Internet Identity Workshop 16

Book of Proceedings

www.internetidentityworkshop.com

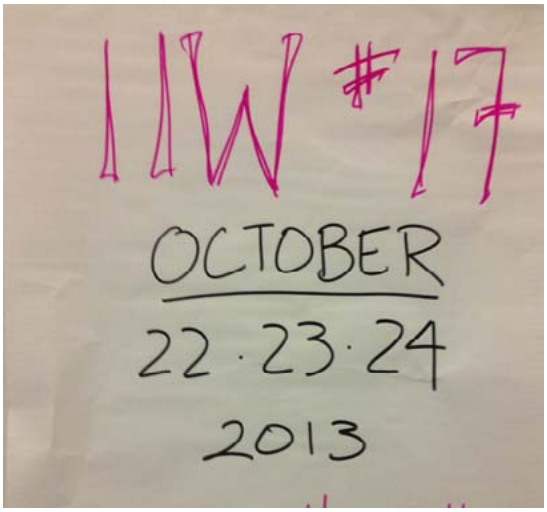
Compiled by
KAS NETELER, HEIDI NOBANTU SAUL AND EMMA GROSS

Notes in this book can also be found online at
http://iiw.idcommons.net/IIW_16_Notes

IIW founded by Kaliya Hamlin, Phil Windley and Doc Searls
Co-produced by Kaliya Hamlin, Phil Windley and Heidi Nobantu Saul

May 7-9, 2013
Computer History Museum
Mountain View, CA

Contents



MITREid Connect

Tuesday 1A

Convener: Justin Richer

Notes-taker(s): Amanda Anganes

Tags for the session - technology discussed/ideas considered:

open source, OpenID Connect, MTIRE, MIT, MIT-KIT

Summary: The MITREid Connect project is an open-source reference implementation server & client library for OpenID Connect. We just released the 1.0 version and it is available on Maven under the "org. mitre" group ID, and on GitHub at https://github.com/mitreid-connect/OpenID-Connect-Java-Spring-Server.

MITRE has been working on this library for about 1.5 years, and it has been open source from the start under an Apache license, so we have had lots of external users and participation from the start.

The code is deployed internally at MITRE at id.mitre.org/connect (but only MITRE employees can log in there).

Several other projects in the healthcare space (RHEx, Blue Button, etc) are using this code.

MITRE doesn't do long-term maintenance (we are a research company), so the MIT-KIT (MIT Kerberos & Internet Trust Consortium) is taking over the project for future maintenance.

The project is built using Java, Spring, Spring Security, and Twitter Bootstrap.

The client code is a Spring Security filter, so it is easy to slide in to existing Spring applications.

We support a few advanced features:

- Token chaining – trade an Access Token for another Access Token
- Dynamic Registration
- Signed Request Objects
- Token Introspection
- All tokens are signed JWTs

We have some other tools available at https://github.com/mitreid-connect/.

Simple-web-app: simple application that shows how to configure filters and settings for our library

Example Maven Overlay: Maven Overlay example, how to extend server code very simply by overriding specific classes & config files. We use Maven Overlays internally for our MITRE-deployed version.

Account Chooser: not related to Google's Account Chooser, this is just a simple JS app that allows users to choose their IDP.

It is possible (and usually easy) to slot in any kind of primary authentication method to the OIDC server. At MITRE< we are connected to Oracle SSO. Outside the firewall, you go through 2-factor authentication; inside you get an SSO experience.

Demo

Questions:

Cross site scripting?

Not turned on (yet), Justin thinks there is a Spring filter for it

Who else is using this?

Several organizations we can't talk about

Maine Health Information Network, RHEx

State of Utah

Clipper (cross-lingual web browsing), another MITRE project, is using this library with Token Chaining

We have PHP client libraries, have hooked up to Wordpress, Elgg, Drupal.

What about the "kitties are fluffy" phenomenon? (ie, MITRE employee uses MITRE OIDC credential to post a random blog comment, is it official policy now? Etc)

It's working so far!

Educate and trust

Same risk as giving employees corporate phone and email accounts

No special disclaimers

But, we are working on a future Trust Framework for the company

The UI is backed up by a RESTful API, OAuth2 protected. MIT will be using the admin API through external web calls (authenticated with an OAuth2 token).

What about collaboration?

The issue tracker is available on GitHub

We do not have a mailing list (yet, MIT-KIT will set one up eventually), but Justin and Amanda's emails are listed on the page – feel free to contact us directly for now.

What about speed? Lots of redirects.

In practice our code seems to operate pretty quickly, haven't had any speed issues.

What about in a constrained environment, can we avoid some of these redirects?

Yes, can use Client Credentials or Username/Password flows.

Scalable Privacy Manager

Tuesday 1B

Convener: Keith Hazelton

Notes-taker(s): Keith Hazelton

The vision: Users have a well-designed tool to more effectively manage the release of their information to relying parties. That tool is common across any number of attribute stores and personal data stores.

The challenge: In practice today if users have any control over the release of attributes it is just-in-time consent via a bewildering variety of approaches. The consent flow depends entirely on the particular pair of Relying Parties (RPs) and Identity Providers (IdPs). My experience with Facebook privacy settings differs from my experience with mobile application install-time permissions differs yet again from, say my university's release of attributes in SAML transactions with federation partner applications and resources.

The proposal under discussion: There are research-to-deployment projects underway by UI and privacy experts to come up with privacy manager applications. If those are architected to be pluggable to any number of back-end attribute and personal data stores, users could end up with a single, familiar tool for managing application and service access to their personal information. The privacy manager would be optimized to do the best job possible of giving users more than a "click-through to get the goods" experience.

In discussion the following points were raised:
- The schemas representing the specific information whose release is to be controlled are not standardized, so it will be difficult to "plug" privacy managers to applications and present the choices to the user in any comprehensive and broadly understandable way.

- How does one oblige the RP not to do an onward transfer of information (downstream data release) once the RP has the data? What combination of rules and tools could address this problem. One model is the User-Managed Access (UMA) notion of "binding obligations" perhaps backed by a federation or trust framework model that limits onward transfer as part of an "acceptable use" policy. If violations are discovered, the appropriate federation/trust framework could specify the consequences. The problem is a hard one at the end of the day.

- This vision is premature because it can only succeed if there is a meaningful and widely deployed means for the mutual authentication of all parties in the transaction. If I don't really know to whom I'm releasing information, I can't meaningfully manage the process. One response was that we can move in the direction of the vision, in favorable, constrained scopes for now, such as the higher education SAML federation space where the RP identities are well managed. If OpenID Connect or other approaches to RP authentication becomes ubiquitous, then the scope across which privacy managers operate could grow.

Rent or Buy: Taking Control of Your Credit, Reduce Your Mortgage

Tuesday 1C

Convener: Kevin Cox

Notes-taker(s): Esther Makkay

Money is a social construct and can be thought of as IOU's. Our normal money is an IOU that issued by the government that says we can use the money to pay our taxes.

Banks today create most of the IOU's. 97%+ of all money in circulation are IOUs issued by banks.

There is no reason for each of us not to issue our own IOUs. That is, one form of personal data is the IOU that we can control.

Bank IOUs are issued with interest attached. When a bank issues a loan to an individual the individual takes on the conditions of the bank issued IOU and agrees to pay interest on the IOU. Because interest is itself an IOU we end up with IOUs that compound in cost.

If we issued our own IOUs directly to a lender then we could issue them with different conditions including having no interest. Rather than interest to compensate the lender we could give the lender rent on the product or asset we purchased with the IOU.

An example of how to do this is being built. At the moment it is called Rent and Buy but will probably be called something else when finally launched.

The system looks very much like the current system because people understand mortgages and people understand rent. It can be thought of as renting money to purchase part of a house. The buyer buys part of the house with a deposit and the loan money is used to purchase the other part of the house. The rules of the IOU or loan are different.

When a repayment is made the money comes directly off the loan.

Rent accumulates until the loan is paid off and then the rent is repaid

Rent does not attract interest.

The Loan plus Rent outstanding is adjusted yearly (or monthly) for inflation.

These set of rules make a difference to both buyers and sellers. The total amount of present day funds transferred between buyer and seller reduces by the amount of interest on interest. By increasing the amount owed by inflation means that the effect of inflation on transfers is cancelled out.

For a 25 year loan at 7% the borrower has a reduction in repayments of 60% - but the repayment amount increases with inflation. However, for most borrowers their income increases with inflation and so the increased cost in present day terms is the same. If the borrower cannot increase repayments then the length of the loan can extended with no loss in value to the lender.

For a lender they receive a 6% return on the money invested that is inflation adjusted. That is if inflation was 3% then the return is about 9% fixed. This is a superior return for most annuity low risk products.

For lenders interest with Rent and Buy is classified as a Capital Gain while interest on a traditional loan is classified as income. In many countries the tax treatments are different.

The system should be operational towards the end of 2013.

Rent and Buy illustrates what can happen when we take control of our own personal data which in this case is our own IOU or own ability to create credit.

PAL: Program Aggregation Layer: Interoperability of

Tuesday 1E

Convener: Kenneth Lefkowitz, Emmett Global

Notes-taker(s): Kenneth Lefkowitz

Many solutions are available in this innovative space. The innovations and services are labeled with names such as tracker blocker, ad blocker, personal data store, personal cloud, authentication scheme, authorization scheme, intent-casting, life management platform, trust network, etc. Solutions are more or less interoperable depending on their API (eg JSON), base paradigm, data structure, and communication protocols.

People at the session were very interested in

- Identifying best of breed solutions

- Integrating the various solutions

- APIs

- making services pipe-able, such as bash on the linux command line

- the ability to script the above pipe

- content addressability

Emmett Global discussed their process for identifying candidates for inclusion in the PAL, a collection of solutions meeting the goal of a simple, one-click set of services and data stores that enables fast, safe internet surfing. The process works like this

- Clarifying the requirement

- Searching for candidates

- Examining the license and business model of the candidate

- Examining the code base

- Assessing integrity of the community, last updates, who are the “star” or lead developers

- reading reviews of users

Besides the above metrics, the software can also be assessed by more complex and nuanced qualities. Emmett uses “CANDOR” as its guide, an acronym for qualitative values Consent, Attribution, Notification, Dignity and ongoing Remuneration. To assess these, we recommend an A/B comparative process. While it is almost impossible to define “dignity”, people have a remarkable consensus when presented with two choices A and B, and asked to rate which one accords more “dignity” to the user than the other.

In discussion, the following points were raised:

- The aggregating organization should make explicit the taxonomy of requirements

- Terms of Service need to be considered

- an innovation incubator is a good setting to test these kinds of integration

Infosharing

Tuesday 1H

Convener: Joe Andrieu

Notes-taker(s): Joe Andrieu

See infosharing wg on Kantara.

It is a nutrition sharing information about my personal information, at the point you are about to share the info at the transaction. ToS too hard, and encourage click train..

Started with per transaction contractual agreements, moved to simple representation of labels, something you can check as opposed to breaking up your session.

Related to Mozilla and ToS DR, and Lloyd Kramer @ Carnegie Mellon nutrition facts privacy label cor the whole site like P3P.

Question:

Is there a role for legislation

Do people read labels?

What info goes on the label?

What are users looking for? Automate the notice? Tags/filters?.. road/traffic light sign type logos.

How do users share back why a user didn't share their info?

Do people see sharing as a problem..

What will change my behavior when asked to release my data?

It's easy

Friend says is scary/crowd sourcing

On-selling data

Viral exposure

Unknown 3rd party redistribution

Clear value prop ….compensation – trading your information to receive a benefit. Quid pro quo..

Ability to negotiate, opt in, opt out

Social, fun and useful and in context.

Paying attention to the label 'after the fact'..e.g. when doctor says you are sick. So you need a 'health check'

Education and awareness

Peer pressure

What are the inflection points? Mobile, cookies, SSL

Behavioral characteristics:

Drive to acquire

The drive to bond..

The drive to learn

The drive to defend

The drive to feel

How to avoid irrelevant marks becoming ‘marketing’

Bacon labeling. an example of behavioral influence…

Raw-cooked, rating score, presentation, but all on one service level. What is wrong is there are different rating systems and these should be distributed, accessible for users

Salesforce Identity Q&A

Tuesday 2G

Convener: Pat Patterson, Chuck Mortimore

Notes-taker(s): Vikas Jain

Q. What’s Salesforce plan around user provisioning, SCIM support?
A. We currently support Just-in-time provisioning through SAML and Facebook. We plan to add SCIM support in the next couple of releases. Right now watching the market adoption for it.

Q. Will responsibilities be provisioned too?
A. Yes

Q. Does Salesforce handle multiple Identity providers?
A. Yes, it will be out in Summer ‘13 release

Q. How does Salesforce whitelist the IdP
A. Through explicit metadata exchange with the IdP

Q. For Google, can we trust specific google app domain names
A. Yes, you can do it through the custom code in the Auth registration handler.

Q. Can Salesforce allow login through trusted identities that are identity proofed?
A. Not today, but we are looking into it.

Q. What are you doing for sessions?
A. We are adding session levels (aka assurance levels). We are going to allow authentication that yields a particular session level, step-up authentication, etc.

Q. Are you finding any existing assurance profiles that you plan to use or is it just Salesforce assurance levels?
A. Salesforce assurance levels.

Q. Can Salesforce Identity be reused to login to other web properties?
A. Yes, Salesforce can act as Identity Provider today such as to Docusign.

Q. Can Salesforce convert OAUTH to SAML?
A. Yes, Salesforce can broker incoming identities from one protocol such as OAUTH, and convert it to other protocols such as SAML as outgoing protocol.

Q. Will the NSTIC trust framework help Salesforce?
A. Customers today are using bilateral agreements. In some cases, they have established their own little trust framework by using RNS attribute in SAML assertions. That said, we are watching NSTIC trust framework.

Q. What's Salesforce direction on SAML metadata exchange?
A. There's currently metadata export. We have stories in the backlog to have metadata export through addressable URL. Then, we plan to look into metadata import.

Q. Can Salesforce can go out and acquire attributes from other attribute providers?
A. We can accept attributes from authentication flows such as SAML and OpenID.

Q. Is Salesforce designed as one IdP or N IdPs?
A. N IdPs for SAML, one IdP for OAUTH. But, for OAUTH we allow policies that each IdP can establish control.

Q. Access to federal govt resources with Salesforce as an IdP?
A. Defintely as an SP. As an IdP if federal govt customers are using it, we aren't aware of it.

Q. Is OpenID connect on the roadmap of Salesforce?
A. We've it in pilot, and will be releasing GA version in couple of releases.

Q. Does Salesforce provide APIs to revoke the tokens when a user leaves the company.
A. Salesforce doesn't expose API to revoke OAUTH tokens remotely, but it exposes API to deprovision (disable) the user after which access to all Salesforce resources are disabled.

Ego Identity

Tuesday 2H

Convener: Alan Karp

Notes-taker(s): Amanda Anganes

Tags for the session - technology discussed/ideas considered: definition of identity, psychology

Erik Erikson "Identity and the life cycle", child psychology http://www.amazon.com/Identity-Life-Cycle-Erik-Erikson/dp/0393311325

very hard reading – Alan did not read the whole book and does not recommend it

Book defines "Ego Identity", which is "how does the child come to know about the child's self":

sense of child's own continuity in space and time

AND

the recognition by others of those properties

Personas - we know Alan as the IIW attendee

HP knows him as employee

wife knows him as her husband

Organizations have continuity in space & time and we think of them as identities

Definition doesn't include recognition of others as being "other"

Definition of self as not belonging to other groups, not being the same as other individuals

*Boundary - recognition of boundary

Who is allowed to use an organizational identity

related to discussion of Anonymous

Jeff Jonas, “space time travel data” talk

he builds fraud detection for casinos

take question of two twins on stage presenting the same identity-which one?

physical body has continuity over space & time so that is how you recognize the real one

Perhaps we don’t need both components? My self-asserted person, plus personas that others recognize; could be two different things

I don’t have control over what an external circle identifies me as

Identifier vs identity

If I self-assert something about myself and others don’t verify, it is not a valid ego ID

IDESG discussion about definition - WHY do we need to define Identity?

how is this useful? What does this help us with when looking at identifies and internet id?

