University of London, Macmillan Hall

Book of Proceedings

October 11, 2010

Notes gathered and compiled by Heidi Nobantu Saul

Sponsorship Support Provided By

Consult Hyperion
Innopay
Mydex

Logistics Support
Brook Schofield - TERENA

Facilitated by Kaliya Hamlin and Heidi Nobantu Saul

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

Table of Contents

Session 1

What is the MYDEX Prototype? (1A)

Convener: William Heath and Iain Henderson
Notes-taker(s): Rod
URL: http://iiw.idcommons.net/What_is_the_MYDEX_Prototype%3F

Tags for the session - technology discussed/ideas considered:

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

Announcing the Mydex Community Prototype

This was by way of an announcement of some real technology - mostly this was questions and answers about understanding the whys and wherefores of the product/ service.

See http://mydex.org/ for details - this is but a brief summary.

Opportunity:
- Restoring user control of personal data
- A shortage of money will require (especially governmental organizations) to innovate in order to save on costs
- (and if done right the data will be more accurate, quicker)
- Help people realize (both meanings) the value of their personal data.

So what we have (I understand) is a *real* *working*, albeit prototype product. This allows a limited group of people to see what can and cannot be achieved. "The world's first VRM enabled personal data store". The principal themselves makes an assertion to the RP and this is then blessed by some secret sauce, including external verification.

So an example might be moving house. You know that you have moved and need to change address - you can make that statement, but in order for it to have credibility it needs to be accredited. Perhaps (in some futureworld) the lawyer handling the conveyancing can supply the token which makes your statement valid.

Another example - you seek to buy a mobile phone. The Phone shop consults Experian who makes a statement about your credit worthiness. Why should that not be information that you carry and assert (again suitably blessed).

The centre of this is the personal data store - think of it as a database with a single row (you) and many, many columns (all the information that anybody, including you, collects about you) which you can chose to give it to people as and when required.

But this is a sought after future - we need to start the bootstrapping process (without consumers why do the providers do anything, without providers what do the consumers care) and indeed to start to bootstrap the trust process.

Enter The Mydex Community Prototype - a first, tiny, but very real step. Three London Councils (Brent, Croydon, Windsor & Maidenhead) & one central government office (plus several other players) are acting as test RPs, and so people will/should/can (Iain, delete as appropriate) interact with them via this service (using Experian as the provider of external verification services).

Importantly (I believe) One council (Brent) is also willing to *push* data to the principal. So the principal doesn't have to start from scratch to manufacture their personal data store.

We get back to the well known (to Fed people) issue of "we then have to teach the RP's to only ask for what they really need" (and I'd guess then the answer of "and what happens if the user says no").

Project "Higgins" is the underlying technology.

Federated Network Access (1B)

Convener: Klaas Wierenga
Notes-taker(s):
URL: http://iiw.idcommons.net/Federated_Network_Access

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:

Partial Identities Privacy and Credentials (1C)

Convener: Dave Raggett
Notes-taker(s): Dave Raggett
URL: http://iiw.idcommons.net/Partial_Identities_Privacy_and_Credentials

Tags for the session - technology discussed/ideas considered:

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

I presented some slides:

http://www.w3.org/2010/10/raggett-priv-ids-creds.pdf

We started with a look at what online identity is used for, and the varying requirements these different uses bring. Privacy is at its heart about avoiding harm: discrimination, loss of face or just a loss of control.

Static credentials when brought online tend to facilitate linkability - the means to build up detailed pictures of people by combining separate pieces of information that on their own aren't particularly worrying.

Dynamic credentials and partial identities make it practical to adhere to the principle of "minimal disclosure". I presented two broad ways of realizing this, and am in the process of building an open source demonstrator as a Firefox extension. This aims to enable websites to be confident that you are say a child or are a current undergrad at such and such a University, but to do so without forcing you to disclose your full identity.

In discussion, we touched upon the triangular relationship between law, technology and social conventions. All are important to effective treatments of privacy.

The user interface is challenging for privacy. It is easy to imagine a view of (let's say) a driving license with some info redacted when you just want to reveal limited aspects about yourself, e.g your age but not your address. However when it comes to presenting information from multiple credentials, it gets much harder.

Users hate being pestered with confirmation boxes and there is plenty of work to show that users just click though these legally motivated irritations to get to the game with the fluffy white bunnies or whatever they are seeking to do. This is where trusted independent advisors have a big future as guardian angels that metaphorically

sit on our shoulders and help us when we are otherwise distracted (fluffy bunnies) or just not sufficiently well informed about the trustworthiness of the sites we visit.

We also discussed the value of "sticky policies" that stay with personal information as it flows within and between businesses. These stick policies determine what the information can be used for, who it can be shared with and how long it can be retained. You can also consider this as the other side of the coin from P3P. P3P is couched in legal terms for the obligations websites make to end users. Sticky policies on the other hand are about how to operationalize those obligations and need to be in terms that IT systems can execute.

There are plenty of opportunities to give people back control of their privacy, and it is a two way street -- we willingly give away personal information in exchange for services -- but we need better ways to establish and maintain trust. Companies (and governments) need practical solutions for implementing all of this.

There was quite a bit of talk around OpenID at the workshop, but I reckon that old fashioned user names and passwords still have plenty of life in them. The Mozilla Weave/Firefox account manager is a new breed of tools that help users to manage their online identities and breaks free of the understandable tendency of most of us to re-use the same id for multiple sites. This is fueling the need for standards by which websites inform the browser how to manage user accounts and sessions.

Today websites are forced to demand much more personal info than they really need. We need to find ways to bring a balance back through means that respect business models *and* end user's rights and needs.

