as an initial goal.

Craig Wittenberg, Microsoft: Looking for participants for the W3C effort. Talked with several states who are interested in being issuers and RPs - title issuers in VA, employment insurance in CA, something in WA. Commercial partners, including Northrop Grummand; other vendors. Federal agencies, are interested, perhaps as RPs since they are not yet ready to be issuers, e.g. USDA is interested in fraud prevention. Commercial issuers, including some large banks to be issuers.

Sal D'Agostino: VA is issuing smart cards for emergency responders, e.g. RP case is

that I'm a firefighter.

Craig W: The cards are great for some cases; the underlying tech is x509 certificates, which doesn't work in every case.

Discussion: Is the WG going to work on authentication of RPs to a claims agent? The threat model here is inappropriate disclosure of claims to an RP, or the reuse of a bearer token to an RP.

UMA was brought up again - does UMA enumerate these use cases? Counterargument is that UMA is focused on authorization, not claims discovery.

Discussion: Identity Oracle concept? e.g. The ability to purchase a beer could be conveyed by a minimal disclosure token that indicates legal age, or it could be conveyed by an oracle that indicates whether you can buy beer. UMA is closer to the identical oracle; front-channel solutions different in that the issuer doesn't know who is asking the question. Paul: The claims agent could be stateful (it's my identity oracle) or state-free (it's more generic).

Issuer-to-agent discussion: How does the issuer announce claim availability? This has been a major problem with models before this. The infocard model expected the user to provision cards beforehand. If you didn't have a card, the UX was pretty bad.

Wendell Baker, Yahoo!: In the targeted ads business, all this stuff happens everyday. Content sites and ad networks generate ephemeral claims about the users. The requesting parties are advertisers, or agencies that try to get the ads in front of users. The claims agent is an economist's agent. Lots of discussion here has been about login or heavyweight claims; this is very different from ad placement which is very fast and low cost. Craig: to what extent would the user be involved in the flow? Wendell: somewhat if the user goes into an interest manager and flips bits; more granularly as the user signals their intent by moving around the web.

Discussion: Interesting parallels exist to the ad industry. Cost of a false positive for a "is a doctor" claim is obviously much lower! Privacy issues for some claims are much more important. Machine-readable privacy policies allow the claims agent to be much more interesting - InfoCards demonstrated that the "rational actor" theory of claims management doesn't work (too much user interaction, too invasive). Definition of "minimal" is very hard. Informed consent is also hard.

Note for WG: The claims agent should be able to broker claims that range from fully identity-bound to fully blinded (that is, the issuer does not know who the RPs are). This becomes a policy issue for the RP; the claims agent would process a policy from the RP to determine which issuers or claims could satisfy the request.

To participate in the WG, talk to Paul T. Notes by: Patricia Wiebe

• Work group is under IdCommons, not Kantara

• Claims agent focuses on claims passed over front channel, user centric model

••• UMA and OpenID ABC protocols are over back channel

• Craig (Microsoft) reported that he has commitments of some companies, state govts to deploy

• Bearer tokens have problems, need something stronger

••• Has this problem has been solved in UMA, SAML; caution about re- inventing

• Are there similarities to Bob Blakely's work on "identity oracle"?

• Should a claims agent be stateless? Require authentication to use the agent?

• The agent needs to have a relationship with both parties (claims provider, relying party)

• Need to enable both strongly identified and fully anonymous users

• Relying parties need to have declarative policy, as a machine readable document

••• Policy specifies who to trust – should be able to specify issuers or trust framework

• Need more discussion on agent-to-claims provider "introduction"

•••Need to do better than idea of provisioning information cards

• Consider different solution layers, e.g. transport versus application

• Should the agent be able to say "yes" on behalf of the user?

• The rational actor model isn't accepted anymore

••• can't prompt the user to consent to share their claims for every transaction

• Next steps... start participating in working group conference calls; meet weekly or biweekly?

Thanks Patricia. Great notes!

I have one minor correction and one addition. The one minor correction is that "UMA and OpenID ABC protocols are over back channel" isn't quite correct. Both have front channel elements (e.g., UMA and the permission granting process) and back channel elements (enabling the out of band retrieval of some claims). Craig.

Citizen ID's & Winlogon credentials? Why AND/OR Why not (1B)

URL:
http://iiw.idcommons.net/Citizen_ID's_and_Winlogon_credentials?_Why_AND/OR_Why_not

Session Topic:

Convener:

Notes-taker(s):

How Will the Enterprise do Identity In The Cloud? (1C)

URL: http://iiw.idcommons.net/How_Will_the_Enterprise_do_Identity_In_The_Cloud?

Session Topic:

Convener:

Notes-taker(s):

UK Government ID For Digital Public Service (1E)

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

Session Topic:

Convener:

Notes-taker(s):

Why (Identity, Privacy, Turst) Frameworks are Failing (1G)

URL:
http://iiw.idcommons.net/Why_(Identity,_Privacy,_Turst)_Frameworks_are_Failing

Session Topic: Why Frameworks Are Failing

Convener: Jeff Stollman

Notes-taker(s): Jeff Stollman

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:

Jeff posited that ALL past and current framework efforts – be they identity, privacy, or trust frameworks – have failed to gain traction because they have not identified the fundamental requirements.

The hypothesis presented is that we need to articulate a trust framework meta-model. Identity frameworks and privacy frameworks are merely subsets of this larger meta-model. It was further asserted that the trust framework meta-model describes a "system-of-systems" problem. As such, component sub-systems, such as identity and privacy, cannot be expected to address the entire problem space. Furthermore, as a system-of-systems problem, it is necessary to first articulate the structure of the overall trust framework in order to specify system-of-systems requirements that apply to all component systems.

For example, you can design a space shuttle by itself and come up with a clever design. But the shuttle can't fulfill its mission without other major systems: command center, launch pad, launch vehicle, etc. If the launch vehicle doesn't have the thrust to lift the shuttle into orbit, the project will fail. If the launch pad can't withstand the heat or weight of the launch vehicle, the project will fail. It is necessary to specify the overall requirements and the "interface" trade-offs. Should the launch vehicle be bigger or the shuttle lighter? She the launch pad be stronger of the launch vehicle less demanding?

It was further asserted that most current frameworks have assumed a technical solution before they developed requirements. Accordingly, they never really developed fundamental requirements.

Regarding the trust framework meta-model, Jeff claims that it is not something to be created, it is something to be revealed. The meta-model already exists and is characterized by our behavior. We use it every day – however unconsciously—in

making decisions whether or not to engage in a transaction (both live and online). The mission is to articulate the various trust elements that comprise the trust framework.