Alan says we can attach trust to this definition of ID

Mark Miller, Jed Donnelley and Alan wrote paper called Horton’s “Who Done It?” http://www.erights.org/elib/capability/horton/

If Joe introduces me to Peter, I will hold Joe responsible for Peter - sock puppet, no Ego ID

If I later receive independent knowledge of Peter, now I hold Peter responsible for himself

now Peter has an Ego ID

Recognition forces it to be “owned” by others - I do not “own” my Ego ID, others “own” it when they recognize me and form an Ego ID of me

How is an identifier related to an Ego ID? When I send an email to you, I recognize your continuity in space & time and you have Ego ID

Fraud makes this interesting - creates a discontinuity of “own self”

This is NOT verifiable - not practical, this came from a psychologist!

Thinking about this definition may help us avoid vulnerabilities

Mark Stigler, short story “The gentle seduction”, about the singularity

Short Cuts, short novel

What about replacement? Where does continuity stop? All of my cells have been replaced since I was born, new person? Organization has members, buildings, etc. that constantly change.

AT&T was bought & sold as a brand, now discontinuous

Identifiers are completely separate from Ego ID

HP & Agilent - HP recognizes itself as the continuation of old HP, but really Agilent (instrument company) is what HP used to do. Label has moved, ego ID is still intact through split. Agilent has its own new Ego ID?

For corporations, who decides what “the corporation” believes it’s own self to be?

Privacy Features of Authentication Methods

Tuesday Lunch 2H

Convener: Francisco Corella

Notes-taker(s): Karen Lewison

Tags for the session - technology discussed/ideas considered:
Privacy, authentication, privacy enhancing technologies, crytographic authentication

Presentation/discussion notes:

A survey of 18 different authentication technologies was presented, based on a presentation at ID360 2013 in Austin TX, which

consists of a classification scheme and a privacy feature matrix.
Summarized in a table with two parts--

1. 4 facets of classification--how the service provider receives identity and/or attributes, 2 versus 3 parties involved, attributes v identity,
open v closed loop

2. 7 privacy features

In-depth discussion of the included technologies and their privacy features. Lots of useful feedback from both the

session participants, and from an online discussion started the prior day on the IDCommons mailing list,
which will be included in a revised paper.

Links:

Paper

Table

Poster

Blog post

Personal Cloud Discovery with XDI

Tuesday 3B

Convener: Markus Sabadello

Notes-taker(s): Markus Sabadello

We talked about some of the technical challenges in building a distributed system of Personal Clouds, especially around interoperability and discovery. We spent time with a demo application that illustrated how these challenges can be solved with XDI. A central part of this is the introduction of Cloud Names and Cloud Numbers, which are identifiers that are used to point to Personal Clouds and discover them. During the session, several participants registered Cloud Names for themselves.

One focus of the demo application was to show that in such a system of Personal Clouds, several

parties can be involved and interact with each other in various ways, e.g. Cloud Service Providers, Registrars, Registries, and of course individual Clouds. In this system, no single centralized party is involved. Instead, XDI messages can be exchanged between any one of them in a peer-to-peer pattern.

After the initial steps of registering Cloud Names, we also looked at what XDI data looks like on the low technical level, for example when storing a "first name" attribute in a Cloud, or when linking an attribute in a Cloud to an external non-XDI data source such as Facebook. There was some discussion about how to achieve interoperability between heterogeneous data models, which in XDI can be done with "dictionaries". Finally, basic "link contract" functionality was also shown, i.e. the ability to make certain data in one's Cloud public or private.

This session effectively gave an overview of the "developer alpha" stage of XDI infrastructure that will become the basis of the Respect Network. A fully functional network with all components in place is expected for the end of the year.

"An Auth reqeust you can't refuse;" The OAuth Complicit Flow

Tuesday, 3C

Convener: Justin Richer

Notes-taker(s): Jason Cowley

Tags for the session - technology discussed/ideas considered:

OAuth

Applications tend to ask users for excessive permissions

Users grant permissions without thinking

Abuse of TOFU (trust on first use) model

Key problems

Users don't really see permissions being requested (e.g. like a EULA that user's never actually read)

App developers tend to ask for as many permissions as they may ever need

Related Issues:

Course grained vs. fine grained permissions

course-grained results in less control, over-permissioning

fine grained results in too much information (EULA type page that users don't read)

Goal: have apps ask for only the permissions they need when they need it

Additional Notes:

Facebook allows users to de-select individual permissions, which does put some fine grained control

back in the user's hands at authentication / authorization time

Some kind of "progressive permissioning" model would be desirable, without the need to re-auth the user

Apps could get permissions as needed

Ideally, minimal or no user inconvenience to grant additional permissions

Could have classes of apps, or classes of permission sets that are vetted and shared

Recipes of permissions that users create and share

App store model (aka "walled garden") can rely on the app store to vet apps and reject apps that abuse permission

Patient ID and the Fair Info Practices for ID

Tuesday 3E

Convener: Adrian Gropper

Notes-taker(s): Scott Mace

Adrian: A well-defined patient ID is essential.

Frameworks of patient ID can allow for auditable criteria.

First level: Clinical encounter. Data doesn't go anywhere. Isolated.

Second level: Payment/association. No need to introduce external sharing beyond that.

Third level: Aggregation (registries).

Third (B) level: Coercive – PDMP, mental health for guns registries

VHID, a proprietary scheme for one group that hands out unique identifiers.

EMPIs vs GUIDs

The challenges are cultural and legal, more so than technical.

Adrian: I have never seen a study that payment fraud is a problem other than intentional sharing of identity in places like New York; identity theft at the medical record level that can be tricky to unwind.

It's the economic value of the information. One respect is the ability to do value-based rewards or shared savings. The other one, more important, the institutions want to lock in patients and providers to negotiate better (37:00).

How does Partners manage to get a 30 percent premium?

Michael: Healthcare is very personal. Within our system – we're in 23 states – if you go up to Alameda, there's a good chance we have no idea who you are. What if they come in an ambulance and they're unconscious?

How do we deliver the highest quality of care? Patient ID is another word for transparency.

The Patient Privacy Rights Proposal has two components. Globally unique voluntary ID should be a Direct email address. It's voluntary to the extent the Direct standard allows for a Direct certificate to self-sign. (42:00). At that point you have a system of verifying when I seek care from you. You

want to know you're in control of that ID. You just send me an email. This is within the existing law. Meaningful Use. Direct is in 40 of the 50 states, not sure what the number is.

The second thing we recommend, there is the W9 form. The thing that has your SSN, name/address, signature, and some governance, the IRS. Standardized form with one purpose. Make sure people aware on both sides as to how they are being tracked or their info is being aggregated. So having a W9, if you are going to allow for a transparent, non-coercive way of doing aggregations, the easiest way to do it is ask people what ID they want you to use (??). If patient forgets the email address, create a second one. Possible to do what's being done in India, shoot first and ask questions later.

Free Trade Zones

Tuesday 3I

Convener: Colin Wallis, Jeff Stollman

Notes-taker(s): Jeff Stollman

Building general-purpose trust frameworks is something hard that attempts to do something that has never been done: build a global (not just a multi-national) system. Because the internet is global by definition, general-purpose trust frameworks would be open to anyone, unless specific efforts were undertaken to restrict them.

Problems with multi-jurisdictional systems is that local laws/regulations are often at odds with each other. This imposes limits on our ability to forge global systems.

Two concepts might help address this:

Free-trade zones that allow data storage and handling independent of such current conflicts as laws the demand immediate destruction of certain data versus other laws that demand retention of the same information.

Treaties that exempt certain activities from local law and allow for a consistent legal regime for those activities among treaty signatories.

We discussed the fact that one way to initiate these concepts might be to follow the money, notably international money flows. Begin with small countries that transfer lots of money (e.g., Liechtenstein or Luxembourg) and have less incentive to resist being a free-trade zone because they would gain business, rather than lose it.

Forever: Personal Cloud Application Architectures

Tuesday 4A

Convener: Phil Windley

Notes-taker(s): Phil Windley

Slides to presentation:

https://dl.dropboxusercontent.com/u/329530/Forever%20Demo%20Deck.pdf

Mobile Single-Sign-On

Convener: Sascha Preibisch

Notes-taker(s): Sascha Preibisch

- Topic: Mobile Single-Sign On (MSSO)
- goal: users should only login to the first app using username/ password. This app will receive an access_token and an id_token. The id_token will be shared with other apps. Other apps will reuse the earlier issued id_token to request their own access_token
- target environment: enterprise apps, signed by the same developer key
- what was discussed/ showed:
-- explanation how mobile single-sign on can be implemented using OAuth, OpenID Connect and JsonWebToken
-- client apps would keep their oauth access_token for them selves but they would share the id_token
-- client apps would also share an app-generated private key which would be used for ssl with client authentication if it is required

Identity Federation: Failed Consumer Experiences and What We Can Do About It

Tuesday 4G

Convener: George Fletcher

Notes-taker(s): George Fletcher

More and more sites are requiring additional forms of authentication in addition to a federated assertion. For example, a site will use Facebook Connect and then in addition ask the user for an email address and password. This creates a security vulnerability for the user and is a broken experience. Relying parties do this because there are a number of issues not currently solved by the existing identity federation flows.

RP Concerns
* Federated IdP auth is not strong enough
* Account recovery flows
* Merging duplicate accounts
* Forgot IdP problem
* Support delegation (password is a broken form)
* Authentication to mobile apps
* Liability and dependence on external party (no contracts)
* Legacy system already takes username and password (maybe requires it)
* Misunderstanding of the value of federation
* Lack of knowledge or understanding
* Return on investment of depending on federation (or lack there of)
* Lack of a successful identity standard (or maybe to many viable standards)
* IdP policy mismatch with RP policies
* IdP data use policies

Consumer issues
* Lack of consumer demand (they are happy with passwords)

* Don’t want to share data in addition to identity
* Don’t understand the risk of reusing passwords

The Business of Personal Clouds

Tuesday 5C

Convener: Gary Rowe

Notes-taker(s): Drummond Reed

This session was to discuss personal clouds as a business proposition, i.e., how there could be a healthy flow of value within the personal cloud ecosystem without conflicting with the core principles upon which personal clouds are based (data control, app control, terms control).

Gary started by explaining three overall approaches:

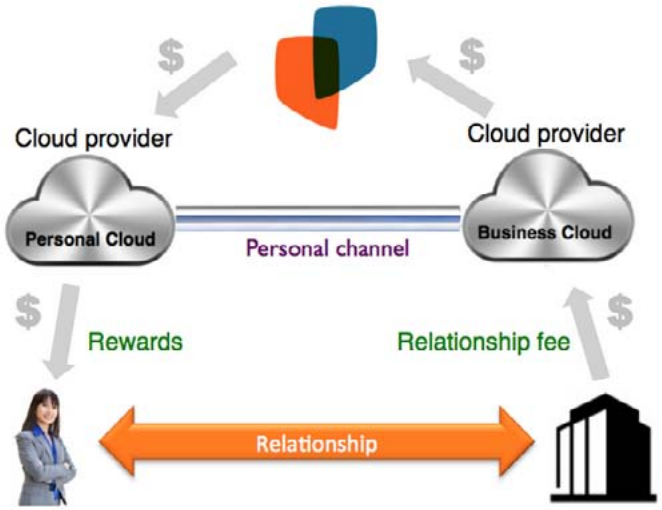
The relationship fee model.

An “enlightened advertising” model.

A CPM fee-for-cloud-lookups model.

With regard to the relationship fee model, Gary explained the basic idea is that businesses will pay to connect to user’s personal clouds because they want the value of the relationship. This is the business model being pursued by Respect Network. It is explained on the Business Model page of their website and shown in the two graphics below.

With the Respect Network, people and businesses are represented by a cloud service provider (CSP) who belongs to the network (or they can self-host). The network and the CSPs are paid for by relationship fees from businesses based on the value of the customer relationships facilitated by the network.



This session was to discuss personal clouds as a business proposition, i.e., how there could be a healthy flow of value within the personal cloud ecosystem without conflicting with the core principles upon which personal clouds are based (data control, app control, terms control).

Gary started by explaining three overall approaches:

The relationship fee model.

An “enlightened advertising” model.

A CPM fee-for-cloud-lookups model.

With regard to the relationship fee model, Gary explained the basic idea is that businesses will pay to connect to user’s personal clouds because they want the value of the relationship. This is the business model being pursued by Respect Network. It is explained on the Business Model page of their website and shown in the two graphics below.

Identity & Government

Tuesday 5D

Convener: Kaliya Hamlin, Elisabeth Mouchy

Notes-taker(s): Scott Fehrman

European workshop for identity workshop, how diff countries are doing it

Who uses eID, Nordic countries: 1/3 people

Who uses smartcard

England pulled out of identity program

France:

Mapping digital identity to Physical (name, address, etc.)

Use of postal service to process the identity, (like facebook connect model)

User can manage their own account

United States:

What does the US do?

Gov employees have internal processes

looking at USPS for citizens

Identity Lifecycle Flows:
Id Proofing
Enrolling

Countries:
United States
France
South Africa
Finland
Sweden
Canada
Belgium
Italian
Spanish
Norway

England
Germany
Japan
India
New Zeland

Two perspectives:

(Common Law) Person: your who you say you are

(Napoleonic Law) Agency: you are what we say you are

Issues:

How do you identify a new user

Authoritative sources

What problem are you trying to solve (what is in/out of scope), mandatory, optional, prohibited

What is benefit to the citizen

Government is suppose to provide services to citizens

Authentication mechanisms

What are peoples “legal rights” in myself as human being

Gov data aggregation practices

Liability, responsibility

Who can / should be an identity provider (should a federal gov. be an identity provider)

What used for health / tax, public / private

France postal: digital verified mail, banking (soon), digital safe vault, authen to website

Adoption rates, what is optional / mandatory

What services can be actualized with an “in place” infrastructure

Precursor: document authority (trust level)

What has been tried ... (and failed)

Data protection privacy regulations

Risk level schemas for countries

Range of attributes (schema alignment / mismatch)

What “is issued” as credential

User consent, flow requirements

Who (agency) is authoritative or not

Age of issue

Proxying / delegation (youth / elder) eTrusteeship

Vertical integration

Phase of lifecycle ... continuity

Biometrics

How is it “monetized”, make money, save money, just because we are government

Federated SSO for Multi-Party (IdP-IdP) with Standards Based Solutions and Maximize Interoperability.

Tuesday 5E

Convener: Steve Tout

Notes-taker(s): Steve Tout

Problem: Discuss various ways to build federated SSO for multi-party, where IdP looks to federate access with another IdP, and develop a standards based solution and maximize interoperability.