Privacy + Federated Social Networking w/o Correlation (1D)

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

Tags for the session - technology discussed/ideas considered:

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

OpenID Tiered Providers (1E)

Convener: Mark Cross
Notes-taker(s): Mark Cross
URL: http://iiw.idcommons.net/OpenID_Tiered_Providers

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
I was interested to know other people's thoughts on the requirement for a private middle tier OpenID provider (Tier two), although there others, as I have fully narrated my thoughts below. On the session day I wrote them up on the board the wrong way around and only listed three, but they should have perhaps been structured thus:

Tier One
Government, Banks & Telcos
Good SLAs, trust relationship with customers for some tasks and high bar set against fraud.
Suitable for digital signatures in the future, as certification will be affordable for these institutions.

Tier Two
Private institutions
Good SLAs, trust relationship with customers for some tasks – *which may require anonymity* and also have a high bar set against fraud.
Suitable for digital signatures in the future, if the Identity Provider can obtain certification.

Could be used for signing content and embedding your OpenID URI into your published papers, this then allows people in the future to trace your current working location etc. Only a government issued OpenID could remain fixed, and relatively easily allow for someone to change their persona identity. IE Change their name.

Tier Three
Private individuals
SLA is as good as their setup, trust is not an issue

They will have a particular marketplace in relation to Darknets and future private digital money. For example, the Tonido platform running the Ripple Money Protocol over a Darknet would be particular interesting...

Tier Four
The traditional .com publishers, AOL, Google, Yahoo! Etc
Good SLAs, zero trust from customers regarding trading profile information to advertisers etc. Identity maybe anonymous to the institutions that could choose to accept them.

Audience feedback from the session
Denmark have nemID backed by their government and banks. See this person basic appraisal for more information http://tinyurl.com/2ctz9md

“Spain have an id card, but not an on-line one, and the Spanish pubic don't see why they should use it.” was stated by a person at the session.

When I raised the topic of demand for a tier two provider, because of usefulness of digital signing for activities like property conveyancing, car ownership transfers etc, a member of the panel directly involved in the commercial identity sector pointed out the issues brought about by low frequency of usage. Although he could foresee a reason of Tier two OpenID providers for certain closed communities. Frequency of usage also came up again in my second session gathering feelings on how OpenID could be marketed better to the general Internet public.

No mention of private user data (personal data stores) was raised or discussed.

Federated Identity as a Business Model (1F)

Convener: Douwe Lycklama (Innopay, the Netherlands)
Notes-taker(s): Jacob Boersma (Innopay, the Netherlands)
URL: http://iiw.idcommons.net/Federated_Identity_as_a_Business_Model

Tags for the session - technology discussed/ideas considered:

business models, scheme, paying for identity services, government and business cooperation

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

This business model takes its inspiration from the payments industry, which also functions as a network. There are many roles for users and relying parties in transactions that require identification, resulting in a 'keychain' of identity solutions.

This leads to the idea that Identity is a two-sided market: there is room for service providers for users and service providers for relying parties. Such a market often starts with 1 service provider that wants to reach the entire world (platform approach), cf. American Express in payments world or Facebook.

Next step is a 4-corner model, where service providers for end-users and service providers for relying parties agree to be interoperable based on a universal set of agreements / in a standardized way.

In the project 'eHerkenning' ('eRecognition') in the Netherlands this standardized method of communication uses SAML on the technological level, but there are also agreements on the application and business level. The business case assumes that everyone pays for their own side of the model: users pay the user-side service providers, Relying parties pay the RP-side service providers. If there is an imbalance between the two sides, the service providers can pay each other an interchange fee to create a positive business case on all sides.

The Dutch eHerkenning system uses different levels of assurance based on the 'STORK' model.

Discussion issues:
- where are the advertisers in this model? They could be relying parties themselves (looking for user identity information in order to provide targeted content) OR they could provide the revenue side of the business case by providing embedded advertisements.
- how do we create a positive business case? If end-users are not willing to pay because they perceive no added value, how can you run this 4-corner model? Will a transaction-based fee be

enough to finance all parties involved, considering that the first identification of an unknown end-user is the most valuable?

Summary: Electronic ID is a two-sided market. A business model based on the 4-corner model used in the payments world has been developed in the Netherlands (project ‘eHerkenning’, focused on Business-to-government transactions). Service providers on the end-user side and service providers on the relying party side connect to each other in a standardized way based on a scheme. Interchange fees allow for a working business case.

Session 2

Scoping the Single European Digital Identity Community (2A)

Convener: Dave Birch and Vic Victoriano
Notes-taker(s): Dave Birch
URL: http://iiw.idcommons.net/Scoping_the_Single_European_Digital_Identity_Community

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:

European government don't even trust each other for mutual identification

European vision should be inclusive (not just for e-government)

Current visions are based on a specific technology (PKI)

There are no payments or liabilities in the current visions

Only 1 out of 17 govts (Germany) currently charge for the use of the ID service

Wider use of govt eID is often restricted by law

We should aim to emulate the physical world or design for the virtual world?

Do European govts want to me database linking easier

Infrastructure should enforce European rights

Private sector has free use of eID infrastructure (eg, Spain)

What is the ID equivalent of the European GSM vision?

What is ID equivalent of "European" Visa/MC?

Europe built GSM on an existing business model

Citizens expect govt to abuse their data

Governments and their policies change

We can only deliver on a European constitutional position

EU vision is a collection of regional and national visions?

Identity is too national for a European vision

Could we at least agree a goal, such as minimizing transaction costs?

WebID & DNSSEC – combined session (2C)

Convener: Henry Story (WebID) & Esther Makaay (DNSSEC
Henry.story@bblfish.net / esther.makaay@sidn.nl
Notes-taker(s): Esther Makaay
URL: http://iiw.idcommons.net/WebID_and_DNSSEC_-_combined_session

Tags for the session - technology discussed/ideas considered:

How WebID works ('foaf' + SSL) – a new way to construct trusted social webs.
How DNSSEC can enable and strengthen identity use cases from the core of the Internet.