For example, if Alice seeks to purchase a widget from Bob online, she may need to trust

- that Bob is the authentic Bob that she has chosen to purchase from
- that Bob has access to the widget that she wants
- that Bob will deliver the widget to her once she provides her credit card information
- that her credit card company will approve her transaction
- that her credit card company will be online to approve her transaction promptly
- that her transaction information is not being monitored by unwanted spyware on her device
- that her network connection is secure
- that Bob's network connection is secure
- that her ISP is not monitoring her transaction data
- that Bob's ISP is not monitoring her transaction data
- that Bob will treat her personal information according to the terms or his Terms of Service and Privacy policies
- etc.

Similarly, Bob will have his own set of trust elements that need to be satisfied - as will all of the other parties to the transaction: the ISPs, regulators, appropriate legal systems for the jurisdictions involved in the transaction, etc.

Once defined, the meta-model provides several useful capabilities:

1. It allows us to map frameworks to it to determine how complete they are in addressing all of the trust elements needed for a comprehensive trust model.

2. It can serve as test criteria to determine whether specified Service Assessment Criteria effectively address the trust elements determined to be "in scope" by the framework developers.

3. It can be used to define boundaries of the various subsystems (e.g., identity, privacy, notification) of a trust framework and identify any gaps between them.

Rainer Hörbe has begun documenting the various roles involved in the full range of transactions. He has also taken a stab at identifying the various trust relationships among the parties. (See http://cmmls.portalverbund.at) This site also includes some work Rainer has begun to develop sample test criteria to assess whether a framework effectively addresses the requirements of the meta-model.

Jeff has begun identifying the trust elements that comprise these trust relationships.

Trust Framework Categorization v1.xls

A first pass is included in this spreadsheet:

Some definitions are included in slides 3-9 of the attached presentation.

Elements of a Trust Framework v2.ppt

Scott David is establishing an OIX risk wiki web site. This site is not yet available.

Session 2

Identity In The Browser (2B)

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

Session Topic: Identity In The Browser

Convener: Michael Hanson and Dan Mills and Dick Hardt

Notes-taker(s): Patricia Wiebe

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:

• Browser has role in verified claims

• Identity "in the browser" means it is baked into client software, not in the cloud

••• Browsers are generally accepted as being in the trusted zone, trusted by user

• Developed model based on verified email, which is understood by user and should be trusted as well as scenarios where passwords are reset by email

• Model:

••• Browser stores user's private key in safe location

••• User logs into browser, which provides access to user's keys

••• Browser discovers the user's public key based on their email address, request to server

••• Browser generates identifier based on keys, provides to RP

• Claim is "I control this identifier", based on proof that "I control this email address", SMTP

••• Is this assurance level 1 only?

• Approach to logon initiation is left to the RP, to determine when is the appropriate time to ask the user to logon

• User experience – need to have user determine whether to disclose their identifier, and which type: correlatable (e.g. email address), pseudonymous (pairwise by domain of RP), ephemeral (one time use)

• Who would provide such an email verification system (that hosts users' public keys)?

••• Mozilla is willing

- Could an RP be able to query the user's browser to determine if it is capable?

ID Adoption Discussions: Compliance + Service Certification Requirements for Cross-Domain IDM Deployments – Govt, Financial etc… (2C)

URL:

Session Topic:

Convener:

Notes-taker(s):

Personal Data Ecosystem Personal Data Stores & Services Emerging. What is Happening, How To Be Involved, What To Do Next (2D)

URL:

Session Topic:

Convener:

Notes-taker(s):

Architecture for A Personal Data Ecosystem (2G)

URL: http://iiw.idcommons.net/Architecture_for_A_Personal_Data_Ecosystem
Convener: Sandy Klausner
Notes-taker(s): Sandy Klausner

Tags for the session - technology discussed/ideas considered:

Link to Blog Post by Sandy Beyond Passwords: A Context-aware Internet

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

Introduction:

My previous SENDS blog post reflects on the current effort to redefine cyber-security and what the opportunities to empower individuals to manage their identity and ***cyber-presence*** might look like. This post describes a vision for a new Internet architecture that is context-aware, a key requirement to automate and secure online transactions, as well as provide trusted user identities and enhanced cyber-presence.

Addressing privacy challenges of user cyber-presence

Our identities and collective cyber-presence are captured across numerous service providers in today's Internet environment with each site registration, transaction and social posting (Figure 1). We have limited control over what information is captured and how it might be exploited. The prevailing business model is based on mining and perhaps selling information to third parties: this leads to potential contention between maintaining user privacy and maximizing service provider revenues.

Even if user privacy is 100% preserved, these walled gardens base their service offerings on proprietary metadata, which hampers the economic potential for location and transactional services to interoperate between websites.

Under an expanded vision of the NSTIC described in part one of this blog series, each user's cyber-presence could be represented in a secure, user-controlled ***iSelf*** space within a **Context-aware Internet** layer. Web, data, ontology and document content could transparently pass between the layer and the current Internet through the Identity Ecosystem gateway.

Each user would have absolute control over identity ***attribute*** and ***personal data*** disclosure. Attributes are associated to a user's authority, roles, rights, and privileges. Modification control of personal data would not apply to such information like health care records where the user may take a role in verifying its accuracy.

When combined, attributes and personal data are called a ***profile*** when represented in an iSelf.

Metadata (data about data) is replaced with the notion of a ***concept*** (a natural language-neutral universal idea), controlled by a user-driven community and not by a service provider. Concepts enable mass interoperability between iSelfs, internationalization of concepts, and efficient processing of contextualized content by software agents.

Service providers' still benefit under this Internet framework by matching accurate personal data to directed advertisers and marketers. A user might choose to financially benefit from more detailed personal data disclosure through a micropayment mechanism, for example.