Discussion:

Steve provided high level overview of Use Case

IdP #1 wants to send SAML assertion and SSO user into the IdP #2 premises and into a target destination (as opposed to a generic landing page or dashboard)

IdP initiative SSO

N number of target systems in IdP #2 which a user might need to SSO into, and most cases are unique to the user

Explained that SP initiated SSO is already proven and not a requirement

Fielded questions about nature of target applications

Explained that target application may or may not be SAML compliant, and one should not assume that it will be. In other words, it could use Kerberos, WS-Trust, access token, etc…)

General confusion and questions about why there is no SP in the initial drawing on whiteboard

Explained the requirement that to not be forced into having a 1-to-1 relationship between SP and downstream target system and thus the desire to avoid having an SP profile for each target system

Peter made the suggestion to look at the Delegated Auth portion of the SAML spec (which he contributed) as possible use in the solution

Peter shared his experience implementing a “Concierge Service” for UltraViolet to abstract the underlying authentication mechanisms or protocols and suggested that a stronger protocol bridge/ architecture was needed in order to realize what he thinks is trying to be achieved in the use case presented

Several folks who are contributors to the original SAML spec (such as Peter and Prateek) and few others chimed in to explain that this is the classic use case for SAML

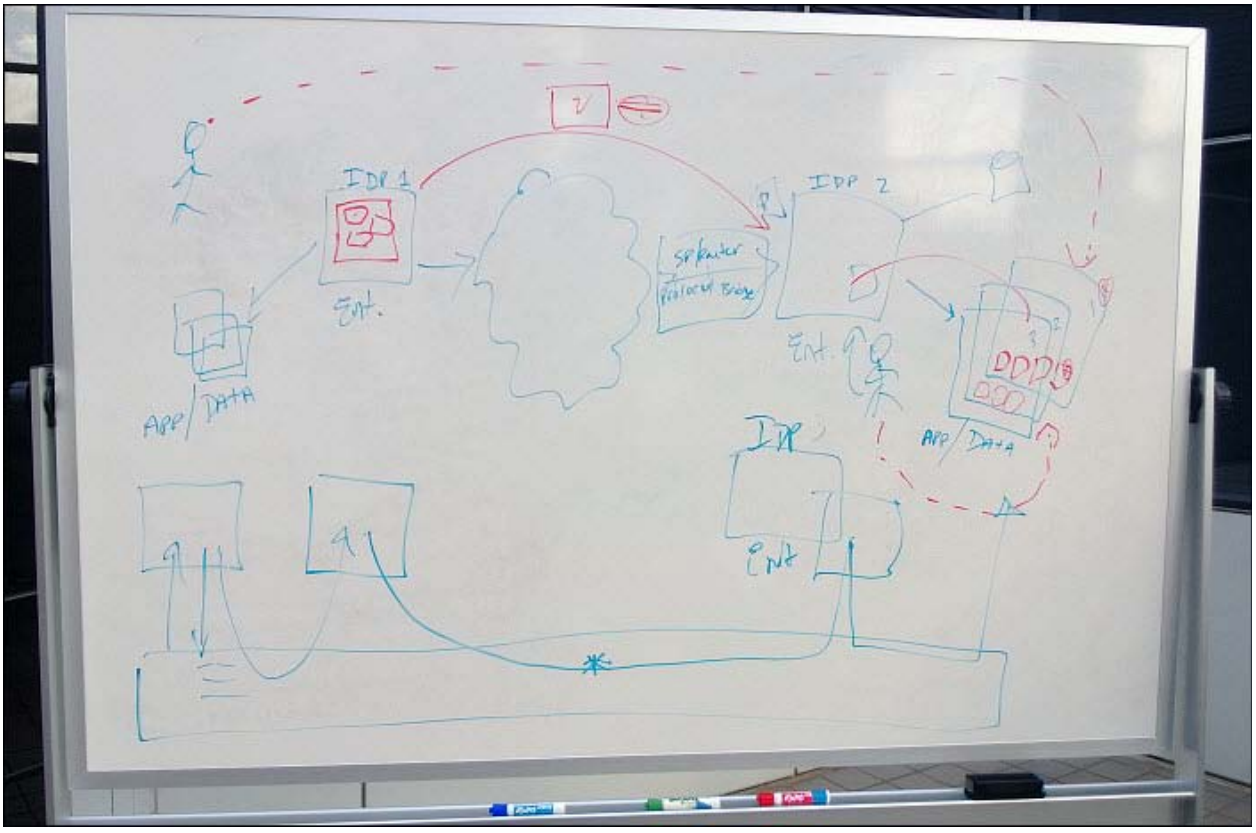
Paul jotted down a high-level flow of how the interactions between IdPs and subsequent down-stream protocol conversions would work together

Chuck encouraged the strict use of HTTP and URLs for evaluating incoming requests and parsing in order to route it to the appropriate authentication protocol or mechanism that can support that request

Prateek made mention that the SAML spec made provision for this exact use case

The general consensus among attendees was that this use case would not be possible without the use of a SP profile on IdP #2 and that the solution is made more dynamic and scalable by having a some type of protocol bridge/proxy or concierge service to handle the routing and upstream/downstream conversion of Authentication request types

Whiteboard:



Digital Identity in Smart-Device Era

Wednesday 1A

Convener: Takashi Kusumi

Notes-taker(s): Takuhiro Yoshida

Tags for the session - technology discussed/ideas considered:

SMS Authentication, QR code

Introduced to the registration and login system of LINE(Japanese mobile messaging app)

- without password
- registration using phone number and SMS authentication
- remote login by QR code scanning of mobile app
- not common authentication, but only in LINE

Discussed QR code authentication and the other authentication using mobile app.

- use QR code as ID (but who issue it?)
- a picture of license is easily faked, but QR code is comparatively secure.
- useful for low value services (e.g. messaging app)
- difficult to introduce it to high value services (e.g. payment)

How do we login to future device like Google glass or iWatch?

- wink
- QR code

Group Identity

Wednesday 1B

Convener: Phil Wolff

Notes-taker(s): Barbara Bowen

Tags for the session - technology discussed/ideas considered:

Focus: model services that are appropriate and flexible for an endless variety of group identities.
Goal: presenting groups as entities outward facing and addressable by machine or human.
Discussion on essential importance of group identity, it begins with mother and child.
Group dynamics will continue to expand exponentially with additional 1 bn people online in next decade
Some examples of collective online identity
- family - individual relationships presented as entity
- investment - ownership
- enterprise

- events
- locations

Comments and Concepts
- Open social specification concept of a group is defined by individual identities.
- Authenticate individual and then access permissions and status
  - Applications can give meaning to what groups do
  - Ad-hoc overlay onto personal address points.
- Concept of personalization for a group
- groups with nda and updates.
- references with identifiers
  - portable and referenced
  - manage personalities in context

Example with Xbox media apps, movies, games family entertainment preferences.

UI group defined attributes-with administration panel (viewer control levels) could be changed dynamically; on or off, and persistent or temporary

Conclusion: Very difficult problem, yet big opportunity for personal cloud application developers

Relying Party Assurance

Wednesday 1D

Convener: Ben Wilson

Notes-taker(s): Ben Wilson

Not all identity solutions are created equal and trust frameworks vary from community to community. A free web mail or social network account has a low threshold to obtain.

The value of an identity credential/solution depends on factors such as the number and quality of associated claims and subject attributes and the overall security of the solution. As a generalized illustration, a credential maintained using a stronger password policy is more valuable to a third party than one with a week one.

Vetting process to issue credential, what proof goes into it. How do we elevate low assurance credentials to higher levels? One way is to go back to the local communities where face-to-face interactions occur and interject human involvement in the creation /upgrading of these identities.

The market for identity solutions is comprised of multiple submarkets of identity tokens, attributes, and claims. A credential issuer able to assert claims of “country of residence” and “age over 13” might augment its credential by acquiring additional claims from a third party. That relationship will require a contract or other legal memorandum setting forth the strength of the assertion, liability, etc. Embedded in such relationship will be enforcement mechanisms to help ensure the accuracy of the claims made.

Information sharing can be limited by scope, subject matter, permitted use, etc. For example, the

claim/attribute provider could say, “I provide this information with the express restriction that it be used only for the patient’s health and secured in accordance with HIPAA/HITECH.”

The claim/attribute provider might say, “I take no liability” or “I back each assertion with maximum liability of $1.” This is where insurance backing might come in. For information security or contractual liability reasons (insurance-backed warranty), each solution provider (and each contracting partner, relying party, business, consumer/subject) might want to ensure that the total potential liability is covered. Insurance companies have the best experience in the area of evaluating these types of risks. Trust frameworks need to also be aware of and/or educated about contractual liabilities and risks.

One postulate of economics is that markets operate more efficiently when there is better information available for all parties involved. “Information” includes each party’s understanding of the rules and risks of the market and the products involved. A relying party (service/resource provider) in the market for an identity-attribute solution needs to know what each service provides.

The relying party / service provider / attribute consumer might only need to purchase the solution once. After that, it has a relationship with the subject, and a trust relationship can build upon that initial enrollment. If a third party identity credential is used, then if the credential is compromised or if required by token management processes, the solution might need to be consulted again for re-enrollment.

Inter-Framework Relationships

Each trust framework evolves with its own social contexts, underlying assumptions, frames of reference, liability rules, contracts, enforcement mechanisms, etc. These will all need reconciliation. The federated credential market needs common rules for levels of assurance and

A cross-framework legal model requires a common vocabulary and frames of reference. The legal document will likely contain certain boilerplate that both sides can agree upon relatively easily. The difficult work will be in creating a framework-to-framework comparison/cross-walk/gap analysis. One side may be asked to change parts of its model / policy / rules for better interoperability. Equivalencies will have to be agreed upon by both sides. Cross-trust between 2 frameworks requires at least 4 trust decisions—(1) does TFa trust identities/attributes/claims asserted in TFb; (2) does TFb trust identities/attributes/claims asserted TFa?; (3) does TFa trust the permitted uses of information within TFb?; and (4) does TFb trust the permitted uses of information within TFa?

Some frameworks are likely to be inherently incompatible.

Work going on in Refeds and OIX might be helpful and/or important.

Login Hint for SAML?

Wednesday 1E

Convener: Mike Jones

Notes-taker(s): Prateek Mishra

Do SAML authentication flows (AuthNRequest <--> AuthNResponse) accommodate
the SP providing a way to give a user-name hint? One requirement is that
the IdP should NOT fail if this hint does not succeed. So if the SP offers
“sam@yahoo.com” and the IdP can only find “samuelo@gmail.com” after user authentication,
that’s OK.
-discussion-
Mike - the desired solution is pragmatic (should work with existing SAML infrastructure)
and should not involve extension or new protocol flows.
Consensus: not clear if the current flows (as described in the samlk core specification)
includes this case. It will be helpful if attendees check their implementations and figure out
if this case is handled, and if it is, how it is achieved.

Human-to-Human Delegation Issues in Open World

Wednesday 1G

Convener: Hidehito Gomi

Notes-taker(s): Amanda Anganes

Tags for the session - technology discussed/ideas considered: Delegation, human interaction, OAuth 2

FitBit, NIKE air band, personal information tracking – data is viewable on your smart device and also shareable

Human-Human – directly sharing information with other people

This is more often accomplished in the real world via human-software (or software-software) interaction (unless you email someone an access token)

OAuth example on the board – Alice stores her data (including personal health records) on a server, using an OAuth token; application can access the data using another Access Token

What happens when Bob wants access (and Alice wants to give it)?

Bob talks to the application; connection between Alice and Bob is not tight. This is possible using OAuth 2.0 flows / UMA where Alice can grant access to Bob so he can get a properly scoped Access Token to access the data.

Enter Carol, malicious. She tries to intercept token from Bob – if it is a true bearer token, then she can use the token maliciously to get the data.

Solutions – SSL everywhere (can use Bearer tokens), or stronger signed tokens (such as SAML

assertions).

Open World – no pre-arranged agreements, Bob may not necessarily have an account on the same IdP that Alice is using. We don't want to assume a full PKI environment.

If you can assume SSL everywhere then Bearer tokens may be OK in this scenario.

Hidehito's proposed solution – we need delagatee authentication

But how to do this with non-connected IdPs?

Identity federation? Doesn't quite fit with Open World assumption.

Or, Alice puts in a rule that says Bob, authenticated at IdP2, is allowed to access her data as long as he can prove that he is Bob at Idp2.

This requires some amount of channel/message security

Cryptographic notion of the "1 free round/message"

PIN transfer, secret exchange, etc

If you can do a secure secret exchange, can use same client secret from both Bob & Alice. Still have the problem of getting the secret to Bob over a secure channel, and man-in-the-middle attack.

Hidehito – what about some kind of "context", such as geolocation

This is easily forged, VPN tunnels into particular locations

We need a formal definition of the problem – security framework, assumptions, use case, threat model – then we could talk about proper mitigations of attacks.

Action item – if Hidehito can contribute to notes his description of

Goals

Assumptions

Network model (what is open, what is not)

Threat Model

Then we could continue conversation further

For example, it matters who Carol is and what she knows/how she is attempting to attack & intercept the personal health records.

Can we assume that it would be OK to transfer "1 free message"? Once a secret is established, we can establish a secure channel.

Alan Karp from HP showing a demo of person-to-person sharing; "Home Page for Sharing"

Family with data for each person

Lisa can share data with other family members, see what she has shared

Home page is protected with URL containing unguessable random home page URL, + SHA of Lisa's key. Not OAuth based but could use OAuth tokens. Based on WaterKen. Waterken server guarantees no failures, everything is processed exactly once.

Things on the desktop environment can be arranged in 2-dimensions; not hierarchical. Claim that humans have evolved to handle 2D nav well, but not hierarchical. Interface is a proof-of-concept (good interaction design, not UI).

FIDO Alliance – Fast Identity On-line

Wednesday 2A

Convener:

Notes-taker(s): Brendon J Wilson

Why is authentication important?

Authentication is the ignition key to the cloud, applications. And like an ignition key, it needs to become a more seamless experience; currently a serious point of friction in everything you do online.

Key problem is that world is incredibly heterogeneous (devices, platforms, operating system), and while certain systems have scaled (data, storage, compute power), authentication hasn't kept pace.

JanRain study "47% of people would rather clean a toilet than pick another password"

Ponemon study of data breaches re-examined the root cause of breaches, and it turns out that authentication failure was one of the major sources of data breaches.

Ecosystems are inhibited from growth - without a simple, consistent authentication protocol, many of these new waves of applications won't be able to reach their ultimate success

Tower of Babel: Problem is not that there aren't ways to perform strong authentication, the problem is that all the solutions are disparate. If you're a relying party, you currently have to maintain multiple pieces of authentication infrastructure, wiring to applications.

Authentication metods aren't static in time - new methods coming around all the time, such as ARM/ TrustZone, Intel IPT, Secure Element - again, reinforces the core problem for relying parties, namely the need to support multiple authentication mechanisms, with redundant infrastructure, redundant integrations into applications

Full Ponemon study of user's desired authentication mechanisms available on noknok.com

Authentication is only one part of the overall solution, part of a large identity stack: rIsk-based authentication stack, user provisioning, lifecycle management.

There's a balance as well between explicit authentication / implicit authentication

Motivations for deploying strong authentication

Regulatory requirements that demand the RP use a certain form of strong authentication

Managing business or reputation risk

Delivering ease of use for the experience to the end user

Note that authentication is a risk problem – don't always need to use the strongest risk

Whatever you deploy, you need to deploy authentication that is risk-appropriate, and business appropriate

What is FIDO?

A standard to provide unified plumbing for strong authentication

Network diagram of the typical FIDO solution - see the posted slides

Protocol has three key pieces

Discovery: Figure out what capabilities are available on the user's device, and what capabilities for strong authentication are acceptable to the relying party

Provisioning: Local enrollment process that performs a setup of a public/private key protected by the authenticator (for example a fingerprint sensor); keys could be protected in hardware or software.

Authentication: Triggering authentication by providing a challenge, user authenticates locally to the device, unlocks the private key stored by the authentication device, signs the challenge

Allows the relying party to determine which authentication method is appropriate for their requirements, as well as switch up between them as the user triggers functionality. Even "weaker" authentication methods are useful, as the RP can use to feed their risk engine, characterize the risk associated with use of a particular authenticator

Answers to common questions:

How does this fit with the other components in the identity stack? Solely focused on authentication, complements other identity technologies such as SSO stacks (OAuth, OpenID, SAML)

How do I (the relying party) know that's really an XYZ class of device and not a software emulator? Uses a device attestation mechanism, ultimately can root this trust in hardware

How will this get adoption, enable solution to the true user problem? FIDO Alliance's work is not only focused on the technology, but also on bringing together the ecosystem of elements (hardware, software, browser, operating system) to enable a true solution – still early days.

What makes the FIDO Alliance different from other two-factor authentication approaches? Where are the boundaries of this protocol that will allow different authentication tokens, infrastructure, software vendors to interoperate and build different components of the solution. Boundaries are the protocol specification (to be published for public review later this year), the interfaces to the authenticators. Some elements of establishing trust will be managed by FIDO Alliance; whether it continues to be the anchor forevermore is an open question.

What is the ideal end state if FIDO is successful? Devices, software solutions that at FIDO-compliant - you use the device you have already to authenticate using its native capabilities to authenticate. Goal is unified plumbing for a variety of authentication methods, providing insulation for an RP as old authentication methods fall out of favor and new methods are invented.

Not all devices will necessarily support all potential modalities of authentication - doesn't make sense in the context of different devices

Who else has to come to the table to make this work? Browser, operating system vendors, relying parties are the people to bring together. FIDO Alliance doing the yeoman's work to bring together those players, get initial pilots with large RPs to build the momentum.

Where does this overlap with the efforts of federation protocols? Very complementary - essentially the first mile authentication is FIDO, second mile is federation via other protocols (OpenID, SAML, etc.)

What are you going to do about attestation infrastructure? FIDO Alliance is the organization will bootstrap the mechanism for verifying the genuine nature of the authenticator

Why a new organization?

The focus is on bootstrapping a complete ecosystem - it's not just about a protocol - much broader scope than most traditional standards bodies

As the protocols mature, there is a commitment to handing the protocols off to the IETF/W3C or similar organization - it's baked into the membership agreement

Why does it cost to see spec? Won't cost to see implementation draft spec, we're not there yet. Initial membership fees focused on bootstrapping the organization and ecosystem.

See fidoalliance.org for more details

Faith, Religion and Cultural Context

Wednesday 2C

Convener: Judith Fleenor

Notes-taker(s): Vince Conroy

Premise (Judith):

Our religious context factors into how we design and architect identity systems -- hierarchical vs. flat vs. circular?