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

WebID

For background information and slides, see: http://esw.w3.org/Foaf%2Bssl (and see the FAQ there)

The status of social networks these days: users are prisoners of the network, seeing only a small part of the information, while the 'owners' of the network see everything. Furthermore all communication requires the communicators to be on the same network. With the telephone and e-mail people can communicate across service providers.

The WebID protocol enables browser based one click login to any server without the user needing to remember either a username or a password. It works in the great majority of desktop browsers as is: using the SSL/TLS stack on which https and the whole of web e-commerce is based.

Of course there is a small twist in how it is used - since client side certificates never took off. The trick is not to rely on Certificate Authorities, and to make creation of Certificates cheap and replaceable. This requires changing the TLS authentication procedure at the Relying Party's server.
First the Social Web CMS should make it easy for a user to create any number of compliant X.509 certificates for each of their browsers. This is easy to do using the now documented html keygen tag. Using this the browser can create a private key and send the public key to the server which then creates certificate containing a a URI identifying a user (eg: http://bblfish.net/#hjs) - in the X.509 Subject Alternative Name field. The certificate is returned to the browser and automatically added to the keychain. By simultaneously placing placing at the document location (http://bblfish.net/) a machine readable description tying the WebID to the public key in the certificate the client is set.

Secondly in order to allow users to login the Relying Party need just make an https endpoint available that requests a client certificate. The browser will then ask the user to select one of his certs, which will be sent to the server. The Relying Party's https server will then check

that the WebID Profile does indeed list the WebID specified in the certificate as knowing the private key of the published public key.

The Document to put at the WebID is defined semantically. It could be a list of simple PEM-files, open-contact documents or foaf files annotated with cert ontology. To get feedback on the best way to do this it is worth participating in the discussion on the foaf-protocols mailing list.

Question: Does WebID suffer the same problems as MS Infocard? (Moving it between different devices, using it on mobile devices.)
Answer: Creating WebID certificates is cheap, so you can create one for each device on the fly.

Question: What if you lose your key?
Answer: If you loose your key, your Social Web CMS - aka Personal Data Store - need just remove the public key from the WebID profile document. How would they know you are the owner of the account? Of course you would need other secure methods of authentication such as one time passwords sent via SMS perhaps.

Did PGP not show the web of trust to be a failure?
PGP requires users to sign each other's keys which is cumbersome. Instead of placing information in the Certificate WebID places it on the web where it can easily be changed without changing certificates.

Question: How do you authorize?
Answer: Now – if you receive someone's business card, you can add them to your profile as someone you know. Their e-mail can tie them back to their WebID using WebFinger, or their home page could be their WebID profile...

Question: How does that tie into the Web of Trust?
If your friends/contacts link to other friends and contacts, then you can gain some assurance that someone you don't know who is connecting to you is at least somewhat known, or trackable via your friend.

Question: If I hand over my laptop, do I hand over my certificates?
Answer: That depends on how you handle your accounts. On OSX one can have a guest account that just deletes all information when the user logs out. No need to hand them your browser with your cookies and passwords available.

DNSSEC

The WebID protocol relies on DNS and CAs for security. With DNSSEC re-inforcing DNS and potentially reducing the need for CAs, deployment of WebIDs will be even easier.
For more information about DNSSEC itself, see the notes on the session "DNSSEC explained" at IIW10: http://iiw.idcommons.net/DNSSEC

DNS: the navigation-protocol of the Internet. Enter an address (manually/machine), together with the chosen protocol and it either directs you to a location or provides the needed information. Using DNS for IdM-solutions has been looked into in the past, but discarded because of security-issues. While DNS is very scalable and robust, it used to be untrustworthy.

Until now: DNSSEC is being deployed world-wide. The root zone and many TLD's already use it or have announced deployment in the next year.

What does it mean to have DNSSEC?
It means verifiable DNS answers. DNSSEC provides for origin authentication, data integrity and authenticated denial of existence. There's a metaphor describing it as a sealed, transparent envelope around the (DNS-) message. Anyone can still read the message. The seal is attached to the envelope and applied by the sender of the message.

DNSSEC is a real game-changer when it comes to using DNS for identity-related use cases. WebID is a good example of this, where self-signed certificates need to be verified by browsers.
A certificate is most commonly used for TLS (SSL), where information send to and from a web server is encrypted for confidentiality. Browsers use their stored keys from the CA's (certificate authorities) to verify the certificate. CA's are third parties, providing these certificates in various degrees of both encryption and validation. The lowest level of validation basically provides verification of the domain name the certificate is issued to, where the much more elaborate (and costly) 'Extended Validation' certificates (that turn your browser-url green or blue) also identifies the party that registered the domain name (and even identify the person applying for the certificate as a valid representative of this party).

There are quite a few situations where I want to have TLS to provide confidential server-communications, but don't really need a third party validating the certificate as belonging to this domain name. This happens for example when I'm using my own servers at home (under my own domain name, with the certificate I put on the server myself), or when I'm connecting to the mail server from my employer. These certificates are usually 'self-signed' and any browser will go through the well-known 'security risk' warning-procedures before allowing you onto a site that has such a certificate.

DNSSEC offers a solution to bootstrap these certificates into DNS, allowing for a scalable, self-manageable (and cheap) solution to use TLS with self-signed certificates. Any validating resolver can verify all information in any DNSSEC-signed domain zone file, using the public key for the root zone as a trust anchor.
If you include a certificate or a public key into the zone file for a domain, that information can also be validated. This would tie the (self-signed) certificate to the domain zone, obsoleting the need for a third party (CA) to validate this information. Of course, there's no identification of the person or party that has registered the domain name. You'd still need EV for that.
People in the IETF are working to standardize inclusion of keys and certificates into the zone file for different purposes. (is it RFC4398 and RFC4398 ?)