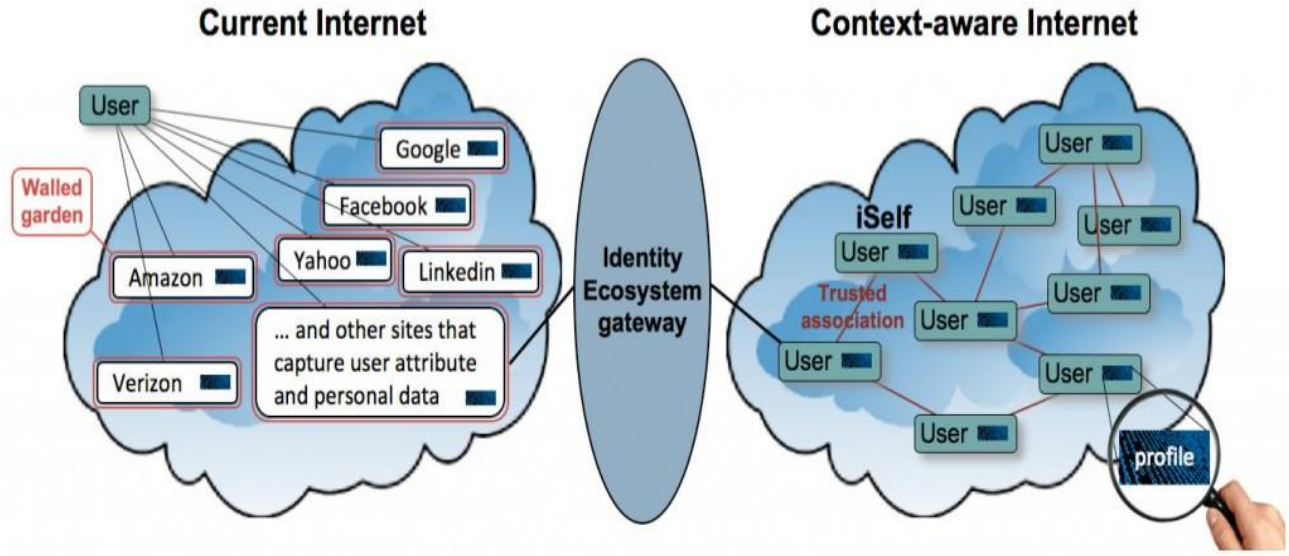


Figure 1: Addressing privacy challenges of user cyber-presence

Context-aware Internet

A Context-aware Internet would leverage semantic technology to achieve a level of machine understanding necessary to manage the Identity Ecosystem and more (Figure 2). An early application of semantics can be found in rich snippets that make it easier for users to decide whether a Google page is relevant to their search. Taking this technology to the next level requires contextualization. ***Context processing*** recognizes similarities in design intent, identifies relevance of existing work to new efforts, drives consolidation of redundant concepts and components, and enables unprecedented transparency and interoperability between systems.

Under a context-aware Internet, a user's identity is fused to a legal and architectural 'entity' that can be a person, company, organization, or government. Anything created by a user is traceable to the entity allowing crisp management of intellectual

property including an integrated metering and micropayment mechanism to support global reuse. Applications and apps are developed from a finite set of well-constrained recombinant components based on an icon-based executable design language. This 'white-box' software technology should be easy to understand and authenticate due to the graphical nature of its architecture.

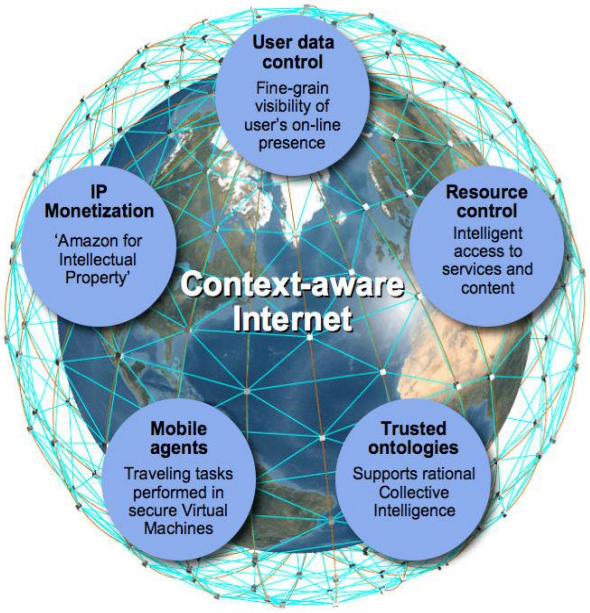


Figure 2 – Context-aware Internet

User-controlled identity/cyber-presence

Within such an environment, each user would be able to easily modify their iSelf profile values within well-established boundaries (Figure 3). Profile types are grouped under different concepts, shared between the iSelfs. **A Context-aware Internet would execute algorithms that automatically compare, match and disambiguate concepts across natural languages and subject fields.** This ***concept harmonization*** capability would support a new generation of social and professional networked communities that meet specialized interests, as well as enable deterministic expression of intents and sharing of fine-grain profiles.

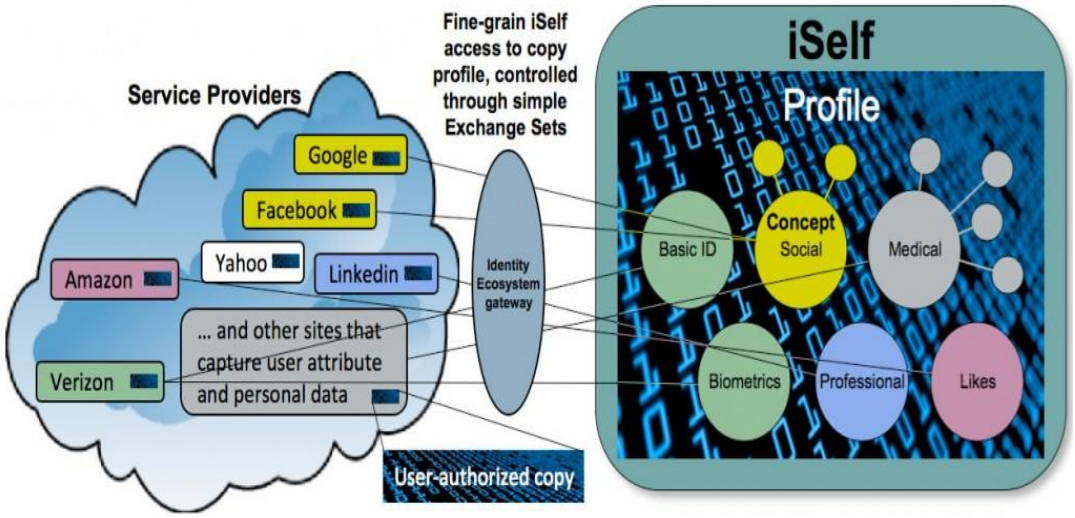


Figure 3: User-controlled identity/cyber-presence

Universal ID Management

The Identity Ecosystem would consist of four players (Figure 4). It is anticipated that Users will conduct transactions through Relying Parties[1] who contact Identity Providers[2] that provide credentials based on Attribute Providers[3].

1 – Relying Parties make transaction decisions based upon its receipt, validation, and acceptance of a subject's authenticated credentials and attributes.