1) If and how should religious factors affect how we architect and design identity systems

2) How does your view of good and evil affect how you trust others

Do religious beliefs/cultures factor in, or "is the world just like this"?

Comment:

Ponemon Institute (http://www.ponemon.org/) study: cultural beliefs about privacy across about a dozen nations/cultures

example: in the US we don't trust the govt, while in Europe they do

some cultures will give up private information very easily, others will not

Many questions were presented with lots of lively discussion

How does faith and culture affect how we trust people?

What architecture/system map to the various religious contexts?

For example, the following premise was presented:

Abrahamic religions (Christianity, Judaism, Islam) tend to be more hierarchical systems and structures

While "new thinking" and other religious systems (e.g. Hinduism) tend to more "circular" or social

How does one's view of an afterlife affect trust and willingness to share data? Does "identity" persist beyond one's natural life :-).

Example of a role-based system developed by an attendee:

used a "bottom-up" approach to user assignment in a role-based systems

experimental system

used the XDI stack and SAML for authentication

Delegated authority vs. Socially validated identity?

Other Questions raised:

What is the difference between monotheistic vs polytheistic based cultures, and much does it matter?

e.g. in Germany is there a national ID but not in the US

Is Identity the center of the world? No, its important but all there is

Should we be taking a philosophical or pragmatic approach to this based on what people do vs. what they "believe"?

The concept of good and bad -- these are defined differently in different cultures. Should be we using other terms?

Example: Steve Jobs - no on/off switch on Apple products is reflective of his religious beliefs

Some cultures might be more interested in or resistant to personal clouds.

new book from Google's Eric Schmidt - ?

Bottom line:

How can reflecting on these issues help us design better identity systems?

DNS vs XDI
Who is better at solving which problems?
What are the pros and cons i1n which situations?

Wednesday 2B and 5C

Convener: Esther Makaay

Notes-taker(s): Esther Makaay

Aspects for comparison:

Discovery of attributes associated to names (+requirements)

Registration (+characteristics)

Trust of authenticity of discovered data (technical)

Dependencies (decentralisation)

Use/functionality: finding "what"/"where"

(Suitability) (not in this phase)

Start of comparison based on explaining XDI by Drummond:

XDI	DNS
Graph model (tree with references)	Tree model (no references)
Protocol (under development, OASIS) Objects=graphs, sentences/ontology Transactions: modifications (add, get, mod, del)	Protocol (RFC 1035) Objects=RRs (separate protocols and RFCs) Query/response protocol (modifications of RRs out of band)
Typed name structure (persistency)	Typeless name structure

But how do these names co-exist?

My subdomain: esther.makaay.nl

My iname/cloudname: =esthermakaay

Or should we fathom something like xdi:esther.makaay.nl -> RR …

[and then time ran out]

Session continued 3:30 PM

Let's do a short paper on this topic, in two parts:

1) core capabilities / characteristics (Including objects exchange mechanisms)

2) scenarios / use cases ("How would you do...in...")

Examples and aspects mentioned to go into this:

Data portability, Portable permissions / authorisation for a part of the graph, Performance, Revocation, Permutable data structure, RDF graphs vs RRs, XDI variables vs NAPTR wildcard resolving, Different 'types' of RRs: visible (usage/referencing) & administrative, Graph signing (and XML variants to do so) vs DNSSEC

Working lunch & post-closing time on Thursday will be used to flesh out this paper.

Patent Trolls Gonna Kill VRM?

Wednesday 2E

Convener: Clive Boulton

Notes-taker(s): Clive Boulton

Tags for the session - technology discussed/ideas considered:

ppt: http://www.slideshare.net/clibou/patent-trollls-gonna-kill-vrm

note taker(s) clive boulton

No one at all attended this session. I think this means too early to be of interest.

Customer Commons OMIE

Wednesday 2F

Convener: Doc Searls

Notes-taker(s): Lionel

Doc Searls presented the OMIE, a project of Customer Commons, a non profit organization committed to empowering the individual consumer in the marketplace. OMIE is a device--an Android-powered mini-tablet with touch screen--that allows a consumer to engage with apps at the beginning of the demand chain vs. end at the supply chain.

The purpose of the session was to engage participants around apps that we collectively would like to design/see on the OMIE product within this context.

The “r-button” expresses the relationships.

This is the loop:
Demand Chain >
Better Sign-in >
Better Management
Big Individuals .....
<--- Payments

As background, Doc shared the original array of apps that Ian Hamilton suggested when he originally conceived of the OMIE product.

Suggested apps included:
- My wallet- amazon has an AB
- My credit card bill- Mint gets credit card info. Best Buy wish list.
- My guardian
- My fitness (Qs/fitness/health: de-siloed data/athletic/elderly/caregivers)
- My month (timeline)
- My shopping list (comparison engine)
- My loyalty card
- Photo verification- scanability

Ideas also referenced from Australia: my pocketbook

Doc captured jobs for Customer Commons:
- feedback to API developers
- when is it to the customers’ advantage?
- pooling the developer forum
- provide help with selling this
- payments- getting the money- $ has to come from the device owner/cloud owner; need capacity.
- Kickstarter around My Wallet app. Show benefit to retailer. Customers pay money-- its a measurable benefit.

Discussion:
==========
Data more reliable from scraping than from APIs- thanks Kevin Coxe who offered case study from edentity involving government and data scraping.
Business of access, low-risk approach to businesses could work
Paying for data is ok

Clive Boulton: highly recommended API lecture, search AL3X:
https://www.youtube.com/watch?feature=player_embedded&v=VVovVjT_H8A#!
The Interaction Design of APIs: (April 17, 2009) Alex Payne explores the interaction design of APIs, particularly through the lens of the speaker’s experience evolving the popular Twitter API. The speaker argues for the notion of a “humane” API”, one derived from simplicity, “explorability” and consistency.

We must humanize our conversation in this space.
- Not CPU, Memory, Network
- Yes: CPU = Heart; Memory = diary; Network = ??

Calendar would be a great application.

Reverse loyalty card: An intention card. Scenario: you are at a retailer, and you need "petite" clothing. They do not have any. You announce your intention, that you wish to be notified. The implementation was discussed: the customer can show the OMIE to the retailer and the retailer scans it. Objection--retailer computer systems and integrations are too expensive. It can work the other way: OMIE can scan something at the retailer, then we can implement it in the OMIE backend.

Quotable quote:
Most APIs are not made for humans like most reservoirs not made for humans, but faucets are. - Doc Searls

Customer Commons OMIE

Wednesday 2F

Convener: Doc Searls

Notes-taker(s): Marion, Lionel

Doc Searls presented the OMIE, a project of Customer Commons, a non profit organization committed to empowering the individual consumer in the marketplace. OMIE is a device--an Android-powered mini-tablet with touch screen--that allows a consumer to engage with apps at the beginning of the demand chain vs. end at the supply chain.

The purpose of the session was to engage participants around apps that we collectively would like to design/see on the OMIE product within this context.

The "r-button" expresses the relationships.

This is the loop:
Demand Chain >
Better Sign-in >
Better Management
Big Individuals .....
<--- Payments

As background, Doc shared the original array of apps that Ian Hamilton suggested when he originally conceived of the OMIE product.

Suggested apps included:
- My wallet- amazon has an AB
- My credit card bill- Mint gets credit card info. Best Buy wish list.
- My guardian
- My fitness (Qs/fitness/health: de-siloed data/athletic/elderly/caregivers)
- My month (timeline)
- My shopping list (comparison engine)
- My loyalty card

- Photo verification- scanability

Ideas also referenced from Australia: my pocketbook

Doc captured jobs for Customer Commons:
- feedback to API developers
- when is it to the customers' advantage?
- pooling the developer forum
- provide help with selling this
- payments- getting the money- $ has to come from the device owner/cloud owner; need capacity.
- Kickstarter around My Wallet app. Show benefit to retailer. Customers pay money-- its a measurable benefit.

Discussion:
==========
Data more reliable from scraping than from APIs- thanks Kevin Coxe who offered case study from edentity involving government and data scraping.
Business of access, low-risk approach to businesses could work
Paying for data is ok

Clive Boulton: highly recommended API lecture, search AL3X:
https://www.youtube.com/watch?feature=player_embedded&v=VVovVjT_H8A#!
The Interaction Design of APIs: (April 17, 2009) Alex Payne explores the interaction design of APIs, particularly through the lens of the speaker's experience evolving the popular Twitter API. The speaker argues for the notion of a "humane" API", one derived from simplicity, "explorability" and consistency.

We must humanize our conversation in this space.
- Not CPU, Memory, Network
- Yes: CPU = Heart; Memory = diary; Network = ??

Calendar would be a great application.

Reverse loyalty card: An intention card. Scenario: you are at a retailer, and you need "petite" clothing. They do not have any. You announce your intention, that you wish to be notified. The implementation was discussed: the customer can show the OMIE to the retailer and the retailer scans it. Objection-- retailer computer systems and integrations are too expensive. It can work the other way: OMIE can scan something at the retailer, then we can implement it in the OMIE backend.

Quotable quote:
Most APIs are not made for humans like most reservoirs not made for humans, but faucets are. - Doc Searls

Whiteboards Are People Too

Wednesday 2G

Convener: Sam Curren

Notes-taker(s): Sam Curren, Alan Karp

Notes from Sam:

Whiteboards are People too.

Personal Clouds are for more then just people. Physical things and even non-physical organizations or social constructs can use them too.
Web 2.0 apps are built as central systems to track things.
Using Persistent Compute Objects (PiCOs) allows a programming model that focuses app development on the individual thing, and not a system to track classes of things.
Channels between PiCOs and other Personal Clouds allow for communication. Multiple apps can cooperate to create the desired behavior.
Event naming will be a problem as this gets popular, and that's a problem we would love to have.
Defining the outer interface of PiCOs will allow them to connect and communicate with other Personal Clouds of different types.
This programming model can scale to trillions of things, and also to the thousands of _my_ things.

(Whiteboard also submitted)

Notes from Alan:

Whiteboards can have personal clouds internet of things use PICO for each.

PICO – persistent compute objects

PICO for IIW has channel to each room's whiteboard PICO

Whiteboard has on electronics, its PICO runs elsewhere

PICO is execution context with Apps

Lots of discussion

- scalable management
- setting policy
- initiate connectivity
- session square tag vs. room square tag
- access control – channel vs. pub/sub

Private Data Stores

Wednesday 2H

Convener: Joe Andrieu

Notes-taker(s): Stuart Maxwell

Instead of sharing information with service providers, why not run their code in our private context?

Does this sound hard? It's what we're doing all the time when we browse the web by using javascript.

Problems:

Data leakage

Code corruption?

Permissioned data layer

Must get data into data store

Collaborative filtering ID(3) - hard to do if we don't share data back out

What are/would be the killer apps?

- Anti-virus?
- birthday alarm service
- medical recommendation app
- insurance recommendation app that looks at your information and recommends better rates or things you can do to get better rates

Could this be run on a 3rd-party host instead of on my device

What sorts of data would we put in a private data store?

- health data
- location history (space/time data)

JANA - Nathan Eagle - analyzes space/time data

Book mentioned: The Daily You, by Joe Turow

Ushahidi http://www.ushahidi.com

Main reasons to do Private Data Stores

- 4th Amendment Privacy concerns in the US (protections against unreasonable search & seizure)
- Companies shouldn't hold data any longer than they need to

Privacy-Preserving Accessibility Support with GPII and UMA

Wednesday 2I

Convener: Keith Hazelton

Notes-taker(s): Keith Hazelton

The Global Public Inclusive Infrastructure (GPII.net) is a well-funded and internationally-scoped initiative "to ensure that everyone who faces accessibility barriers due to disability, literacy, digital literacy, or aging, regardless of economic resources, can access and use the Internet and all its information, communities, and services for education, employment, daily living, civic participation, health, and safety."

GPII has adopted a solution to one of the key challenges: Coming up with an range of issues mentioned in their vision statement. ISO/IEC 24751 parts 1-3, "Individualized adaptability and accessibility in e-learning, education and training". Also known as "Access4All". There is also a defined set of accessibility metadata that is able to express a RESOURCE'S ability to match the needs and preferences of a user. For more, see http://tinyurl.com/uma4gpii

One of the challenges to this vision is that by its very nature, the user has quite high stakes in properly controlling the release of accessibility needs and preferences information. This is a classic case where unlinkability is a requirement. I don't necessarily want health insurance companies or prospective employers to have a complete dossier on my accessibility issues.

Here's where User-Managed Access (UMA) comes in. UMA is a profile of OAuth 2.0 that allows a user to specify conditions under which their resources (in this case, their needs and preference information set) are released to relying parties.

Discussion:

A pilot is under development under the auspices of the Scalable Privacy project (one of the first round NSTIC awards) using the GLUU UMA stack. Bjorn Annestad of UnboundID spoke of the OAuth 2.0 support in their products. They treat consent as a prime condition of access by an OAuth 2.0 requesting party/client.

Debbie Bucci of the HHS ONC explored the parallels between the notion of segmentation of electronic health records under active discussion in her world and the notion of context-relevant subsets of one's accessibility needs and preferences. The solutions being explored in the scalable privacy pilot of UMA for GPII are relevant models. Collaboration should ensue.

Diagrams and other materials relevant to the topics of this session are available at http://tinyurl/uma4all

BlueButtons+ and OAuth2

Wednesday 2J

Convener: Justin Richer, J. Mandel A. Gropper

Notes-taker(s): Karen O'Donoghue

BlueButton+, OAuth2, RESTful, JOSE

Justin provided an overview of the current state of the BlueButton+ effort using OAuth2.

The current documentation is available on github at:

blue-button.github.io/blue-button-plus-pull

Josh Mandel, a regular participant in the work, talked about some of the motivation and the problems being addressed. There is a desire to bootstrap an ecosystem where patients can share specific health information with selected providers in a privacy protecting manner. Blue Button was envisioned to “create portable medical histories that facilitate dialog among health care providers, caregivers, and others” (from Wikipedia). The BlueButton+ effort is looking at the addition of capabilities allowing the user to allow medical providers (and others) with access to various sets of information. This needs to work in a fairly dynamic world.

Justin stepped through the various sections of the online document. There were several questions for clarification. Justin provided a diagram of the basic exchanges on the white board (see attached picture). In one case, he was interested in a better term for class of clients. There is confusion surrounding the terms class and instance.

Justin asked for anyone willing to read through the documentation to send in questions or comments. In particular, he is especially interested in those with related use cases.

For more information, please see the link or the associated whiteboard picture.

Data Durability: Security Over Time

Wednesday 2K

Convener: T. Rob

Notes-taker(s): T. Rob

Tags for the session - technology discussed/ideas considered:

security, data, pclouds, vrm, identity, encryption, key management, iot

There are two use cases which appear to be common for Personal Cloud and VRM and which both require a data centered approach rather than the ubiquitous connection-oriented approach:

A need to prove data integrity and authenticity over time. If the personal cloud collects transactional and experiential data over time, then for that data to be useful for more than trivial requirements there must be a way to prove it is authentic and intact when it is used at a later date.

A need of 2nd and 3rd party recipients to trust data for non-trivial uses. The example given is of a power utility receiving load abatement data concerning LED bulbs. The utility does not receive the data directly from the bulbs but rather the bulbs report to the homeowner who republishes the data to the utility.

Many existing architectures rely on a secure connection to a trusted party. Data received over that secure connection is assumed to be authentic and intact due to the context of the connection. The authoritative source (usually a vendor or merchant) is assumed to have sufficient physical and procedural controls to prevent changes to the underlying data.

The base assumptions change for personal clouds. These may be self-hosted in which case there is no longer an assumption regarding physical security of the data. Regardless of who hosts them, one premise of personal clouds is that you own your own data and so there is no longer an assumption of procedural controls to assure integrity of stored data. On what basis can someone connecting to a personal cloud then trust the data received, other than that to which it is not a 1st party participant?

The answer proposed is that the parties involved counter-sign the transactional data, or that devices

sign the data that they emit. At daily intervals the transactional and event data are signed as a batch. Then at weekly and perhaps monthly intervals hashes of the smaller batched are aggregated and signed. In this way, large databases can be verified after migration or against a redundant copy and any discrepancies can be identified at the data element level by drilling down through the hierarchical hash tree.

The similarity to BitCoin and Ripple history auditing was discussed and the idea of an implementation based on Ripple was tossed around.

We also discussed implications on key management. Currently either a key is valid or it isn't. In Enterprise archival storage key usage is time-bound by category such that, for example, a given key can be invalid for encryption after a given date but valid for authentication and decryption for a much longer period.