Question: Using DNS requires tooling for updating information in the domain zone file.
Answer: True. A lot of registrars already offer tooling to manage common redirects for mail and websites. We hope they adapt this tooling to support new usage, like managing keys and certificates. And looking at the current tooling, it's usually not very flexible or user-friendly. We could certainly do with more sophisticated ways of managing zone file information.

Comment: Work needs to be done to create low-level API's. People need to work towards this, coming from different layers: upwards from the DNS-layer and downward from the application-layer. Open standards on the client side are needed!

Comments/clarifications:
DNS is a public protocol. It's not meant to act as a store for public data. It can be used to point towards data stores though (similar to the way it now points to websites, mailservers or SIP-servers).
DNS is not a P2P-model. Delegation gives it a lot of strength, but also limits usage. E-mail is weird, going through a lot of hops instead of directly P2P. Maybe the model for news-groups is better?
But the delegation in DNS allows for discovery services. There's no working, scalable alternative to DNS.

We're talking about the information in the zone file, not the Whois-information. The information in the zone file is telling about where the services, hosts and sub-delegations for this domain name can be found. The information in the Whois shows contact-information about the parties involved in the domain registration (like the contact persons and the registrar).

U-Prove – How Do We Use Privacy Enhancing Crypto? (2D)

Convener: James Brown (Microsoft)
Notes-taker(s): Rod
URL: http://iiw.idcommons.net/U-Prove_-_How_Do_We_Use_Privacy_Enhancing_Crypto%3F

Tags for the session - technology discussed/ideas considered:

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

U-Prove is a different spin on crypto. It is the fruits of a split in the math heads view of the world 30 years ago. Half went down the PKI route and the other half ended up here.

Microsoft bought a company set up by Dr Stephan Brands which uses this "new way". IBM also owns technology in this space (Identity Mixer).

So what is it? The important thing is to understand that this is done at the crypto level. The mechanism is one in which a principal can release any one of a basket of attributes to any relying party it wants. These attributes are originally issued by a trusted third party (the IdP) as a basket but carry no information which allows anyone to trace back to the IdP.

This gives one the building blocks on which to build quite interesting user centric data. Further you can express derivations of the data. So the IdP may make a statement "Born on the 15 Jun 1963", but the principal has assert (with the authority of the IdP) "Is over 21" or "Is under 65".

So, the Principal can end up with a bunch of assertions (presumably from a bunch of IdPs) and can chose to assert *parts* of any or all of them to any RP. The principal gets to decide who sees the information, but it carries the authority of the issuing IdP.

Now, Microsoft has this technology. Such specs and profiles as exist are in the public domain (and are in the process of going through whichever standards bodies are appropriate). They have a C# and a Java SDK. They have an Cardspace with U-Prove "community tech preview" which uses this and they have an ADFS example as well. They also have a JavaScript version of the crypto engine (but it ain't fast)

We had discussions about precisely how these assertions were to be shovelled about - what are going to be the winning profiles? is this another WS-trust variant?. The impression I get is that we are early on in the process and nothing has really been firmed up yet (except the maths behind the lowest level crypto). Profiles are going

to be everything. For instance I asked about establishing technical trust in this space, and no-one could answer (or the question was meaningless, or we are not there yet).

The issue here is "what to do with it". Microsoft will not be introducing this until there is a reason to invest and bring a product to market. Two ideas were (from Vodafone) child protection and age verification (with respect to geo data and (e.g. from Mydex) to a government administrating social services, reducing the cost of gathering all the data by each group which does the admin.

Microsoft are open to discussions on use cases that will help evolve understanding and market testing in this area.

Session 3

What Do We Actually Mean When We Talk About Identity? (3A)

Convener: Igor Goldkind
Notes-taker(s):
URL: http://iiw.idcommons.net/What_Do_We_Actually_Mean_When_We_Talk_About_Identity%3F

Tags for the session - technology discussed/ideas considered:

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

The Quality of Customer Intelligence (Authenticity/Relevance Correlation (3B)

Convener: Mark Kristel
Notes-taker(s):
URL: http://iiw.idcommons.net/The_Quality_of_Customer_Intelligence_(Authenticity/Relevance_Correlation)

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 Harmonizing = Project Nori DEMO(3C)

Convener: Markus & Sampo
Notes-taker(s):
URL: http://iiw.idcommons.net/Personal_Data_Store_Harmonizing_%3D_Project_Nori_DEMO

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:

Please pull from my web site...

http://zxid.org/tas3/sampo-tas3-fippp-pds-iiw-lon-2010-slides.pdf

--Sampo

Claims (3D)

Convener: Gordon Rae
Notes-taker(s): Ben Werdmuller von Elgg
URL: http://iiw.idcommons.net/Claims

Tags for the session - technology discussed/ideas considered:

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

Privacy and identity are intrinsically linked. We should not think of networked identity as who we are, but as a mechanism for telling services what they need to know about us.

In Europe, whether you have data protection rights is based on your identity. At Vodafone, they're finding that this is a false dichotomy, and they're exploring the privacy implications of any piece of data as well as identities as a whole.

Respecting peoples' privacy is important commercially as well as ethically; users will be turned off if they have to reveal too much, but services need directed piece of information (eg age, medical history, etc).

Trusted intermediaries could help validate claims of specific information. Think social location services, which are free but have age requirements for safety reasons. Credit cards and phone numbers aren't enough, as they can easily be stolen, and prepay phone customers don't provide enough data.