2 – Providers are rresponsible for the processes associated with enrolling a subject, and establishing and maintaining the digital identity associated with an individual or NPE (non-person entity)

3 – Attribute Providers are a named quality or characteristic inherent or ascribed to someone or something (e.g., "Jane's age is at least 21 years").

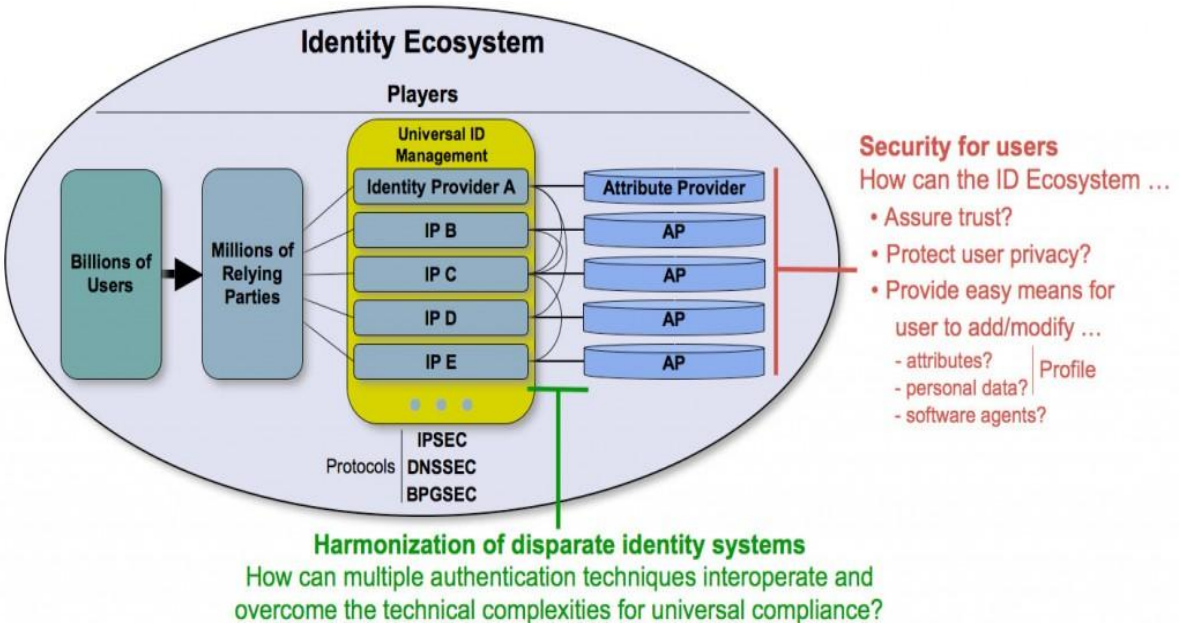


Figure 4: Universal ID Management

Extending Universal ID Management

The current NSTIC vision presumes that each Identity Provider will also be an Attribute Provider that stores attributes in siloed formats (Figure 5). While this configuration may address the multiple password problem (previously discussed here and here), it might open a Pandora's Box as providers choose to compete by extending their attribute configuration. This may leave users bewildered how to manage ever increasing complex profiles. ***It's anticipated that identity management functional demands will quickly escalate from basic attributes to rich personal data.***

Semantic Web-based technologies and the 'standards' process may not be able to meet these escalating challenges to prevent systematic chaos. A secure, new **Context Web** that operates under the Context-aware Internet could be capable of helping people to harmonize concepts and secure profiles at the required global scale.

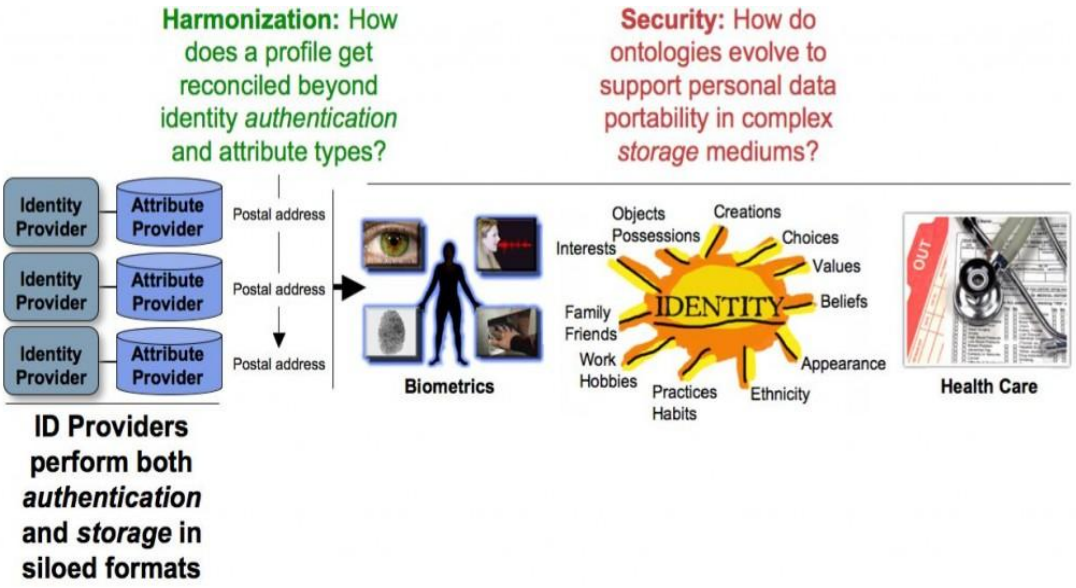


Figure 5 – Extending Universal ID Management

Advanced Identity Ecosystem

The Identity Ecosystem should scale more gracefully by deploying separate authentication and storage infrastructures (Figure 6). An iSelf could execute as a secure Virtual Machine (VM) that computes on semantic relationships.