Data sharing over time was also of interest to the group. Access to the personal cloud is perhaps not granular enough when the cloud represents shared history. When you get married, both parties legitimately have access to their shared history but not necessarily to prior history. In the event of divorce, there needs to be a way to either duplicate the shared portion or else maintain access to *just* that portion by both parties while subsequent history is private.

Similar requirements apply to organizations that outlive membership of any one individual such as Scout troops. Here there is tremendous benefit in maintaining the history and traditions of the troop despite the participation of any one leader or member lasting on average just a few years. Although much of the data would be public, access to current and past membership details would need to be limited and audited.

Although there were no next steps from the meeting, the consensus of the group was that the session's premises were valid and that connection-oriented security alone is not sufficient to address the unique security needs of Personal Clouds or VRM as currently understood.

OAuth 2 Bootstrapping from device to browser (technical)

Wednesday 3B

Convener: George Fletcher

Notes-taker(s): George Fletcher

Tags for the session - technology discussed/ideas considered:

Abstract

This document describes a process that allows a client to seamlessly transition the user from an authenticated state in a native application, to an authenticated state in a web browser.

Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 *[RFC2119]*.

Table of Contents

1. Introduction

In order to provide a good user experience it is necessary at times to "share" an authentication state across disparate environments. For example, a desktop utility that shows the user a list of their last N mail messages, and when the user selects one of the mail messages, opens a browser logging the user into their mail account on the web.

This document defines a process based on OAuth2 *[RFC6749]* to enable this functionality.

1.1. Roles

This specification uses the 'client' and 'authorization server' roles from the OAuth2 *[RFC6749]* specifcation. In addition to these two roles, this specification also identifies the role of the

web application

The destination web application where the user will be seamlessly logged in.

1.2. Scopes

This specification defines an additional scope that MUST be authorized to the client in order to obtain the bootstrap-token.

web_session

A scope that provides the client the authorization to obtain a bootstrap-token

1.3. Protocol Flow

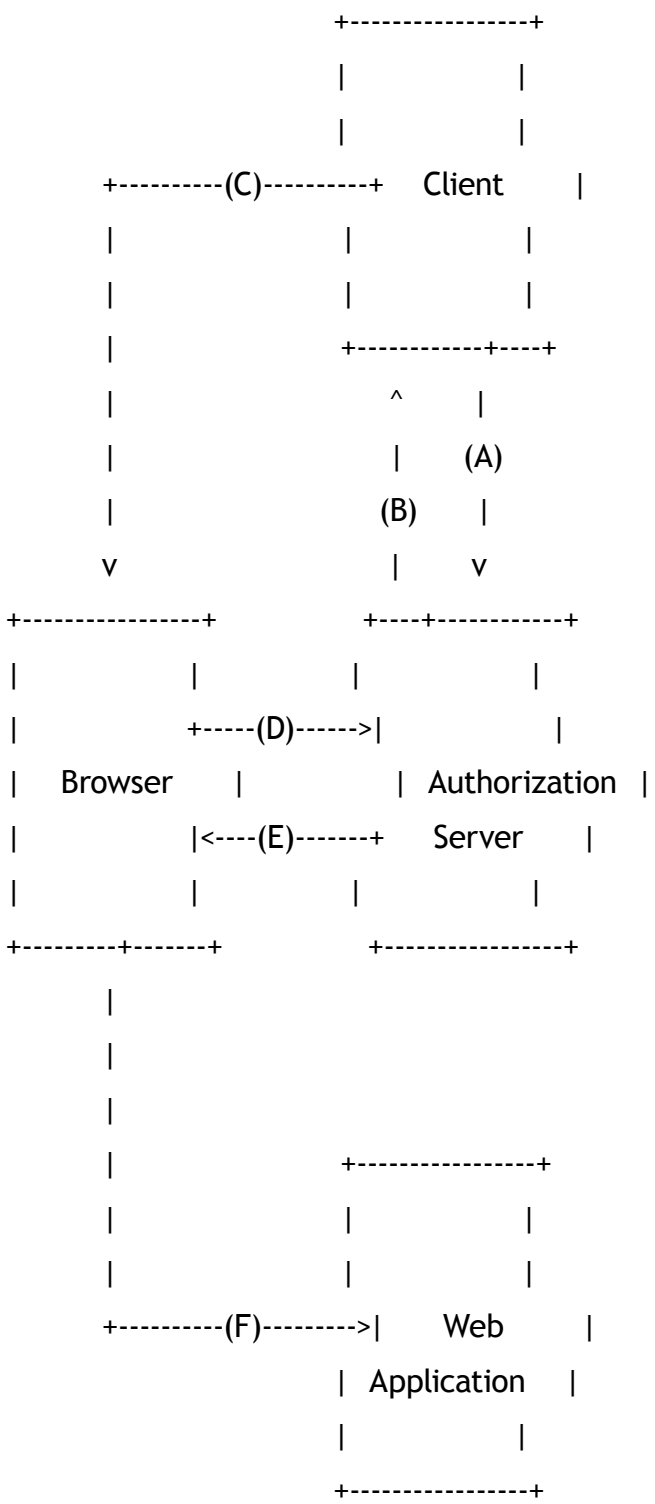


Figure 1: Abstract Protocol Flow

The abstract Web Session Bootstrap flow illustrated in Figure 1 describes the interaction between the three roles and includes the following steps:

(A)

The client requests a bootstrap-token using the OAuth2 token endpoing (e.g. grant_type=refresh_token)

(B)

The authorization server returns bootstrap-token

(C)

The client constructs a URL to the AS (/web-session?access_token=<bootstrap-token>) and loads it into the browser

(D)

The browser invokes the AS /web-session endpoint.

(E)

The AS validates the bootstrap-token and establishes a web session for the user identified by the token. The AS redirects the browser to the destination web application (potentially setting cookies)

(F)

The browser follows the HTTP redirect and loads the destination web application

1.4. Terminology

See OAuth2 *[RFC6749]* for terminology used in this specification. In addition to the terms defined in the OAuth2 specification, the following terms are defined:

bootstrap-token

An OAuth2 *[RFC6749]* access_token that is used to bootstrap the authentication context from the client to the web application.

2. Bootstrap Token

In order for the client to obtain a bootstrap-token, the client MUST have an authorization grant that is authorized with the 'web_session' scope. The process of obtaining an authorization grant authorized with the 'web_session' scope is outside the scope of this document. This specification specifically profiles the refresh_token and Assertion Framework for OAuth 2.0 Client Authentication and Authorization Grants. The required scope for this process is

web_session

This scope provides the authorized party the ability to bridge the user's identity from the receiving client application to a browser based session.

2.1. Refresh Token Authorization Grant

The request to obtain the bootstrap-token uses the token endpoint described in section 6 of OAuth2*[RFC6749]*. This use of the /token endpoint is profiled for grant_type=refresh_token as follows.

grant_type

The value MUST be 'refresh_token'

refresh_token

The refresh_token obtained by the client.

scope

The value MUST only contain ‘web_session’. This is effectively a “downscoped” token and MUST only be used for this flow.

dest_url

An additional parameter used by this profile; The URL to which the browser should be redirected if the seamless bootstrapping of the authentication is successful.

2.2. Assertion Framework Authorization Grants

The request to obtain the bootstrap-token uses the token endpoint described in section 6 of OAuth2*[RFC6749]*. This use of the /token endpoint is profiled for grant types of the Assertion Framework as follows.

grant_type

The value MUST be a valid assertion framework grant type

assertion

The assertion previous issued in an authorization grant.

scope

The value MUST only contain ‘web_session’. This is effectively a “downscoped” token and MUST only be used for this flow.

dest_url

An additional parameter used by this profile; The URL to which the browser should be redirected if the seamless bootstrapping of the authentication is successful.

2.3. Bootstrap Token Request Processing Rules

The authorization server MUST validate the request as follows

Verify the client credentials. The request MUST fail if the client credentials are not valid. The AS may whitelist clients such that only certain clients can perform this function.

Verify the authorization grant. The authoriztaion grant MUST be valid and MUST be granted the ‘web_session’ scope.

Generate a new bootstrap-token with a short expiry time. Note that these tokens SHOULD be treated as one-time-use tokens. The bootstrap-token MUST be associated with the specified dest_url. If no dest_url is specified, the request SHOULD fail.

Return bootstrap-token as the access_token in the response per OAuth2 *[RFC6749]*Section 6

For Example: (line breaks added for readability)

```
POST /token HTTP/1.1
Host: server.example.com
Authorization: Basic czZCaGRSa3F0MzpnWDFmQmF0M2JW
Content-Type: application/x-www-form-urlencoded

grant_type=refresh_token&refresh_token=tGzv3JOkF0XG5Qx2TlKWIA&
```

scope=web_session&dest_url=https%3A%2F%2Fweb-app.example.com

In the case that there are processing rule errors or other failure conditions the /token endpoint response MUST conform to OAuth2 *[RFC6749]* Section 5.2

3. Web Session endpoint

The web session endpoint allows the holder of a bootstrap-token to establish an authenticated web session for the user identified by the bootstrap-token. This endpoint is a protected resource as defined by Bearer Token Usage *[RFC6750]*.

This endpoint defines no additional parameters other than the OAuth2 access token. The client invokes this API by specifying the bootstrap-token as the API's access_token.

The web session endpoint MUST support both the GET and POST methods of the Bearer Token Usage*[RFC6750]* specification. Support for the Authorization header is not required as most browsers do not allow for setting of arbitrary HTTP headers.

The web session endpoint SHOULD identify requests not coming from a browser and return an error of 'invalid_request'

On receipt of a web-session request, the Authorization Server MUST validate the bootstrap-token to ensure that it has not expired and SHOULD verify the token is not being replayed.

The AS then determines the user and destination URL from the bootstrap-token and establishes a web session for this user. NOTE: the web session context MUST identify that this web session was establish with a means other than user credentials.

The web-session endpoint responds successfully by returning a HTTP 302 redirect instructing the browser to load the destination URL and setting whatever cookies necessary to establish the web authentication session.

For Example: (line breaks added for readability)

HTTP/1.1 302 Found

Host: server.example.com

Location: http://web-app.example.com

Set-Cookie: AuthSession=asdfasdfasd; Domain=.example.com; Path=/; Secure; HttpOnly

The mechanism by which web application determines the identity of the web authentication session is out of scope of this document.

Error responses for this endpoint follow the Bearer Token Usage *[RFC6750]* specification.

4. Security Considerations

In some ways this exposes an escalation of privileges because a "restricted" (by scope[s]) refresh_ token is used to generate a full web session. It is imperative that the session semantics generated by the Web-Session endpoint ensure that downstream web-applications understand that the user has not "recently" authenticated and instead this session is generated from an existing token. In many respects, this web-session is equivalent to that generated from a "remember me" or "keep me signed in" cookie as supported on many sites. Access to special privileges for this user SHOULD be restricted and require additional authentication checks. Possible mitiations include...

One way to manage the authentication session is to track the time at which the user last presented authentication credentials (e.g. password). By tracking this within the session context any web-application can protect certain privileges by requiring the user to have presented their credentials within the last n seconds/minutes. For a web session created via this flow, the authentication credentials presentation time is the time at which the user authenticated to create the refresh_ token.

The Authorization Server SHOULD revoke any existing web session if the refresh_token used to create the web session is revoked.

Any additional tokens issued from the web session MUST be linked to the refresh_token that created the web session such that if the refresh_token is revoked or expired, the generated access tokens are revoked/expired accordingly.

The Authorization Server SHOULD provide an interface for the user that shows the active web sessions issued from refresh tokens and allow the user to expire the web session.

5. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC6749] Hardt, D., "The OAuth 2.0 Authorization Framework", RFC 6749, October 2012.

[RFC6750] Jones, M. and D. Hardt, "The OAuth 2.0 Authorization Framework: Bearer Token Usage", RFC 6750, October 2012.

Author's Address

George Fletcher (editor)AOL Inc.EMail: gffletch@aol.com

VRM for SMEs

Wednesday 3C

Convener: Clive Boulton

Notes-taker(s): Clive Boulton

Our session shared a belief that personal clouds will be adopted by small business at scale for VRM and pay for a service (vs. consumers who won't pay today). VRM will be used for exchanging intention data with there currently un-network connected ecosystem. This took us into the schematic for personal cloud to address VRM in the SME / SMB space. We explored Ward Cunningham's Smallest Federated Wiki. http://wardcunningham.github.io/

Well noted at IIW Personal Cloud has many protocols and approaches to deal with identity and data ownership. In a business context, what if we think of identity as a shared relationship between entities, and give people and business dignity and control over data. Then out of this comes a pattern for sharing information at a paragraph level.

In the following demo, create a new wiki page, copy or edit some data, then fork the page and pass it to an new owner. Who gets there own copy in Drop Box or wherever they decide feels like the right place to save their data.

http://oscon.fed.wiki.org/view/welcome-visitors/view/welcome-visitors_rev14

NSTIC HER & Patient ID

Wednesday 3D

Convener: Justin Richer

Notes-taker(s): Nicholas Crown

Tags for the session - technology discussed/ideas considered:
NSTIC, IDESG, OAuth, Trust, Privacy, EHR

EHR & NSTIC

Convener: Jim Sheire

ONC - Office of the National Coordinator for HC technology

-Responsible for the standards, technology, framework for digitizing HC stuff

-Push is for 2016 push

-Working to understand the privacy requirements/standards necessary to participate in exchanges, etc.

-Advisory committees are working to understand these requirements

-If you are patient, how do you interact with your EHR/Data Holder to view records, etc.

-Letter is available online with the recommendations for the what the credentials should look like to comply with meaningful use

-Issue is that the data holder will always look for any possible loophole to avoid sharing your data

-Working to eliminate the loopholes to avoid no action

-What about delegation when the patient is unable to access on their own?

-Justin Richer:

--Blue Button + initiative

---Developing a RESTful API for moving HC records between parties

---Using OAuth for protecting the API

---Interesting work around dynamic registration amongst parties

---Moving away from traditional pre-configured trust-based systems and using OAuth to make this more dynamic

---This allows them to build systems that use patient consent and support interop at the authZ level

---The NSTIC recommendations need to be applied to Blue Button

---NSTIC can then use policy to ensure that the right things are happening at the technology level

-Trying to workout a framework for what FIPPs would look like when applied to patient ID

--From the patient ID perspective, FIPPs would like:

--Don’t ask for more than you need (Data Limitation/Purpose Limitation, etc.)

--Recommending three levels:

--- 1. Consultation (patient can be anonymous at this point)

--- 2. Bilateral payment confirmation (primarily between the HC provider and insurer)

--- 3. Aggregation (non-coercively in a voluntary way)

---- B. Need strong ID and aggregation to avoid prescription fraud (getting narcotics at multiple providers for recreation use)

From the letter under the FICA Community via a hearing focused acquiring advice from the patient/provider communities to understand how to alleviate "identity" issues:

-"NSTIC... Should provide a more scalable solution for patient authentication in the future"

-Could see this a recommendation for using the NSTIC Identity Ecosystem as an identity layer to solve the challenges

-Presents a nice alignment between the problems in HC and the solutions being worked in NSTIC

-ONC is telegraphing what they want to see happen prior to regulating to force the work to occur

-The tiger team that "testified" before the hearing made the following recommendations:

--Identity Proofing

--Authentication

--Best Practices:

---Usable

---Voluntary/Flexible

---Scalable/NSTIC

---Federation/Re-use

---KBA

---Out-of-band AuthN

---Go Beyond Passwords

---M2M

---...

Securing the Personal Cloud

Wednesday 3I

Convener: Peter Davis, Dan Blum

Notes-taker(s): Dan Blum

Tackling this discussion with the definition of the interfaces from figure 1

assumption: architectural relationship between Fred's personal cloud with his services and Lisa and her services

personal data repository is an example of one of these services

the interfaces

table the issues of multiple personas and devices

the security objectives - confidentiality, integrity, availability, privacy - trust boundaries

1 - client application and devices

2 - channel between app and cloud service

3 - service

4 - service to service

5 - service to lisa's service

6 - service to third party

objectives

confidentiality

integrity

privacy

availability

aspects of security

user identity

source (invocation) identity

target identity

target user

access control / policy - need defaults

miscellaneous

need to describe service robustness (catch all for non-identity and other protocol-related requirements)

threat modelling needed

personal trust framework will state these requirements for these interfaces and there will some requirement for attestation (self-assertion and audit)

johannes - what are the implications of mobility

example to check out - liberty audit framework

internet of things - today these things communicate with manufacturer (3rd party)

portability - interesting issues like apps expressing their portability needs as metadata to iaas

what about family "federations" (household versus individual personal cloud)

Respect Network Credits

Wednesday 4A

Convener: Kevin Cox, Drummond Reed

Notes-taker(s): Kevin Cox, Drummond Reed

Kevin Cox Notes:
Respect Network Members enable individuals to interact with businesses, government and other members. The Network Members each have overlapping sets of interactions but many interactions - particularly with businesses and governments - will initially be with one Respect Member. Where ever appropriate Respect Network Members can reduce the burden on end users by using the existing relationship with a member to communicate with them rather than creating a new link. This is particularly important when funds are involved because the transfer of funds can lead to unnecessary costs if the funds are transferred for each transaction. Respect Network members can transfer funds to and from each other using Respect Network Credits.