How do we trust intermediaries? Social reputation doesn't work. Think ebay: the reputation system there is a source of constant conflict internally, and there are all kinds of subjective reasons for negative feedback. And for vital information like age or gun ownership, for example, social reputation isn't trustworthy enough.

For some assertions, a Boolean response is enough: it's either true or it isn't. Is the user over 18? Other times, it's a more holistic assertion that a set of data or assertions are accurate - or mostly accurate, etc. The trouble is, this could encompass infinite knowledge domains, and you don't want to limit the usefulness.

Could questions perhaps be asked of a person / source and then digitally countersigned by a domain-specific trusted party, using a standard API? Could, for example, OpenID be used as a basis to develop a decentralized digital notary system?

This is one way we could assign trust in an assertion, without necessarily assigning trust to the assertion's owner, and without creating a reputation that will follow the

user around for the rest of his or her life. (University library identity providers work this way, by asserting to journals and information services that a user is a valid student.)

When a trusted party verifies some data, it's important to be able to tell that party if the information turns out to be inaccurate, or if the user behaves badly within the domain. It's also a good idea for that party to be able to announce what other information it can vouch for, and for they themselves to be able to recursively delegate that trust.

If identities are centrally stored, the kinds of information within them are naturally limited. Rather, identities could be considered to be a tethered collection of assertions about a person, each of which could be stored in a different place.

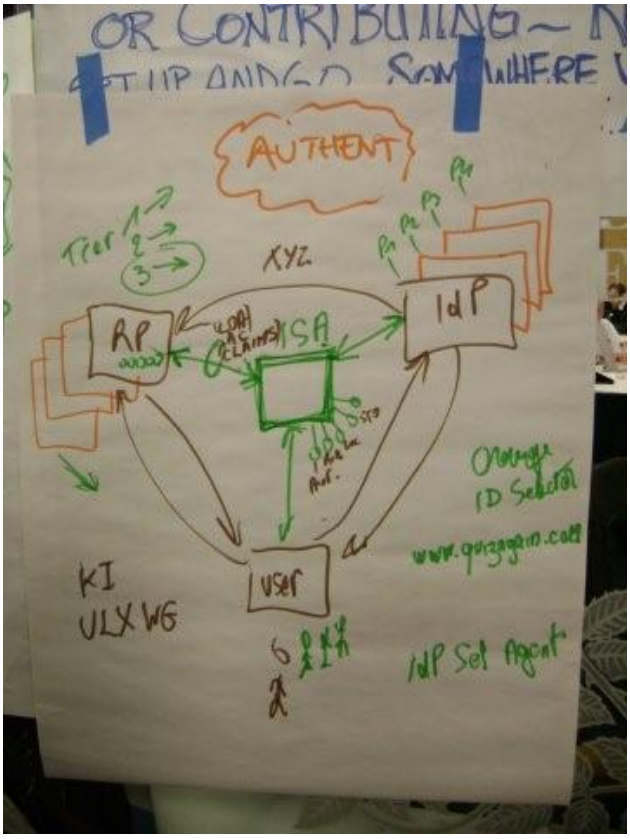
Assertions might have lifetimes, or need to be revoked. They could be timestamped, and in any event APIs - where you constantly check back to a source - are more secure. But delegation here is also important, in order to avoid single points of failure for each piece of information.

Authent – New Tools – Opportunities – Business (3E)

Convener: P. Clement
Notes-taker(s):
URL: http://iiw.idcommons.net/Authent-New_Tools_-_Opportunities_-_Business

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:



Remonetizing the Web: from 'Give privacy, get service' to: A win-win social web ecosystem for customers, Telcos, Banks, Websites (3F)

Convener: Rolf von Behrens
Notes-taker(s): @colinhayhurst
URL: http://iiw.idcommons.net/Remonetizing_the_Web:

Tags for the session - technology discussed/ideas considered:

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

Identity Assurance (merges with) Automated Policy Negotiation (3G)

Convener: Leif Johansson & Rainer Hoerbe
Notes-taker(s):
URL: http://iiw.idcommons.net/Identity_Assurance_(merges_with)_Automated_Policy_Negotiation

Tags for the session - technology discussed/ideas considered:

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

Session 4

CardSpace in the Clouds (4A)

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

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:

CardSpace in the Clouds is a privacy preserving attribute aggregation scheme that gives a user full control over the partial release of his attributes to service providers. The service provider receives signed assertions from each attribute authority attesting that the user of the current session does indeed possess this set of attributes. The user can choose which attributes to release by clicking on multiple cards. Each card will typically contain only one attribute e.g. visa card holder, or address, or age, or club membership etc. (or a small set of highly related attributes such as degree, classification and subject). The interface is highly intuitive and based on the existing CardSpace interface, with the addition that multiple cards can be selected.

The system provides the user with full mobility and multi-device use since the card selector lives "in the cloud" (as opposed to the current CardSpace system where the selector lives in the browser).

The system provides a simple to use alternative to U-Prove and Idemix, as it is based on existing technologies (SAML assertions and Liberty Alliance EPRs).