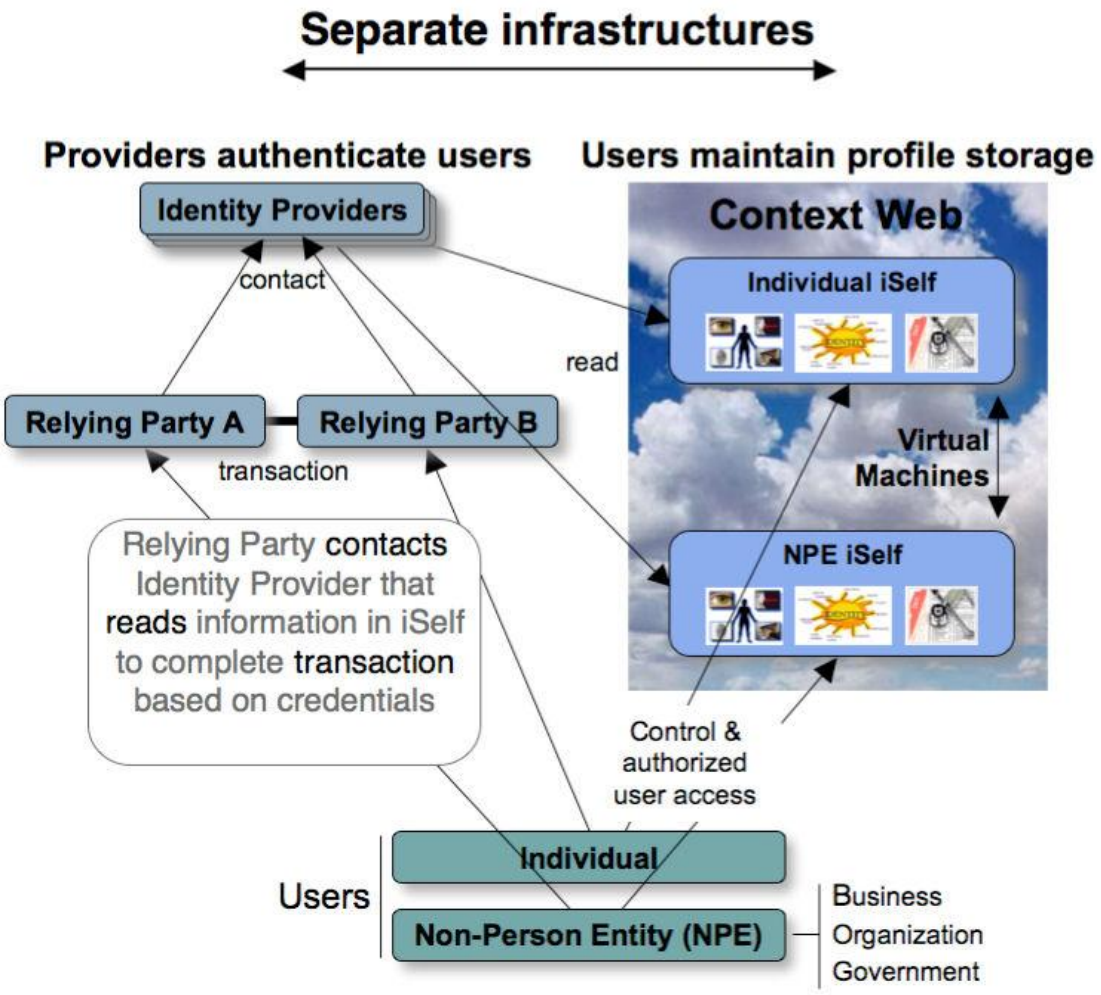


Figure 6 – Advanced Identity Ecosystem

Harmonization example

Creating trusted identities among participants in the Identity Ecosystem requires an infrastructure to support the interactions between transaction participants. A separate Context Web could:

• Automate the development process to provide secure, streamlined access to online services.

• Provide a common framework to assure that identity solutions interoperate.

• Lower the implementation and management costs that are dampening rapid market growth for identity and attribute provider services.

For example, the capability to record and store a user's fingerprint once and make it globally available to any third-party reading device is a first step in delivering

advanced identity solutions (Figure 7). The Context Web could help meet this challenge by providing a Context Registry to harmonize concepts across all VMs and their supporting Community Repositories.

All fingerprint reader vendors could become members of a community where concepts are organized in ontologies. Community members could share attributes based on common types that their devices use for fingerprint decoding by Relying Parties.

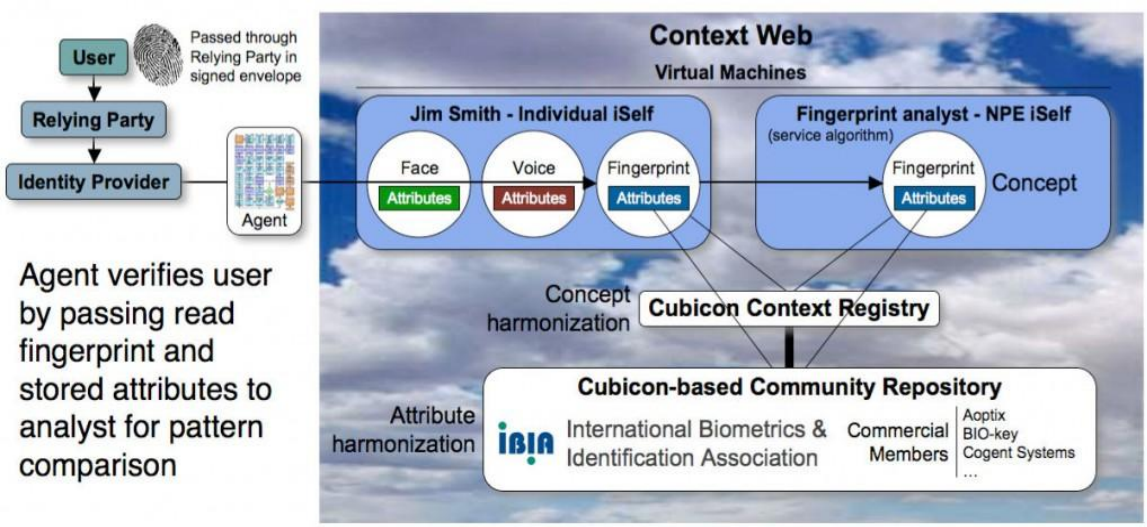


Figure 7 – Harmonization example

Security example

Privacy control in most social networking sites is currently limited to a set of predefined options, i.e. 'friend' or 'friend of a friend.' Exchange Sets greatly expand the notion of privacy control to provide authorized users' access to a profile that may evolve into very complex sets (Figure 8). In this example, all ID Provider Community members are authorized to read Basic ID and Biometrics attribute values. Exchange Sets enable complex access patterns to be easily maintained by each user through an intuitive interface on their laptop or mobile device. This ease of use is vital to assure users adopt best security practices for their cyber-presence. Profile management, like updated drivers' licenses or fishing licenses, are ultimately a user responsibility but it must be easy to do to make such a comprehensive approach effective.

Inquiring users would interact through software agents that travel between iSelfs. Harmonized concepts allow agents to visit many iSelfs, processing profiles that execute safely within each VM's 'sandbox.'