This not only reduces costs but it increases the potential market for each of the Respect Network Members and for each individual attached to the Network. The attached diagram shows the overall structure of the Credit system.

Some members of the RespectNetwork Credit system might allow the individuals whose data is shared to keep some of the Credits for their own use. Some paying organizations might even insist on it as it could be used as a promotional tool. This is very important for those RespectNetwork Credit members who sell directly to individuals as it creates a special rewards currency that has multiple uses and hence is more attractive to consumers than typical rewards currencies while at the same time increasing the network effect for the Respect Network.

Specifying and implementing the details of how this will be done will be the work of this group. One suggestion is that funds in payment between parties in the Network be transferred via Zero Interest RespectNetwork Credits. There will be a transaction charge on the gross transfer of funds to cover the cost of construction and to help build other infrastructure of benefit to all RespectNetwork members but there be no interest on credits accumulated in the system. Instead of paying banks a commission on the transfer of funds a reduced amount could be given to the network and returned to benefit the members and unnecessary offsetting transfers of money between members could be eliminated.

Drummond Reed Notes:

Kevin drew a diagram that explain the ecosystem of personal cloud service providers (CSPs) who would be in the business of helping individuals to exchange personal identity and attribute exchange credentials.

The overall goal is to create a federated system of exchanging digital credits between CSPs which can work across national or industry boundaries and help achieve the network effect for credential exchange. Each CSP can deal with the business customers in its own jurisdiction/country/market and yet still service relationships that need to cross jurisdictions/countries/markets.

One attendee asked about taxes and how these exchanges would be treated by governmental authorities. Kevin explained that the credits should not be taxed because no money is changing hands across jurisdictions, only within a jurisdiction.

As a Respect Network member, Kevin proposed that Respect Network create this system of

credits. Drummond agreed that this was precisely one of the goals for which Respect Network was created, and that he was eager to see how this work could be driven forward by the Respect Network members who want to make it happen.

At least one attendee, Ross Hughson from MyInfoSafe and Personal Information Management LTD in New Zealand, said they were interested in working on it because they see the benefit of expanding their market.

Google's Auth Goals for the Next 5 Years

Wednesday 4B

Convener: Eric Sachs

Notes-taker(s): Eric Sachs

Full account notes of this meeting on the roadmap for Google Identity is at

http://goo.gl/DFLnS

The Legal Forum

Wednesday 4F

Convener: Dazza Greenwood

Notes-taker(s): Nora Draper

Tags for the session - technology discussed/ideas considered:
Legal Issues, MODIS, Terms of Authorization, User-Centric

[note: session taped – see Doc Searls for the document]

Goal: To reassert the legal portion of the IIW Commons. Re-inaugural wake-up call to see who wants to leave. Also to bring forward from case studies in the user-centric economy using what we know about the B2B end.

Building on a conversation that has happened with Doc Searls over the last few IIWs that looks to invert the Terms of Service that feel that it is something that happens to you with something that appears in your apps that tells you all the various parties that have rights and obligations around you and your data. Killing the ToS and replace with the ToA.

We start with an apps page and add more clauses as we add more parties. To get this, we need Business to Business contracts.

[introduction of participants and participant interests]

[Broad ideas that came out in the introductions: Interest articulated in terms and solutions that can be implemented in the near term. Interest in security and privacy. Lots of representation from Customer Commons. Interest in understanding the Terms of Authorization and how that relates to participant platforms. Interested in what our Freedom of Contracts should be.]

Dazza speaking – unless otherwise noted

This is a dynamic part of the transition to the digital economy where technology, law, economic and relationships are all happening apace. This is a place where innovation happens.

Start with an overview of what's been happening at the media lab and how that could be useful for everyone around the table.

Sandy Pentlen (spelling?) (from Media Lab) is happy to do constructive listening and sharing.

Two things we've done:

First – B2B part: to try and express in a more machine readable format the types of structures that governments and businesses have when they are using individual data (and other information). There is a lot to learn from B2B to understand how things might operate in a user-centric world. Started by taking multilateral agreements for financial clearing houses and identity federations and, through a combination of creating and analyzing, found common elements and looked at how those could be better suited to existing conditions. What we have is a template (go get it, use it, update) from creative commons: business and legal structures for identity commons. A few design patterns culminated with MODIS (MIT Open Data and Implementation Systems) – moving from proof of concepts to an open model. Purposes of this system is a design pattern, for whatever system you have, you can see how a system could align with the specifications that users provide. Right now, to integrate those meaningfully across systems is really difficult because of different standards. You can get more predicable outcomes for user preferences and privacy using this MODIS model.

Second – from the PoV of indivduals. Want to see ourselves as an autonomous human with some freedom. Even before getting to constitutional analysis, using widely configured technologies (like OAuth2), turns out that we have been given a legacy of sufficient pieces that can be architected together to give expression to autonomous people. One is Terms of Authorization: starts with the idea that there is an account dashboard related to a human who "owns" the account.

Doc: Account makes an assumption that there is a second party.

Dazza: Maybe that isn't the right word – account may have baggage with it – but we have an idea that the user can use federated authentication to log into the account.

Mark: Who is the identity provider?

Dazza: Hold that. What a human does when they log into the system, they can log into an admin or root page (or account page), what they see is a dynamic page that is the legal part of their relationships including the party providing this. Terms of authorization written in the first person: "I license you as service provider…" (called iAuth). The terms should be as little as possible (but no less). The Dashboard, is not reflected in the legal documents. Want to indicate the obligations and rights with respect to the resources (e.g. give service right to access photos and put in dropbox). May be able to revoke (possibly at a granular level) with a baseline that cannot be revoked. Once revoke, that agreement is remove (although you can see still see it in another section). But what you are shown is always the parties you currently have an agreement with. Dynamic expression of terms of authorization.

Dazza: Goal is a human speech, machine readable content that reflects the business deal. Some business arrangement in the beginning that allows for the granting and accepting of Scopes.

Need resource, scopes and identity

Can add how long the access is, etc. but these are the key components

In terms of creating the forensic data to show what the terms were, this is a good model

The goal is to kill the terms of service with extreme prejudice and then embrace terms of authorization that allows for the ability to support a user ecosystem

Doc: if we look at tracking as authorization does Do Not Track map on this

Dazza: In principle/theory, it may map

Doc: I'm talking more about taking that concern of an individual where they go to a site and are proscribing in a way they could act. One of the guys on our side, Chris Savage (DC Attorney), what he says is that you don't visit a website, it is a request for a file (Dazza: or resource…)

Phil: That's the 1995 version, now it's a discussion

Doc: There is a ceremony about how this works. Let's say you visit Google, there are terms of service that come to you in a file. What if, in the same way, Google says by accepting this, you are accepting our terms. That is flipped.

Mark: We need to solve identity, data and permissions, which is what you've done. Just to clarify, this is an aggregate view across contexts. This is not the agreement that binds both parties – where is the agreement that binds the service provider? This is a one-way IDA.

Dazza: One of the design requirements that would be most useful is to have an implementation that must map to existing business relationships, that do not include the full inversion. The subset of use cases this works for is when you have a system (the "s" in MODIS). It assumes that you have, in some way, some kind of platform, services, apps where there is an identity, platform, apps, services where we know all the parties that have agreed to be in bound by these agreement conditions. Could describe the business, legal and technical terms of the system – by implementing this system, you agree to a minimum set of terms.

Mark: can you see the other party's terms?

Dazza: There is a link where you have to have a link to the terms of the party. There is a tangle between the existing commercial terms and other terms. But there is a section in the legal and technical where you can link to existing terms and rank them. I am anticipating that someone else would do that, because I'm not sure what the assumptions are. This is more primitive than that.

Mark: Is there transparency?

Joyce: Is there a place to put the terms?

Dazza: There is a place in the personal data store in the MODIS system where this information gets dumped in a very unstructured way.

Question: Who should we expect to implement this?

Dazza: Three that we have: Technical University of Denmark, MIT and a hospital, Kansas Secretary of State's Office. Looking forward: e-commerce and NSTIC

All About Identity at Amazon Web Services

Wednesday 4G

Convener: Ian Wesley-Smith

Notes-taker(s): Ian Wesley-Smith

* Check out our best practices for users and permissions: http://docs.aws.amazon.com/IAM/latest/UserGuide/IAMBestPractices.html
* Question on Federating with University via SAML (Nathan from UW)
** Not possible currently, can write a proxy and use GetFederationToken (http://docs.aws.amazon.

com/STS/latest/APIReference/API_GetFederationToken.html)
* Discussed STS (http://docs.aws.amazon.com/STS/latest/APIReference/Welcome.html)
* AssumeRoles (http://docs.aws.amazon.com/STS/latest/APIReference/API_AssumeRole.html)
* Should I use AssumeRole or Federated Users?
** We suggest roles unless you have a special authorization requirement
* Can you assume multiple roles at the same time?
** No.
* Do you support MFA? Yes: http://aws.amazon.com/mfa/
* How are root accounts and IAM users related?
** http://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/aws-properties-iam-user.html
* Cross-account Access? http://aws.amazon.com/about-aws/whats-new/2012/11/19/Announcing-Cross-Account-API-Access-Using-IAM-Roles/
* We have a cloud HSM http://aws.amazon.com/cloudhsm/
* What certifications do we have? https://aws.amazon.com/security/
* Consolidated billing: http://docs.aws.amazon.com/awsaccountbilling/latest/about/consolidatedbilling.html
* Discussion about what federation technologies customers would like to see
** OpenID Connect Support
** SAML Support

Providing 1 Billion People with a Useful Personal Cloud is Cheap & Easy

Wednesday 4H

Convener: Patrick Deegan

Notes-taker(s): Patrick Deegan

Tags for the session - technology discussed/ideas considered:
personal cloud, scaling, deployment, minimum viable product

centralized to distributed

need to replicate services that exist presently and do better

This is the pattern in technology we expect to continue, thus after we distribute personal cloud resources, new services that take advantage of centralized efficiencies will pop up, repeat

bootstrap innovation to crowd-source killer apps

many types of trust frameworks or personal clouds is good

we need general purpose without many restrictions that does something really well

minimum functionality

communication utilities

content addressability

no global identifiers

need more resilient, distributed

discovery

identity

privacy

security

seemed to have some consensus around premise

get something done

various communities like Quantified Self, and internet of things can really benefit from a platform on which they can employ principles of open source collaboration (low coordination costs)

incremental

build upon what we already have and get into market, rather than trying to make perfect app and take a long time to release

experiment often and early to discover what customer wants

communication standards

http is example of protocol designed for one purpose that wasn't perfect for many of the uses we have for it today, however it is better (than what may have happened if the protocol was designed to handle much more) because it wasn't overly restrictive and people have found great ways to use it (ways it wasn't originally intended for)

worth looking into: automatic standard negotiation for interop

local standards

communities should be able to decide locally, don't impose global

some people showed up to see us deploy 1 billion personal clouds

still unsure if rackspace would willingly bill me

or press charges

Auditable Framework for Privacy Policies

Wednesday 4I

Convener: Adrian Gropper

Notes-taker(s): Karen Sollins

Work done about 5 years ago on Patient Privacy rights by Microsoft and healthcare provider

15 principles used for privacy policies – not listed here. (http://patientprivacyrights.org)

Many groups at IIW, each associated with privacy policies. Could be made "better", how dynamic, for each criterion – yes, no, doesn't apply. Not a service provider, so how is it supported? Auditors, standards organization, license to a group such as Kantara (assessments and certifications and develop profiles (FICAM and SAML), field working groups that may lead to work in standards organizations.

Business models (elements)

SDO (AAFP)

Assessment/certification (Kantara)

Auditors (Big 5)

WG – best Practices (e.g. UMA, move to IETF)

Question: how does one deal with unintended consequences? How can one manage the situation in which a mortgage company wants health information to know that won't die tomorrow. Problem is that the more information is available, the more organizations will demand it. Perhaps social norms are key to changing these behaviors. If have an exposable privacy policy, can begin to have a conversation about it. By focusing on a particular framework, may develop norms and can begin to concentrate on the basis on which decisions about privacy/exposure/control can be had.

The point of the meeting is to figure out a business model if privacy policies exist and is associated with the data and that provenance and accountability can be tracked, then the question is how to make a business model of this.

Who is the "source" of the privacy policies. Apparently, the only way the individual can be in control of the definition of the policies can reside with the individual, if they can take the data away. So, in this regime, the holder of the data (the healthcare provider) gets to define the privacy policies.

What would we all like to see in terms of a privacy policy that would allow the doctor to do his or her work, within the bounds of the privacy policy

Clarification: "Framework for Auditable Privacy Policies" – the policies must be auditable, not the framework itself.

Could we come up with a standard policy that is used everywhere, and then perhaps minor additions could be made and identified.

Policies can be controlled contractually, by regulation, social pressure (voluntary). If the latter, then maybe do it by creating a trust label of some sort. Australia has made such a choice with respect to identity in order to give citizens more confidence and happier with what is being done for them.

Another possibility is a Registry with rating of how positive or negative particular corporate policies. Question of how to do and how to fund. Crowdsourcing may not be the great alternative because of managing the possibilities of gaming the system.

Need to "put something out", but not sure what or what to propose to make something happen.

Patient privacy rights in the middle of transformation of healthcare delivery and big data. Needs something to be done that is productive, concrete and feasible.

What are the items that want to be able to audit? Have 75 items from big company and auditor company. Not much pushback on the actual items, as much as how to make the system work.

Who benefits from good results of the audit? Data holder benefits by not showing up on registry or putting gold star on website, or whatever.

Two kinds of registries – service – those sneaky bastards vs. crowdsourcing.

If label doesn't change the end user's behavior then there is no point. What behavior will change how? Want data holders, for example, to make data available to patients.

Patients are happy to share data for research if asked, but furious if shared without their permission.

Organizations that are very good about this are MD Anderson and the VA, but in general since consumers and doctors can't control the choice of who manages the data and therefore they have no interest in better privacy policies.

Regulation as a control mechanism has the problem that it will be controlled by the organizations with the money.

The only way to enforce HIPPAA is to bring a lawsuit.

Cryptographic SSO for Mobile Devices

Wednesday 5D

Convener: Francisco Corella, Karen Lewison

Notes-taker(s): Karen Lewison

Tags for the session - technology discussed/ideas considered: cryptographic authentication, single-sign on, mobile authentication, uncertified keypair

SSO for both native applications and web-based apps based on shared login sessions.

Lively discussion comparing this to the approach in session T4F by Sascha Preibisch.
Blog post which describes the presented technique.

OAuth 2 Federation

Wednesday 5I

Convener: Patrick Radtke

Notes-taker(s): Patrick Radtke

Tags for the session - technology discussed/ideas considered:

OAuth2, Token Introspection

Problem:

Our enterprise has an OAuth2 Authorization Server (AS) that users use for granting consent and revoking tokens. Each SaaS provider we use also has an AS for the resource servers (RS) hosted with them. The user experience is bad since users need to consent in multiple places, and need to visit multiple sites to view what consents are given. From an enterprise perspective there are additional security concerns. If a user's account is comprised or if the user is fired how can we can we view and revoke granted tokens across all SaaS providers.

Proposition 1:

One method to solving this is to have the RS at the SaaS provider trust tokens generated by out enterprise AS. The group recommended that the enterprise AS generate a simple JWT that contain the issuer and then the RS could verify the signature on the JWT (since it knows the issuer) and use a token introspection endpoint (define through a pre-arranged data sharing) to gather additional information (scopes, subject, audience, validity, etc)).

The enterprise AS would need to know a bunch of meta-data associated with the RS such as scopes and scope definitions. Likewise the RS would need to know meta-data about the enterprise AS, such as a verification key, token introspection end-point, etc. It was recommended to look at OpenID connect for how they have defined much of the same meta-data.