Attachments
i) PPT presentation
ii) Paper
--
David W. Chadwick, BSc PhD
Professor of Information Systems Security School of Computing, University of Kent, Canterbury, CT2 7NF Skype Name: davidwchadwick
Tel: +44 1227 82 3221
Fax +44 1227 762 811
Mobile: +44 77 96 44 7184
Email: D.W.Chadwick@kent.ac.uk
Home Page: http://www.cs.kent.ac.uk/people/staff/dwc8/index.html

Introduction to Digital Death – What Happens to Internet Identity After Death? (4B)

Convener: Stacy Pitsillides
Notes-taker(s):
URL: http://iiw.idcommons.net/Introduction_to_Digital_Death_-_What_Happens_to_Internet_Identity_After_Death%253F

Tags for the session - technology discussed/ideas considered:

digital death, protocols, introduction, legacy, centralization

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

The topic of Digital Death was introduced. Most people who attended the session were unfamiliar with the concept so it was broken down first by simply discussing what happens to your data after you die? What are the services currently provided (e.g. digital safety deposit boxes) , how do they work and what different system currently in use eg Facebook, Google, Twitter do with data 'left' after death. This led us to the consideration of virtual wills, the decontextualiation and decentralisation of data and how and why one should leave parts or all of their data for the next generation (i.e. their children).

The general response was one of interest and surprise, it is perhaps always a shock if it is something you had not considered prior. There was a great interest in the practical elements of why this is an issue and what may be done about it in the future, including a short discussion of how a Personal Data Store (if it was to be implemented) could be bequeathed, divided and even duplicated in sections to allow for a more manageable, centralised digital presence which could then be dealt with as the loved one sees fit.

The Digital Death community is growing, as the subject is further disseminated and as awareness grows there will be further encouragement for action. The systems which are currently in place do not work, therefore there must be a continuation of experts gathering within productive working events such as unconferences to discuss various strategies for the practical and legal future of this topic and indeed our data.

One Social Web . org (4C)

Convener: Dan Applequist
Notes-taker(s):
URL: http://iiw.idcommons.net/One_Social_Web_._org

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:

Why do Politicians Understand So Little? Our Fault or Theirs? (4D)

Convener: Dave Birch
Notes-taker(s): Dave Birch
URL: http://iiw.idcommons.net/Why_do_Politicians_Understand_So_Little%3F_Our_Fault_or_Theirs%3F

Tags for the session - technology discussed/ideas considered:

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

I asked the group to help me to develop a narrative around digital identity to help to explain it to politicians, to help them to make good decisions about identity infrastructure.

We discussed a series of paradoxes that might be resolved through digital ID technology and wondered how we might explain these to politicians in order to get action.

Paradox 1: The China Syndrome

Why do politicians want anonymous internet access for free speech in China but not in the UK because of terrorism, paedophiles, stalkers etc etc

Paradox 2: The Chatroom Syndrome

Why do we expect disclosure from other people but don't want to disclose ouservles.

Paradox 3: The Baby Picture Syndrome

Why is it OK to let a baby play naked in the garden where it can be seen by neighbours but not on the web

Paradox 4: The Common Sense Syndrome

When the virtual world has no characteristics in common with the physical world, why to we simulate physical ID

Paradox 5: The Children Syndrome

Why is any ridiculous restriction on online activity proposed in order to protect children

Paradox 6: The Ayatollah Syndrome

Do you want bad guys using twitter or not using twitter

Paradox 7: The Google Syndrome

If the government can "break into" the identity infrastructure, then so can the bad guys.

Paradox 8: The Special Needs Syndrome

Every sector of the economy thinks that its identity needs are special and more important, they can't all be right

Paradox 9: The Whisteblower Syndrome

We want people to blow the whistle but they won't if they can be identified

Paradox 10: The Dangerous Dogs Syndrome

Something must be done about identity -- but it doesn't matter if it makes sense or not

Paradox 11: "The Method" Syndrome

Politicians seem to prefer security theatre to security.

Paradox 12: Pass-the-Parcel Syndrome

Everyone wants something done, but no-one wants the problem.

We then had a very good discussion about the elements of a narrative, which was much to involved to transcribe, but the group did come up with one or two suggestions that mae sense. These included focusing on saving money rather than other benefits, perhaps engaging administrations on the specific issue of digital ID as a way to manage the electronic delivery of public services and less about freedom of speech, law and orders, human rights and other less tangible things that have no votes in them. I can't remember who said it, but someone commented that when it comes to mass-market identity implementations, sub-optimal may be better.

A couple of other tips from the crowd: "fight fire with soundbites" and "use rhetorical tricks" because, I suppose, politicians respect them.

How Do You (we) Manage Heterogeneous Groups (4E)

Convener: Victoriano Giralt
Notes-taker(s): Kaliya Hamlin
URL: http://iiw.idcommons.net/How_Do_You_(we)_Manage_Heterogeneous_Groups%3F

Tags for the session - technology discussed/ideas considered:

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

Issues About Profiling and Cross-Border Data Stores (4F)

Convener: Gianluca Gilardi & Matteo Giovanni Paolo Flora
Notes-taker(s):
URL: http://iiw.idcommons.net/Issues_About_Profiling_and_Cross-Border_Data_Stores

Tags for the session - technology discussed/ideas considered:

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

OpenID the Nascar Problem Revisited (4G)

Convener: Mark Cross
Notes-taker(s): Marc Cross
URL: http://iiw.idcommons.net/OpenID_the_Nascar_Problem_Revisited

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
The Nascar problem narrates the bewildering login user interface that has proliferated since the adopted of OpenID by the founding US corporations of the North American centric OpenID foundation.

I wrongly attributed the OpenID Foundation mission statement present at the last IIW, but this one was infact present by Kaliya Hamlin:

“OpenID Foundation: To foster and promote the development of, public access to, and adoption of OpenID as a framework for user-centric identity on the Internet; and To acquire, create, hold and manage intellectual property related to OpenID and provide equal access to such intellectual property to the OpenID community and public at no charge.” http://tinyurl.com/2ee2tgs

Now as I stated at the session, the first bit just doesn't seem to happening, none of the OpenID Foundation members actually mention that their login is an OpenID to their user base, therefore they are neither fostering nor promoting the adoption of OpenID.