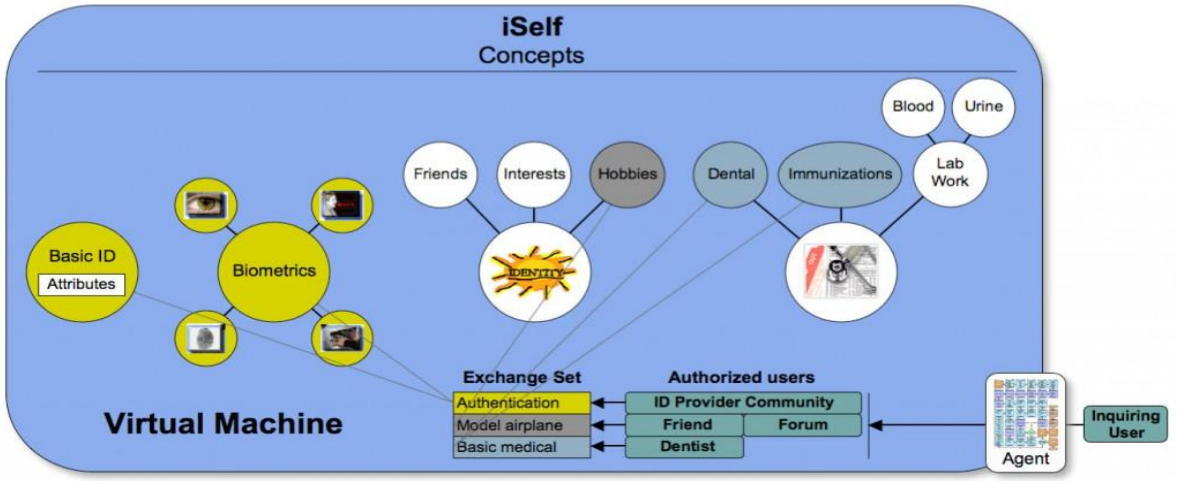


Figure 8 – Security example

User experience

Much of context processing could take place without direct user direction with benefits accruing through the following capabilities:

- User preferences respected at compliant sites
- Filtration of incoming communications by agents, i.e. email, RSS, Twitter
- Attribution and monetary reward for user-generated content
- User-invited advertising based on expressed needs and interests
- Computable, fine-grained, contextualized reputation
- User-created specialized social/professional networks

Conclusion

A Context-aware Internet could provide the prerequisite automation to help secure online transactions and user profiles. This blog suggests a manner that provides users with fine-grained control over their data from a single user interface while supporting the rapid development of a broad range of high-value commercial applications.

Such architecture could extend the Identity Ecosystem toward a trusted, efficient and resilient information and communications infrastructure for generations to come. The Cubicon team has done extensive work in exploring the practical deployment of such architecture and warmly invites dialog on the associated opportunities and implications.

Editor's note: Sandy Klausner ***is the founder and CEO of CoreTalk Corporation, the designer of the Cubicon executable design language, described at*** http://www.coretalk.net/. ***The opinions and concepts proposed by Sandy reflect his thinking about new types of programming languages, and web-based architectures including*** Cubicon. ***SENDS does not endorse any specific product, but seeks to ensure members and guests of the Private-Public partnership of the***

SENDS Consortium are aware of novel thinking proposed by those associated with the Consortium and its efforts.

Follow up: I recently posted the Beyond Passwords: A Vision for Personal Information Management ***blog entry followed with the*** Beyond Passwords: A Context-aware Internet ***entry on the SENDS website. These are good entry explanations of*** Cubicon ***as the technology applies to the identity and personal data management market segments.***

Session 3

Organizations and Their Individual Affiliates (retirees, contractors, etc…) Bringing Their "Own Identity" to the Organizations Services (3C)

URL:

Session Topic:

Convener:

Notes-taker(s):

Measuring ID Assurance Through Complex Supply Chains - "The Weakest Link Breaks the Chain" + Is There a Market for Assurance? (3D)

URL:
http://iiw.idcommons.net/Measuring_ID_Assurance_Through_Complex_Supply_Chains_-_"The_Weakest_Link_Breaks_the_Chain"_Is_There_a_Market_for_Assurance?

Submitted by: RL 'Bob' Morgan, University of Washington / InCommon Federation

This session was kicked off by some use cases related to the market value of identity assurance.

RL 'Bob' Morgan of the InCommon Federation observed that InCommon participant IdPs (mostly US universities) have been strongly encouraged by US government federation partners to meet ICAM Level 2 assurance requirements. This is a non-trivial cost (perhaps an average $50k per compliance project), multiplied across the 200 or so existing IdP sites (plus hundreds more to come). Site CIOs generally appreciate that assurance is important but need more motivation to invest. In this scenario the SPs (eg US government agencies) are gaining the benefits of reduced IdM risk and cost, so economics would suggest that the SPs bear some of the cost, but there is no existing business model for this.

Mark Coderre of Aetna described the Aetna federation situation. Aetna works with many federation partners both as SP and IdP. Many partners connect via other federations or identity hubs, forming complex chains of authentication that mirror business supply chains. All this connectivity is very functional but raises serious questions about assurance that are very important in an industry dealing with finances and health information. The issue is how to get assurance considerations inserted into the business relationships that form these chains.

Joni Brennan of Kantara observed that Kantara's Identity Assurance program is creating a market for certified assurance that is intended to support assessors charging for assessments and justifying their costs of participation in the program. The success of this market depends on IdPs and RPs understanding the value of certified assurance and working it into their business practices.

Discussion:

Someone involved with the NASPO National Identity Proofing and Verification Standard project NASPO described the work going on there, noting that it should be useful in convincing businesses that certified assurance is stable and useful. This would depend on the NASPO/ANSI output being integrated into assurance program's such as Kantara's.

A Canadian government person said that there has been an effort to include Kantara-certified assurance in government procurement procedures but it hasn't yet concluded.

There was agreement that getting assurance requirements into standard corporate RFP processes is essential. Another approach is to get assurance included in "Unified Compliance" procedures which cover things like Sarbanes-Oxley and HIPAA.

Another key development is to accurately reflect the costs and risks of the current way of doing business, both non-federated scenarios and federation without specified assurance. In particular risks of chained authentication scenarios need to be understood and assessed.