Making the SaaS's RS rely on the enterprise AS is only half the coin. The second aspect is how the client knows to send the user to the enterprise AS. For custom, or configurable clients we could configure the enterprise AS, client id, redirect_uri, etc for those clients. However, for existing 3rd party applications ,such as Google Drive, things are more complicated. The default Google Drive

client does not know the user is accessing the enterprise Google Drive and should login at the enterprise IDP, and be sent to the enterprise AS. Additionally, the default Google Drive client won't be registered with enterprise AS and it may not be capable of or, by enterprise policy, allowed to do dynamic client registration.

Proposition 2:

Alternate propose solutions were to perform AS to AS communication. The enterprise AS could talks to the SaaS AS and mint tokens on behalf of the user. There is currently no specification on how this protocol or delegation would work and the group decided to concentrate more on what could be done within the existing RFCs.

It was pointed out the most complicated aspect of this is not technical, but will be convincing SaaS providers to support externalized authorization servers in the first place.

Architecting a Self Regulating Society

Thursday 1F

Convener: Matthew Schutte

Notes-taker(s): Sarah Allen

models & methods of a self-regulating society?

methods for enabling emergence?

matthewjosef@gmail.com

15 years of thinking about how you enable government at global scale

-- need to get the lowest levels right, not too much responsibility, enable innovation

-- what are those components?

Question: what do you want the outcome to be?

wrong way to ask the question: change the bottom levels, and see the system that emerges

actually: platform can be general humans and all systems regulate themselves in some ways, humans have used technologies over time to enable collaborate

language, writing, print, the internet

belief: if you push power to individual decision-makers, not only allow them to turn to or subscribe to resources

also control what they put out

if you build this stuff in (privacy, reputation), it will be a self-healing system with opportunity for redemption

what is the content?

how do we create graphs of relationships?

not requirement of forcing agreement of the identity of things -- I make a cell phone and you make a cell phone, but maybe they aren't the same thing... you could make a map of the similarities and difference of the things, allow people to understand how to navigate between them

this is how ants work... if an ant has done the work of exploration, there is some signaling

3 principles (someone notices from initial summary)

- continuity over time

- reachability

- designations that are persistent

what about forgotten? story about blah blah car, conversation about public reputation -- allow sharing to happen, but check for time

you aren't going to be able to solve this all with technology, you also need etiquette and...

Bruce Schneider book -- as societies we enforce behavior, mechanisms are different at different scale

hypothesis: if we build this mechanism well, then the problem is simplified, even at large scale, we can respond effectively to social pressure

don't expect this to replace government, but reduce the need for police enforcement

XDI. RDF enabling you to navigate relationships

content addressability

feedback mechanisms

reputation of an object -- need to have meta-data

voluntary dissociation -- freedom to leave without force keeping you there, may be social repercussions

attribution -- who did what (authorship may be too strong a word)

data lineage

Let's get down to the lowest level:

what does an ant need to talk to another ant?

Signals?

signals that people send back and forth to each other, have rate & context

ants have simple rules they are following

who are the players?

- autonomous agents or people or ...?

what mechanisms do you need to start from disjoint nodes and build a social graph?

thinking back to the beginning of time? what do people need for collaboration? trust & ethics

response: push that to the users

discussion of crime, negative & positive reputation, with systems of contract, insurance, and reputation systems (escrow is an important part of this)

is crime relevant to the purpose of collaboration? if someone creates a new identity & creates a bit of knowledge, do I care that they committed a crime with their real identity?

immutable information, you don't necessarily delete things, but rather add markers that it is no longer relevant after a certain point in time

graph theory

how to address things? what about a URL? URL has domain name in it, which assumes it is remote (or relative which is imprecise)

we need some unique identifier, use git as a model

note: Zooko's triangle

low level mechanism : reliable designation

no one naming system can all have three

memorability is something that content addressing doesn't have

the HCI of content addressing is not that you look at the address and make sense of it -- you look at the content and know what it is

without human readable addresses, the web would actually be less breakable

this is part of Time Berners Lee's initial vision of the semantic web, but he couldn't build Xanadu

there is a level of maturity of supporting technologies that enable us to do new things

not enough to understand that something that went before didn't work

not that the vision was wrong

important to know why it didn't work

Granovetter designation system, "pet names"

It is significant that we can find something, not what it's underlying technical content address is

anti-requirement -- it is ok if 2 people (or two things) cannot talk directly

two people could have different graphs of meaning that refer to a single object, objects have annotations which are user's meaning, definition of what they are

Objects can

- able to designate itself to others

- able to pass on other's designators

- specify actions

- permissions -- if you don't have permission to use it, then it should act like it doesn't exist

UMA (User Managed Access) & OAUTH might be useful (as concepts), but details will need to be changed since these are http based

Metaphors and Models of "What is Personal Data": Implications for Policy and Technology

Thursday 1H

Convener: Marc Davis

Notes-taker(s): Nora Draper

Tags for the session - technology discussed/ideas considered: Metaphors, digital self, personal/ private space

[note: version of slides on slide share @marcedavis]

Applications of humanistic theory to computer systems

Understanding metaphors that support understandings and definitions of personal data and personal clouds

[introductions around the room]

Marc's Presentation:

Tremendous variety and overlap in interests in this space

Goal: new definitions and metaphors for understanding what is data, identity, privacy and personal data

Whether it is the cloud, store or vault, what is inside is personal data

First question: What is a person? Depends on our history of what we understand as a person. Right now we have protocols and norms about what it means to be a person (build around normative structures and behaviors). The ways people understand digital architecture are based on their experiences of embodiment and physical architecture.

George Lakoff: our forms of embodiment depend on the architectures we embody

Digital architecture is largely invisible. Very little standardization. Knowing what are the expectations of how to behave is difficult.

Privacy is about who has access into my behaviors.

In the digital landscape, which we have had limited opportunities to experience with. We gain a lot from understanding our physical metaphors that allow us to communicate with each other.

Another notion of personhood has been created in the law – legal personhood. Legal manifestation of ourselves with is related to how we think of ourselves and how we create value.

Web of the world. Three phases of the web: (1) web of pages; (2) web of people (5 years ago with Linkster and Friendstar); (3) web of the world (overlay of connections between people, places, times, actions and relations)

In the web of the world emerges the digital person – based on the generation of digital data

Personal data (EU) – information or data related in some why to an identifiable person

Metaphors:

Personal data is the new old of the internet and the currency of the digital world (Meglena Kuneva)

Interesting metaphors because it suggests data has value – because does it need to be refined, is it an

asset, is it property

No answer to “what is personal data” that anyone has access to

If you say data in currency – your data is your back statement – money is data (symbolic)

Documents and data has value – more holistically

Whole set of existing metaphors for brokerage and trading that people understand (not necessarily applicable on a one-for-one basis, but a starting point for understanding personal data)

Three notions of me: physical, legal and digital

Dominant Metaphors:

Digital self: my personal data is me: what rights apply if data is me? Human rights that are inalienable

Digital property: my personal data is mine: ownership rights in data (Personal.com and the Ownership Agreement) – challenge: data doesn’t have only one owner (subject and producer) – essential in rethinking

Digital Speech – my personal data is by me – this is about authorship – data as a speech act

Other Metaphors:

Data is about me (utterances by others)

Data is to me (information sent “to” me)

Data is from me (information send “by” me)

Data is for me

Just a few prepositions give you a string of metaphors that attach to personal data – helpful frame for analyzing the approaches to personal data.

If it’s a human rights, there are things you can’t negotiate away through contracts. If it is ownership, it is not clear who has ownership.

Always need to think of who are the parties. The assumptions may not be the same in all contexts.

When we talks about groups – who has ownership in groups?

What kind of space is digital space?

What space do digital persons live in

Private physical spaces

Public physical spaces (domains – metaphors that is transferred to the web)

These metaphors don’t necessarily transfer that well to the digital act – because data in the cloud is not treated as a personal space

In western democratic societies – the public square is really important

In the web: where is your home and where is your public space and where is your private space?

Other spaces: work space and prison space?

Do I live in a personal space, work space, corporate space (e.g. email stored in corporate spaces)

Redefining ideas of personal space in the digital space

Panopticon: redefining notions on privacy in digital space, corporate space/prison space

In digital space: we don't have public or private spaces anymore

Political Economy in which people live in: we live in digital feudalism because we don't own our name, property, labor, etc.

Digital enlightenment: human rights, property rights, free speech

Forming new types of societies through the new types of digital metaphors that we are inventing

Reference: The Online Initiative

Reference: Rik Van Der Kooi – To Track of Not to Track

In the 18th Century – can we experience change without the bloodshed and pain that we experienced in the revolutions that brought us to the enlightenment era?

Bloodless revolution:

The stick: EU data directive is about the fundamental right that citizens have to their data

The carrot: VRM (a better economic model for advertisers)

The right left alignment in the US around ECPA – Grover Norquist

At this point, the pain isn't bad enough and the pleasure is too good (it's not 1984, it's Brave New World)

Anonymity is dead – so you need to have a way to claim ownership

Data Protection (Avoidance?) in EU and US

Thursday 2E

Convener: Valter Nordh

Notes-taker(s): Valter Nordh

Background:

Transfer of Personal Identifiable Information (PII) within and out of EU is regulated.

How do we enable the transfer, for access to services needed attributes, of PII within an id-federation – WITHOUT the need for signing a full mesh of contracts between all IdPs and SPs?

This talk discussed how the GÉANT Code of Conduct solves transferring PII in order to ENABLE access to a service, such as e-mail, username, Name – primarily within the EU.

Full information about the Code of Conduct is found at:

https://refeds.terena.org/index.php/Data_protection_coc

The Code of Conduct is licensed as creative commons, meaning that this work can be reused for other purposes as well.

Out of the Ivory Tower

Thursday 2H

Convener: Nora Draper

Notes-taker(s): Tom Brown

Two sociologists

1. Erving Goffman - identity as strategic, many selves depending on audience w/ consistent narrative

2. Anthony Giddens - identity as inherently risky in terms of outcomes (not necessarily consequences)

Identity is complicated by digital landscape. Early days of Internet was like Goffman.

As web became more commercial, companies are asking us to perform with a consistent identity.

Certain speech and behaviors get lost when limited to one identity. For instance, part of liberty is being a banker and talking about anarchism.

Emergence of cities important to freedom as it allowed reinvention.

Consider commercial tools that have given us a space to have some control over the identity choices we have.

Giddens says that identity is not just a series of performances as it is constrained by different attributes.

Online, we are constrained even further. Is your personal cloud your one true identity?

Under certain circumstances, the web is more forgiving of performances than in real life.

Notion of physical person vs. legal person, vs. digital person.

Because digital architecture is invisible, people are not clear about what can be seen.

On whose terms am I performing?

You should be able to see what you've done. With today's web, there are some other people who have a better knowledge of how you are presented than you do. For instance, in aggregated space, if my friends have defaulted on loans, I'm perceived as more of a risk.

The model of identity chosen influences the design that is produced. Which model of identity is more desirable?

Is society enforcing a norming effect?

Practical Obscurity

Online, middle ground is curtailed -> Norton's law: in the end, all data is either deleted or public.

namecoin.info

A trusted system has ability to betray me

No idyllic past. Not looking to go back to optimal moment.

Respect Connect

Thursday 3A

Convener: Peter Davis, Dan Blum, Drummond Reed

Notes-taker(s): Drummond Reed

Online slides available here: Here is the link to slideshare … http://www.slideshare.net/lchasen/iiw-16-neustar-presentation

Drummond Reed provided an introduction to this session by explaining that shortly before IIW, Doc Searls had issued a challenge to the IIW community that we have been working on user-centric Internet identity for 8 years now (this is IIW #16) and not solved the problem, so can the emergence of personal cloud infrastructure finally solve the problem? The purpose of this session was to discuss how it could be done via a service that Respect Network called "Respect Connect". It is a single sign-on protocol that operates similar to Facebook Connect but from your personal cloud.

Peter, who is a security architect at Neustar that's been involved with SAML, OAuth, OpenID, and other federated identity protocols, then explained that the purpose of this session was to gather requirements for Respect Connect.

Peter proposed to do that by building a list of "positive goals" for the Respect Connect protocol. Following is the list that was compiled in this session.

Positive Goals

- Does not spill your life (presence silence)
- Convenience/ease of use
- Non-invasive
- Adoption by relying parties – RP acceptance
- Relationship management
- Redundant login

Following are notes on the discussion that took place as the list was built. Note that they are incomplete because the attendance was very large (~60 people) and discussion was extremely active.

Sarah Allen, whose company Blazing Cloud has done a number of social login integration projects, said there were two main reasons that relying parties (RPs) want to offer social login:

1. #1 reason is ease-of-use: one-click login.

2. #2 reason is "do what I mean" login, i.e., users know how social login works, and are confident it is going to "do the right thing" (i.e., get them logged in without hassle, not necessarily do the right thing with their data).

Sarah also said that people to NOT want to give permissions to something that they do not yet understand. The drop-off is very high if you ask for more than 3 things.

There was a long discussion of user experience. Current UX is based on norms set by Facebook, Twitter, or LinkedIn. It can be different for personal login.

Kevin Cox said, "I want to be able to just 'Say hello'".

Others said there was strong desire for being able to start a relationship with as little information as

possible, and then go through “progressive disclosure” or “selective disclosure” or “iterative identity”.

Another positive goal was the ability to have a direct contractual relationship with the site vs. having another third-party (e.g., Facebook, Twitter) in the middle.

George Fletcher made the point that sites will only adopt Respect Connect if it gets the RP more customers and/or better customers.

There was a long discussion about account recovery, and how Respect Connect personal cloud login would need to account for that. George felt that was very important.

Kevin Marks pointed out that LinkedIn is good about having multiple account recovery options because people lose their email addresses when they lose their job.

Drummond and others talked about how a personal cloud could make account recovery easier since there are so many reasons for a user to keep a strongly authenticated connection to his/her personal cloud.

There were many comments about adoption. Someone observed that Karl Marx said, “It’s not human consciousness that will change, it is the human condition.” This means there has be some benefit to everyone of this new way of doing login.

Gary Rowe made the point about the benefit of individuals having one place from which to use it, manage it, update it, back it up, etc.

Drummond made the point that Respect Connect needs to work for any personal cloud hosting option, i.e., both self-hosted and CSP-hosted.

Kevin Marks suggested that it needs compatibility with Mozilla’s Browser ID.

Doc said that personal cloud login could be a way to start a VRM relationship but he doesn’t want to overload it so it becomes unsimple.

We also talked about terms and how Respect Connect could help individuals assert their own terms. Doc was concerned about the RPs not wanting to stop “being the cow” in a calf-cow relationship.

It was observed that Grameen Bank made micropayments work by using group reputation pressure.

Peter said that reputation could be very important because it be associated with each “individual IdP”.

Mark Davis brought up levels of assurance (LOAs). That could an issue, but there are also ways to handle it.

T.Rob brought up the challenge of physical security becoming important for an RP, and many personal cloud hosting options not providing it. This could be addressed by a personal cloud trust framework architecture.

Drummond brought up pseudonyms and how they are also important to consider as part of Respect Connect from a privacy perspective.

Conclusion: there was tremendous interest in driving Respect Connect forward, and a number of participants volunteered to work with Peter and Drummond to develop the specification.