I drew the audiences attention to the parallel of the credit card and OpenID, the credit card was devised many decades before it eventually took off, but then did. OpenID more poignantly is being sidelined in favour of brand values. When you walk into a shop to purchase something, you merely ask whether they accept credit cards or cash only. You don't say, “Does your shop accept my Cat's Charity Affinity Card?”

This observation didn't make any great stirring with the audience, as the technology of OpenID was merely perceived to be single sign-on, or at least from the audiences (customer) end-user perspective. It seems to me that OpenID's early loss was not promoting both *delegation and personal data storage*.

Here is the post-session illustration I should have had to hand, but provides the sentiment I was trying to emote. “You can sign in with any of the following OpenID providers…”

P*ersonal data storage* was not perceived as a major potential of OpenID. OpenID's Attribute Exchange specification is perfect for the personal data store when combined with Oauth v2 / DNSSEC! It was discussed in a minor way between myself and a domain registrar at the table, who saw the *personal data storage* as something that perhaps could be handled by a not for profit, with the knowledge of maintaining high SLA resilient systems. Whilst registries don't want to assert claims, they are already starting to handling important business critical data beyond DNS, such as ENUM. They are mitigating against the risks of offering such services by employing third party independent validation agents.

Audience feedback from the session
79% of Lady Ga Ga site log in via FB/Twitter/Google, few create site account
Logos have trust and brand values
Do we need not for profit OpenID data stores?
Best point to gather information, is at the point of usage.
Task flow – don't disrupt it.

Idea

With regards to the Nascar branding problem, I neglected during the session time to point out that both Orange in France and NTT docomo seem to be quite happy to promote the OpenID brand in a none partisan way.

Another post session issue I would like to explore in the future is finding ways of promoting OpenID Identity Providers to become Personal Data Stores. Then the perceived value from an end-user's point of view of having an OpenID would be much greater.

Session 5

UK Gov. – They Want To Talk Identity. How Do We Help? (5A)

Convener: James Brown
Notes-taker(s):
URL: http://iiw.idcommons.net/UK_Gov._-_They_Want_To_Talk_Identity._How_Do_We_Help%3F

Tags for the session - technology discussed/ideas considered:

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

Embedding Privacy Controls in OnLine Identity Mechanisms: How and Why? (5B)

Convener: Kasey Chapell
Notes-taker(s): Dave Birch
URL: http://iiw.idcommons.net/Embedding_Privacy_Controls_in_OnLine_Identity_Mechanism:_How_and_Why%3F

Tags for the session - technology discussed/ideas considered:

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

The Privacy Policy Crisis: The privacy policies are not appropriate to the technology.

A "legalistic" policy makes no sense because customers can't make an informed choice based on informed consent (see VOME).

Companies are not meeting the "spirit" of the law.

We overly rely on consent.

Is there a way around this?

VOME are working on visualisation.

There are three basic categories of consumers: paranoid, don't care, pragmatists (trust based on other things: brand, and so on).

These groups require different kinds of input and education.

We need a new vocabulary for privacy.

Are we communicating with consumers or with consumer groups?

Watchdogs or crypto?

Lawyers have no incentives to come up with standard policies.

We could ask the technology community to propose alternatives as part of the Commission's Data Protection review but they wouldn't understand them so what's the point.

European Consumer Protection organisation

Touch2ID is an example where the technology obviates the need for privacy profiles.

For targeted marketing, companies don't need to know who you are.

The regulatory environment treats "profiles" as personal information.

Companies are beginning to provide more granularity over the control of data.

The consumer "wins" need to be tangible.

Some data is much more sensitive than others, such as location

Here's an example policy:

Because we understand that you would be concerned if people could locate you without your knowledge, Vodafone takes robust measures to ensure that all location based service providers that use Vodafone network location data as part of their services comply with the Industry Code of Practice For the Use of Mobile Phone Technology to Provide Passive Services in the UK [From UK - About Vodafone UK - Legal Information - Privacy Policies - Location based services]

Google can use location data more freely than telecoms companies, another quirk of the law. This sort of thing happens because privacy regulations are often formed in response to specific outlying events rather than according to general principals.

What can technology offer? Some combination of personal data stores (PDS), VRM and the like.

Is there an analogy between privacy and organ donation? Once you make it opt-in, then participation rates fall.

New legislation will bring breach notification to Europe.

Perhaps multiple identities might provide a way forward: give up on privacy, and when an identity is violated, it gets deleted.

There are no criminal penalties for privacy breach.

How can we balance or cap the liabilities associated with identities? Suppose a mobile phone company was an IDP -- if the liabilities are too draconian then how could it be a business.

One remedy under consideration for review in the data protection directive is a "private cause of action" which means that consumer groups could sue for violations.

Privacy Dashboard Demo (5C)

Convener: Dave Raggett
Notes-taker(s): Dave Raggett
URL: http://iiw.idcommons.net/Privacy_Dashboard_Demo

Tags for the session - technology discussed/ideas considered:

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

This is a Firefox extension that allows you to what data collection behaviours websites use, and to set you privacy preferences on a per site basis, e.g. to block 3rd party content, to clear Flash cookies and so forth.

Initial problems with WiFi and inability to get an IP address. I therefore started with some screen shots from a one sheet flyer (from ICT2010), see:
http://www.w3.org/2010/10/dashboard.pdf

After a while the network weather improved and I was able to show the Dashboard in operation.

In discussion it became clear that there is interest in finding out more about how different sites track people, and exposing the degree to which they do so. This is encouraging as I hope to launch an open source community project to take this further. One avenue would be to pool information collected by different people for a crowd sourced analysis of the bigger picture.

One thing I learned was that some 3rd party ad sites themselves load resources from other sites, sometimes as much as 15 levels deep.