U-Prove CTP RZ (3G)

URL: http://iiw.idcommons.net/Architecture_for_A_Personal_Data_Ecosystem
Convener: Craig Wittenberg
Notes-taker(s): Patricia Wiebe

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:

Microsoft U-Prove Community Technology Preview (CTP)

- New U-Prove agent released today, along with 2 sample relying parties
- Meant as a working idea for discussion in the Claims Agent working group
- See www.microsoft.com/u-prove
- Emphasis on multi-browser support, broad set of scenarios
- Purpose of agent is to get RP policy, help the user make choices, and broker the communication
- Agent is aligned with user's interest. Helps protect privacy by providing unlinkability and untraceability, and by enabling minimal disclosure of information
- Agent is currently stateless; optional use of client components to provide additional features
- Currently built to handle only one claim provider at a time; in future – many claim providers in one transaction
- Currently built using WS-Federation protocol; post RSA starting to work on OAuth/JSON profile for U-Prove tokens
- Also, smartcard POC with Gemalto – issued tokens bound to card, thus card is required to present tokens to RP

U-Prove is an advanced cryptographic technology that, combined with existing standards-based identity solutions, overcomes the long-standing dilemma between identity assurance and privacy. U-Prove technology offers the same level of security as X.509 certificates, with additional privacy protecting features.

These capabilities unlock a broad range of scenarios that have historically been out of the reach of both the private and public sectors - cases where both verified identity information and privacy are required.

Microsoft is releasing a second Community Technology Preview (CTP) of U-Prove and related software innovations, so policy makers, developers, end-users and members of the Internet Identity community can try out the concepts, evaluate the capabilities and provide feedback.

Links

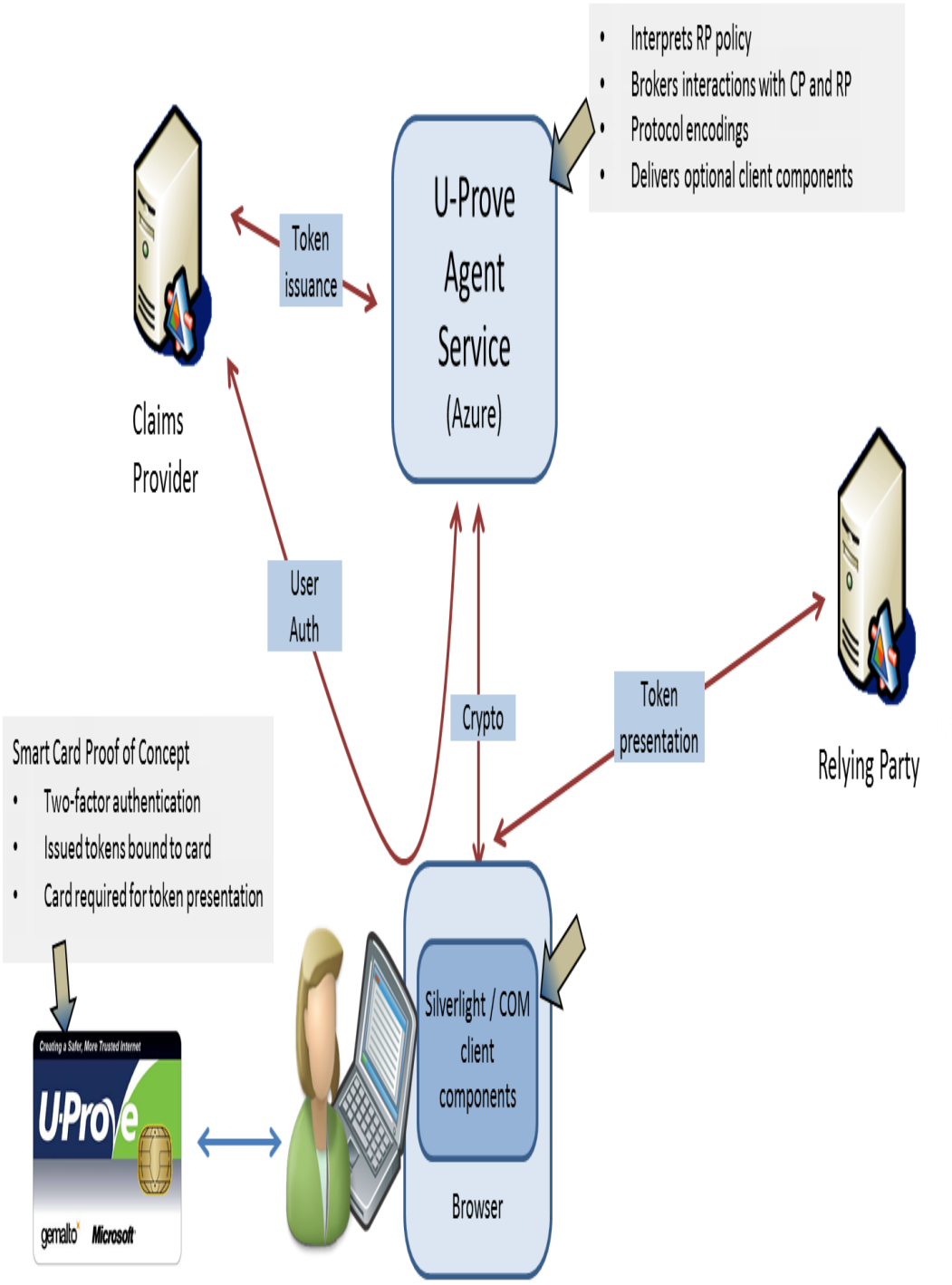
Learn more about U-Prove, its privacy protecting features, try it for yourself, and download developer tools
http://microsoft.com/u-prove

Watch technical videos on U-Prove
http://channel9.msdn.com/identity

Learn more about Microsoft's Open Specification Promise

At the core of Microsoft's vision are U-Prove Agents—software that acts as an intermediary between websites and explicitly represent the users' interests in choosing to share (or not to share) their personal information with sites on the Internet.
In this Preview, Microsoft offers a U-Prove Agent running as an online service, accessible from any computing device with a web browser. Optional client-side software delivered by this service provides enhanced security and privacy capabilities. This Preview also includes several sample websites, representing organizations in public and private sectors that can issue verified information or consume this information.
You can find white papers, specifications and developer toolkits to help discover the technology at http://microsoft.com/u-prove.

Overview Architecture - Identity System with U-Prove CTP Release 2



Session 4

ANSI / NASPO – ID-V Standards Workgroup Update (4A)

URL:http://iiw.idcommons.net/ANSI_/_NASPO_-_ID-V_Standards_Workgroup_Update

Convener: John Biccum

Notes-taker(s): Salvatore D'Agostino

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:

ANSI is ISO template

John is doing trust framework and Anna is doing privacy

Some people just there for sand in the gears

Chunking out the work, started with 20 people on call with open agenda, progress from there

Referring to them as Trust Frameworks

Quantification – quality of the identity proofing that is taking place

www.naspo.info

http://www.naspo.info/pages/idpvprojects.html

The existing risk management methodologies assume you know who the relying part is

Say what we are doing, let someone else check it.

Also complementing this is the ABA task force trying to establish a legal framework.

Federation is more than identity.