Durable Online Identities

Thursday 3G

Convener: Jeff Hughes

Notes-taker(s): Vicki Milton

Goal: Determine the attributes of an account that might make you want to hold onto them for a long time

- Reasons to create an account
- Got a new device and it requires an account
- Want to communicate people -- want an email service
- Forgotten password on previous account (inverse to reason to abandon on previous account)
- Got an anonymous email -- persona expression
- Got a real name -- persona expression
- Changed name -- persona expression
- Required to purchase/download transaction
- Easier to create than to recover an account (where value doesn't justify recovery effort)
- Creates different identity per service to determine where spam is coming from
- Control issue- Uses as a redirector to important, highly protected email
- Reasons to keep the account
- Got the exact name that you wanted
- Data held within the account is of value
- Represents identity well
- Known address to friends
- Has a geo attribute that you can only get in that country
- Access to platform specific services (reuse of a seldom used account)
- Identity is sold off to others -- created ongoing target market persona used by services
- Personal domain that user has lifetime control over (as long as they pay the money)
  - Can move personal domain to different mail servers
  - Personal name I own
- Tied to history/data/people
- Used email in a research paper and known to other people (long time reference)
- Google account is tied to too many services (calendar, place, android) that limits ability to use
- Persona expression -- uses across similar sites
- Certain types of accounts are more secure or more trustworthy than others (FB vs. Google)
- Can't transfer the storage quota purchased with the account (digitial asset tied to the account)

- App licenses
- Content
- Game scores
- Points

o Have developed a trusted relationship with vendor

- Trust brand
- How data is handled

o Tolerance for only a small number of accounts to use/remember

- Reasons to Abandon (stop using)

o Switch devices

o Account compromise/security concerns/trust

o Seldom used accounts may hold data that is public facing and desires to keep visibility but doesn't update

o Community moved away from method -- so moved with community (myspace --> facebook, starting to happen at Facebook)

o Switch to another service (choice or move)

o Forgotten passwords

o The account has lost its utility (Reddit has concept of throwaway account) -- utility is that they are not durable

o Name change that requires a new account

o Public facing name such as email expresses name

o Death

o Created for the purpose of a one-time transaction

o Easier to create than to recover an account (where value doesn't justify recovery effort)

o Desire to start over completely

o Effort to clean up account is too high

o Spam

o Organization ID no longer available (EDU, company)

o Misusing account in marketing campaigns -- not targeting

o Didn't value me as a customer

Goal: Determine the attributes of an account that might make you want to hold onto them for a long time

- Reasons to create an account

o Got a new device and it requires an account

o Want to communicate people -- want an email service

- Forgotten password on previous account (inverse to reason to abandon on previous account)
- Got an anonymous email -- persona expression
- Got a real name -- persona expression
- Changed name -- persona expression
- Required to purchase/download transaction
- Easier to create than to recover an account (where value doesn't justify recovery effort)
- Creates different identity per service to determine where spam is coming from
- Control issue- Uses as a redirector to important, highly protected email
- Reasons to keep the account
- Got the exact name that you wanted
- Data held within the account is of value
- Represents identity well
- Known address to friends
- Has a geo attribute that you can only get in that country
- Access to platform specific services (reuse of a seldom used account)
- Identity is sold off to others -- created ongoing target market persona used by services
- Personal domain that user has lifetime control over (as long as they pay the money)
- Can move personal domain to different mail servers
- Personal name I own
- Tied to history/data/people
- Used email in a research paper and known to other people (long time reference)
- Google account is tied to too many services (calendar, place, android) that limits ability to use
- Persona expression -- uses across similar sites
- Certain types of accounts are more secure or more trustworthy than others (FB vs. Google)
- Can't transfer the storage quota purchased with the account (digitial asset tied to the account)
- App licenses
- Content
- Game scores
- Points
- Have developed a trusted relationship with vendor
- Trust brand
- How data is handled
- Tolerance for only a small number of accounts to use/remember

· Reasons to Abandon (stop using)

o Switch devices

o Account compromise/security concerns/trust

o Seldom used accounts may hold data that is public facing and desires to keep visibility but doesn't update

o Community moved away from method -- so moved with community (myspace --> facebook, starting to happen at Facebook)

o Switch to another service (choice or move)

o Forgotten passwords

o The account has lost its utility (Reddit has concept of throwaway account) -- utility is that they are not durable

o Name change that requires a new account

o Public facing name such as email expresses name

o Death

o Created for the purpose of a one-time transaction

o Easier to create than to recover an account (where value doesn't justify recovery effort)

o Desire to start over completely

o Effort to clean up account is too high

o Spam

o Organization ID no longer available (EDU, company)

o Misusing account in marketing campaigns -- not targeting

o Didn't value me as a customer

Gender Lens

Thursday 3H

Convener: Kaliya Hamlin

Notes-taker(s): Kaliya Hamlin

Tags for the session - technology discussed/ideas considered:

Gender, Women, Protocols

We opened the session, as I like to do inviting people attending to share why they came and why I wanted to host the session. I took notes via post it notes and this is a reflection of those.

Why?

Being fascinated by the issue and dynamic of gender in the world, the language around the internet, around the event (IIW), what are we creating and how are we creating it. The body language seen. How the conference flows.

Media frames of women and the emerging tools.

Protecting them from “online predators”

And how good girls are seduced into sexting

What does technological production of their own experience of technology really mean

Big Data is a Gendered Issue.

Big data is being mined to find the “commercial value points” of life marriage, family etc.

What about user (women) friendly translation services to consider the implications?

Mommy tech blogs?

BlogHer but they are being drawn into existing advertising tools/networks that “comodify” their users

She’s Geeky creates place for peer learning between women

Kaliya put forward a vision of an event that might bring leading well known Feminists with public voices and and Technoliterate women together.

Imbalances throughout the whole chain of value. Women are making 82% of all purchasing decisions but are not even at 50% in so many aspects of the value chain that brings them products.

Chief Household Operating Officer

use-case development

What are current folk data management practices

Women who are technical and hacking it together

Complex households beyond nuclear family

Celebrating Gender differences – between men and women with different leanings/capacities.

What do women want?

To manage their things?

Or to manage their people?

Data from custodial / stewardship relationships

Children

Elder parents

Disabled adult children

Will it help you manage

What will be more burdensome? Better tools might make “more work”

How are different generations interacting with technology differently.

Criteron Gender Lens Project

Women and investing with a gender lens is an opportunity

The guy who joined the conversation put it out that the kinds of architecture and shapes/designs are feminine and that these new distributed autonomous node architectures are part of the return of the divine feminine.

Protocol: How control exists after decentralization. An inspiration for me in doing the work I do about identity - the Identity of people and the protocols that define it really matter for the future – because

they will define how people are. This book talks about ICP/IP was a balanced protocol/central decentralize.

Are the current tools (big data etc) stripping the end user of their humanity? Is there a cognitive disconnect between the tools and the marketplace. The formation and sculpting of these tools matter.

Women are being encouraged to entrepreneurship and funding and to do coding/developing.

TED talks and presenting…(Getting support to do them)

We thought maybe we should start Teddy talks - sponsored by Victoria Secret with women in all kinds of bodies.

Self-Hosted Personal Clouds (FreedomBox and Raspberry PI)

Thursday 4F

Convener: Markus Sabadello

Notes-taker(s): Markus Sabadello

There are still many different ideas around personal clouds, but what everybody agrees on is that they are about giving individuals more control over their personal data and identity online. Therefore it seems logical that it should be possible to self-host personal clouds using appropriate hardware+software at home.

During this lunch session, we looked at two different projects that could be relevant for this purpose.

1. http://ark-os.org/ is a Linux image for the Raspberry Pi. On its website it uses language very similar to the personal cloud community (“ensure your privacy”, “decentralize your web”). During the session we got ark-os up and running on a Pi and were able to access its web interface “Genesis”, and we experimented with some of its functionality.

However we couldn’t quite understand what it is that qualifies it as a “personal cloud”.

2. We set up a combination of FreedomBox + Unhosted + PageKite. The idea of the Unhosted initiative is that on the web, apps should be separate from data. When using an Unhosted app, then that app doesn’t have its own backend storage. Instead, you tell it the location of your storage provider (“remoteStorage”) which you can choose yourself. Several companies currently offer remoteStorage. Your FreedomBox at home can also be your remoteStorage and therefore provide the storage for Unhosted web apps, if it runs appropriate software. In this case, the PageKite tunneling software gives your box a public IP address through which it can be reached from the Internet. During the session, we successfully set up this stack of FreedomBox, remoteStorage and PageKite, and we used the “SharedStuff” Unhosted web app as an example, which allows you to request and offer physical assets for sharing with friends.

What do Women Want?* * From the Personal Data Ecosystem

Thursday 5E

Convener: Lisa LeVasseur and Marion

Notes-taker(s): Lisa LeVasseur

Tags for the session - technology discussed/ideas considered: Gender, Women, Personal Data Ecosystem

Lisa's slides in .doc form.

Hypothesis: Women's needs/values/ expectations of what PDE's can enable are different from men's

Purpose of Session

Open a dialogue for understanding women's expectations regarding PDE-enabled services.

Share this information to developers in the PDE space, because there may be opportunities.

Time Savings

Auto Form Filling for me and my family

Solutions must recognize that certain tasks are time sensitive

Populating the PDS has to be painless

Don't make a new task for me

Remember me, but

Tell me what you're doing (details, please)

Be trustworthy

Ask for my permission

Customer Service should actually work

Trustworthy

I'm suspicious of sites that aggregate too much of my information

I want to aggregate things myself within the safe confines of my PDS

I'm wary of bank services

If I'm going to put all my and my family's stuff in a PDS, it had better be secure (like military grade security)

Controlled Sharing

I want to get vendor recommendations (reputations) from my social graph not strangers

Especially from my female community (My Village)

I want intelligent sharing to My Village, but I want to retain control and be in the loop

To confirm

I want easier ways to share and/or solicit feedback from My Village

Easy to Use, Reflects My Needs

Technology should be smart enough to prevent me from accidentally torpedoing myself.

And should be forgiving if I do.

Technology should support my multi-tasking behavior

Tasks are often accomplished in an interrupt driven fashion,

Work with organic, non-linear task completion in mind

My priorities “algorithms” have MANY factors and are deeply ingrained in my head; hard to instruct other people and services about.

Often, I’d rather do it myself.

A Wife or Personal Assistant

Calendar help and automation

Supply Calendar – when I need to re-stock stuff

Schedule Calendar – what I’m doing

Automatically produce a journal/archive/historical reference that I can consult.

Help me understand how I spend my time

Weekly spending summaries,

Activity summaries, etc.

Help me not waste my time

Summary

We want things to be more like people.

We don’t want more ways to manage things

Marion’s Notes:

Women represent a superset

Solutions should be designed not just by men

Women want things to be more like people

Women are not only interested in managing things; women want:

customer care

more time

autoform filling for the entire family

trusted bill pay service; banks not considered trustworthy

remember me with permission, detail and trust

forgiving tech and pre-emptive

clarity

support multi-tasking in time and space

Women:

-dont trust services that aggregate information; women are skeptical. Women want the option of aggregating themselves within their own private domains

-have algorythms in their heads- they are variegated and they factor in their priorities

-want vendor reputation that is overlaid on social graphs especially within the female community (the my village concept)

-easy opportunity to share and get feedback from ones own village

-smart sharing and social graphs along with sole control

-want to be kept in the loop

-want what has historically been embodied in the image of a “wife”-- a holistically supportive, keep every detail of one’s life in order and ever moving forward toward achievement and completion:

supply wife, scheduling wife,

-a calendar that works through female cognition

-a journal/history/archive

-a dashboard with summaries of spending

-a way to help me not waste time

-a weekly reflection and summary of activities that can/should/should not “carry over”

Creating a Personal Cloud Community

Thursday 5F

Convener: John Light, Kaliya Hamlin

Notes-taker(s): Judy Tuan

Why did you come to this session?

seemed the most interesting

what does “personal cloud” mean?

Identify what we’re going to do with pdec (what does it to, and how does it relate to the other orgs doing work here?)

trying to understand the personal cloud space, collectively where people think they’re going (in terms of next steps) after this conference (in the next six months). Find patterning/overlap and connect. Carnie labs (learning technology) – student and learning efficiencies. Consumer of products that would be developed here. Want identity and tracking services as part of a suite (instead of

community (john)

because I missed all the other Kaliya sessions

future of user-centric identity & personal clouds

fascinated with personal cloud tech, want to see who’s building stuff, integrate with the one I like the most

Kaliya made me come

Kaliya: worked really hard in the last ten years on these topics. How do we support the good things that we all believe in happening faster? How do we support a mix of organizations and business models and strategies for those companies? Organizing the resources to convene and bring people together: how do you sustain that glue that connects the pieces to make stuff happen? Questions about how to navigate moving forward. Also: really concrete next steps. What are the core problems we want to get solved? What community infrastructure should we set up tomorrow?

Roadmap / learn

more talking. I like community. Make sure we don’t end up in little silos. Share information and actually use the stuff!

Continue the conversation after we leave here. One of the key things pdec can help with

communities share values and also resources. Purely peer to peer environment: makes sense to have p2p currencies, and p2p pretty much everything. If people are going to own their data, no need for the intermediaries. Fitting all the pieces of the puzzle together to have a vibrant ecosystem, and people feel empowered to do whatever they want with their personal cloud. But one company can’t do everything for all people, and there needs to be synergy between the pieces!

If there are different strategies to get to an outcome, then what did you envision?

partnership. Share customers. Example: my customers need storage, your customer needs currency to trade between each other.... we should all be specializing. What’s going to be the standard holding us all together so everyone can talk to each other?

XDI is important: secure protocol for information/data sharing

if there are other options, small communities can choose different protocols and the larger community can't talk to each other. But hopefully we can build a p2p environment where we can all talk to each other

VRM (vendor relationship management)

strategies for a couple key things

how are we growing the userbase? Adoption.

do we want to grow a community of people who want to adopt it but can't yet because it doesn't exist yet?

Homebrew computer club spirit – would love to see this happen in more places. Linking them together / viable ongoing strategy

how do we create interop? Early winter in London: brought the companies in the consortium together to talk about interop. Convo about hosting some interop jams: let's meet and figure out what interop looks like and how we're going to get there in 2 months, 6 months. Is the time right to do this?

How do we get funding into this community? Companies, but also time and attention for people to organize and support it.

Funding

identify people who need or want this tech and are just dealing with what we have now because that's the best there is

growing spirit of people who aren't happy with the status quo

indiegogo? Etc

get commitment from people before the things are actually developed.

What are the things that we could crowd-fund? There's R&D....

Here was a lively discussion: some say "research can be crowd-funded," others say "no, that's not sexy enough for the end user" or "no, i'd rather build something with that money." Kaliya mentions there've been other conversations about what it would mean for corporate money to come into the research area of what we want to accomplish here.

or we could ask the users what they want.

Pure utility of having a single login

What's the best way of keeping in touch?

Mailing list. Archives are public: http://lists.pde.cc/lists/arc/personal-clouds

What we want: hand the user something and say "have fun"

There are a lot of great projects here. A lot of interop comes down to data formats. If we can read and write to the same data stores, that's powerful. One possible answer: semantic graph.

federated social web summit: bring together projects and leaders and do interop

work with federated web people, have a focused "we're hackers, I've got something, I want to make it work with the neighbors" and get them in a room together

pros/cons of semantic graph stuff? Other ideas?

Should we have this as a theme for one of the personal cloud meet ups? They're monthly. http://

www.eventbrite.com/org/3106466104

There's also "build the collaborative internet" in SF: http://www.meetup.com/Build-the-Collaborative-Internet/

What is the http://pde.cc/ ?

Membership fees: $150 in garage, $1000 if angel, $5000 if venture-funded.

By next week we'll have 50 companies (we have ~40 now).

Purpose of http://pde.cc/

pay for people to go to the events and represent our side, get the word out to entrepreneurs

infrastructure for community meetings and getting people together who are building stuff

providing a counterweight to nstic. They have people full-time; we don't.

When you do lift your head up from coding, you don't want to waste your time.

If you're a pdec member, you get my time and attention (helpful filter for other companies)

there is a role for totally open community. And fostering open-source projects. Coordinating role to support this

crowd equity funding is gonna show up soon

Volunteer development is leadership development. Recruiting volunteers == leadership.

We're inviting people who want to blog once a week or once every two weeks. We need to manage volunteers. What do people want to volunteer to do?

John drew a picture on the board: there are people here working on each piece. We need interop. People say: "oh, that's all!" People say: "no, this is spot on"

Drummond: this is the first IIW where instead of being pulled into conversations about high-level stuff, people are saying "i want to use this with that right now!" Maybe by next IIW we'll be seeing some of John's picture come together.

What do we solve in interop?

Doc: do mobile location privacy. Tons of policy and regulation around it. One of the biggies.

Sarah A: an instance of a personal cloud that a consumer would find useful and easy to make use of.

XDI? Is this an open question still or have we settled on it? Honestly, I have no idea how to build things on it. If there were a Ruby wrapper on top of it, that would be enormously helpful.

or a personal recommendation engine

what is the CRM tool available in an equivalently easy way as wordpress is available that they can get it installed and email people not through constant contact? Sugarcrm. Civiscrm? (Drupal)

Kevin from Salesforce is going to lead the initiative to build a connector in the next six months? Haha

change of address

Activity tracker

if you can build this tool, this is in huge demand in enterprise

who knows what, is good in what area

a lot of this is in peoples' heads

how are we serving the community? But also people want this

Idea: Personal cloud hackathon! Two weeks before the Napa conference

Trust Frameworks - Not Identity Centric

Thursday 5G

Convener: Jeff Stollman

Notes-taker(s): Jeff Stollman

Note online: http://www.slideshare.net/jstollman/heresy-21361306