In summary, let's turn the tables on the data miners who are profiling us all, and apply the same techniques on them! Knowledge is power...

I also demoed another Firefox extension I've written, see:

http://www.w3.org/2010/09/raggett-fresh-take-on-p3p/

This uses the P3P 1.1 vocabulary for privacy policies and applies it to a simplified object model, that makes it practical to auto generate the UI for user preferences, human readable policies and reports on the mismatch between user preferences and site policies.

P3P is still in use, but has suffered from its very flexibility.

Microsoft implemented a very small subset (P3P compact policies) which only deal with HTTP cookies. My work covers a wider range -- the things that sites can collect from HTTP request headers during a session.

Identity and privacy are strongly coupled, and we are still at an early stage in how these will evolve online.

By a co-incidence, I watched Sandra Bullock in "The Net" on Sunday evening just before the workshop, see

http://en.wikipedia.org/wiki/The_Net_(1995_film)

The movie emphasises the degree to which our lives now depend on our digital personas and how fragile these can be when subjected to attack.

--
Dave Raggett <dsr@w3.org> http://www.w3.org/People/Raggett

Financial Services – distance selling, money laundering, "Know Your Customer (5D)

Convener: Gordon Rae
Notes-taker(s): Gordon Rae
URL: http://iiw.idcommons.net/Financial_Services_-_distance_selling,_money_laundering,_%22Know_Your_Customer%22

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 discussed the delivery of financial services in the countries of Europe, and the possible contribution that federated identity could make.

Our first observation was that payments and retailing have well integrated infrastructure across Europe; but the delivery of financial services does not have a federated structure even within single countries. Advocates of federeated identity might be pushing against a closed door.

There are opportunities, and benefits. The group identified several.

In the Netherlands companies have financial planning tools that could benefit from using a federated identity mamgt. But federations would need to be established within a single conutry federations first.

E-Invoicing - across borders - is another potentially interesting area which could deliver benefits to participants.

Banks are well placed to be IDPs, and could generate income from providing ID and verifying IDs and claims against IDs; they would also benefit from other high-quality IDPs for distance selling.

Also, identity proofing outside payment is still difficult, e.g. for opening an account over the internet.

The European financial environment is quite restrictive in respect to regulations. The technologies are powerful enough to enable more complex business cases to work across borders. But the regulations are difficult. Savings guarantee systems etc. are bound to national laws.

Because of the banking crisis, European countries are looking at changing the regulations, but they are unlikely to support loose regulations. There is a big

emphasis on consumer protection.

People in the IIW community who are interested in advocating / supporting innovation in this area need to build relationships with innovators in the financial sector, and build consortia at national or regional levels first.

Personal Data Ecosystem.org (5E)

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

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:

www.PersonalDataEcosystem.org

Digital Device Capture Me -> my data store Reliance for individual Me - MyTerms & Conditions

Real World Examples Sexy begin gradually with 10 parameters
Talking to users on the adoption curve.
Interaction Delegation
"people won't care"

Usability experience "digital human rights" evolutionary steps

Operational cost Maintain Data

See math problem of 200 orgs $5 each millions

They Government Bank Telco

- Me->We
- Privacy
- Law? Policy Governing

- Technology Part
- Nori <-->Higgins Interop??

Biz Models?
Academic Authors
How to sell "large org" bank
Giving user control - patients mobile
Questions FAQ's educators, researchers
Research subjects Data Liberation Front

End of the Day Reflection

Reflection on the event from participants: As a result of today….

… I'm updated on where Identity is heading. Only IIW can do this

… I will go back to my company and win the battles on identity and data policies

… I go home with a broadened mind

… I met some significant individuals dealing with similar issues to me, a common language, common concerns, surprisingly a certain reticence to deal with the bigger picture implications etc…

… I hadn't realized the depth of thought from a philosophical perspective in Identity; I had thought it was all technology

… I'm more convinced that the right people are paying attention to the privacy implications of technology

… The future changed for the better. Hopefully including "UK Gov end user privacy sensitive national ID infrastructure

… I have several very useful contacts

… I will bequeath my personal data to my kids!!

… I'm more confused, but at a higher level :-) Great day!

… I am more convinced Educational is a key area for investment

... *I'm excited about the picture, not just on the web, but also computing and networked society. Can't wait to build something cool.*

... *I learned some new and interesting things and talked to new people who inspired me!*

... *I found some new "brothers in arms" and expanded the scope of my projects with new, interesting broader areas*

... *I have a clearer picture of the identity ecosystem and opportunities*

... *deploy a One Social Web node, and connect with the wider world!!*

... *I will use as many identities as I want on line – still!!*

... *I have a wide network of friends in the ID community*

... *I'm going to talk to Dave Birch some more*

... *I don't feel alone anymore! Yeay – everything is possible*

... *I feel I have a community of people who can help me get things done*

... *I'm going to have a lot more work to do*

... *Found my ID*
... *I must look at Web ID!*

... *I will continue to expand and build out the story around personal data management*

... *We are planning more activities*

... *I'm more aware of how corporations are already tracking our personal information and less convinced that the general public can be persuaded that this a problem….*

... *Social Networking is part of next gen identities*

... *I got to know more interesting people in this field*

Who would like to have
a next IIW Europe Event?

About IIW

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/

We are considering doing more events outside the Bay Area branded "Identity Open Spaces" once we get feedback from attendees at IIW East and IIW Europe we will know more about when and where they will be and what themes they will have. If

you want to share thoughts with us on this please e-mail kaliya (at) mac.com and Phil (at) Windley.org.

IIW Events would not be possible without the community that gathers or the sponsors that make the gathering feasible. These were the sponsors and supporters for the First IIW Event in Europe. The event would not have been possible without their financial and energetic contributions. Thank you!