Look to certificate practice statements

Someone will create model legislation

Kantara IAWG is taking a look from an ISO 27000 perspective

Domain specific frameworks might evolve

E.g. AAMVA is domain specific expertise

NAPHSIS

Carbon based life form and linkage between that entity and a person sitting in front of you

Differentiation of roles

Virginia law for remote notarization

Limits on digital signatures

Timeline and maturity of the work, April 15th working draft

Kantara interested in having input

ISO driver license is about format not source of data

Machine Readable Policies => Informed Consent (4B)

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

Session Topic:

Convener:

Notes-taker(s):

NIH Seeks Higher LOA (4D)

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

Session Topic:

Convener:

Notes-taker(s):

Personal Data Management (part2) Practical Applications and Market Considerations (4G)

URL:
http://iiw.idcommons.net/Personal_Data_Management_(part2)_Practical_Applications_and_Market_Considerations

Session Topic:

Convener:

Notes-taker(s):

Session 5

NSTIC.US (5C)

URL:http://iiw.idcommons.net/NSTIC.US

Convener: Daza Greenwood

Notes-taker(s): Salvatore D'Agostino

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:

Private sector who are in the NSTIC "identity topology"

E-citizen foundation does not have an advocacy agenda

Able to create a safe harbor for dialog

http://www.nstic.us/

Multiple sites: e.g.

- Home
- Education
- News
- Privacy
- Kantara
- Identity Commons
- Calendar
- Subscribe

Collecting the reaction in the press

Provide feedback to the NIST program office

What is the form and forum for the discussion?

Twitter hashtags

Most important is the work that is being done by member organizations,

The public is not "literate" and is different than the community of identity management professionals.

Practicing writing open editorials, blog can serve that purpose

Multiple conversations, need to push information out to the public.
Contextual to the US
Could NSTIC be part of the communication program?
Never tasted soup so they don't know if its salty.
MADD analogy, I am pissed off and not going to take it any more.
Aspirin or carrot?
High powered PR firm
Equifax or PayPal have horror stories
Does it make sense to try to establish a PR budget?
What happen if NSTIC comes out next week?
Open editorial about NSTIC.
Can I sign onto this?
Why not an FAQ?
Will it accept OpenID? To walk the walk.
Hosting a public dialog?
Do we know the message or the goal here?
Generally what is the educational challenge?
Resource management scenario
Ecosystem is an interesting concept
Enabling authoritative sources to participate

Use Cases for User Centric + Communicating Them On The Web – "Identity Labs?" (5E)

URL:
http://iiw.idcommons.net/Use_Cases_for_User_Centric_and_Communicating_Them_On_The_Web-Identity_Labs?

Convener: Peter Watkins (BC Gov)

Note-taker(s)): Patricia Wiebe

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:

• Kantara (Joni Brennan) is interested in hosting, can show multi-national perspective, helps take it away from any one government, can raise funds

• Unsolved use cases can turn into Kantara working groups

• Vendor can know what to build to sell more of products

• Kantara WG on business scenarios for trusted federation (led by Rainer Hoerbe) – consider using this

• Like the layered approach

• Need for governance? Could a vendor misrepresent themselves? Push vendor content to vendor website, not on Kantara website

• Governments need safe harbour to talk to vendors

• Need to decouple the use cases from the implementation

•Have a look at OASIS government transformation draft standard, mentions IDM as enabler

Additional Recollection of the Session

Peter showed a model idea for a story board which would eventually be come a full featured website. This site would start with a broad view of the world and then work down to specific countries or even cities where X services were offered. The site viewer would then learn the story of: the service, how they can interact with the service, who's implementing the service, of the implementers who is interoperable, the basic messages passed in the service (high-level view) and finally how to specifically implement the service using open source standards.

There was some concern that such a site (story service) would need to find an unbiased "home". Kantara Initiative was suggested as a home for the story site.

Preliminary plans were made for the Kantara Business Cases for Trusted Federation (BCTF) DG to host a session where we could hear the presentaion again and record the details for an on-line capture to further socialize the idea, potentially to gather broad support and/or funding to build the story site as well. Plans are underway for the BCTF DG to host a “re-play” of the presentation which would be recorded for further input. Plans of how to move forward would occur from that point on.

Kantara Universal Login Experience (5G)

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

Session Topic:

Convener:

Notes-taker(s):

Session 6

Open ID ABC – High LOA Secure Discovery (6A)

URL: http://iiw.idcommons.net/Open_ID_ABC_-_High_LOA_Secure_Discovery

Session Topic:

Convener:

Notes-taker(s):

User Managed Access & SMART (6E)

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

Convener: Macie J

Notes-taker(s): Salvatore D'Agostino

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:

UMA

Control, Policy, Share

Trust a token, get a token, use a token

Review of the protocol

Can we get the set of slides that takes you through the flow?

@smartproject

Leeloo code has been moved to Apache Amber project and uma/j

Open source available next month

- Leeloo toolbox
- Gallerify.m (UMA compliant host)
- Smartam.2.0 (Authorization Manager)

5 Minute Higgins 2.0 Personal Data Service Demo(6G)

URL: http://iiw.idcommons.net/5_Minute_Higgins_2.0_Personal_Data_Service_Demo

Session Topic:

Convener:

Notes-taker(s):

About IIW Events

The Internet Identity Workshop (IIW) was founded in the fall of 2005 by Phil Windley, Doc Searls and Kaliya Hamlin. IIW is a working group of Identity Commons. The event has been a leading space of innovation and collaboration amongst the diverse community working on user-centric identity. The spring of 2011 event will be the 12th workshop held in California.

It has been one of the most effective venues for promoting and developing Web-site independent identity systems like OpenID, OAuth, and Information Cards. Past IIW events have proven to be an effective tool for building community in the Internet identity space as well as to get actual work accomplished.
The event has a unique format – the agenda is created live the day of the event. This allows for the discussion of key issues, projects and a lot of interactive opportunities with key industry leaders.

For additional information about IIW, you can go here:
http://www.internetidentityworkshop.com/about/

To read the Values of IIW as articulated by attendees of the 11th event held in November of 2010, you can go here:
http://www.internetidentityworkshop.com/iiw-values/
To read descriptions of 'what IIW is' as articulated by attendees of the 11th event held in November of 2010, you can go here:
http://www.internetidentityworkshop.com/what-is-iiw/

To check on Upcoming Events you can go here:
http://www.internetidentityworkshop.com/

IIW Events would not be possible without the community that gathers or the sponsors that make the gathering feasible.

The sponsors for Identity Collaboration Day were:
Gigya and ForgeRock!

Thank You!