

# Internet Identity Workshop 12 Book of Proceedings

**IIW**XII

INTERNET IDENTITY WORKSHOP 12



[www.interentidentityworkshop.com](http://www.interentidentityworkshop.com)

Book of Proceedings is 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\\_12\\_Notes](http://iiw.idcommons.net/IIW_12_Notes))

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

May 3.4 & 5, 2010  
Computer History Museum  
Mountain View, CA

## Table of Contents

Day 1 – Tuesday May 3 <sup>rd</sup> .....	6
Session 1 .....	6
JSON SPECS Suite & OpenID ABC (T1A) .....	6
Yahoo! DAA DNT Hybrid from W3C webtracking & user ID (T1B) .....	8
Google as an OpenID Relying Party Lessons, tips and updates (T1C) .....	9
RESPECT TRUST Framework (T1E).....	11
Identity 101 (T1G).....	14
Simple Cloud Identity Management – Overview and Use Cases (T1H).....	17
Government Regulation, Security Services and Bill of Rights (T1I).....	19
Session 2 .....	21
NSTIC, \$, IDPs, Telcos, Banks (T2A) .....	21
How to meet privacy goals of NSTIC (T2B) .....	22
Yahoo and Relying Party experience (T2C).....	23
Open ID ABC Identifier + Discovery (T2E).....	26
Federated Identity for Non-Web Applicants (T2F).....	27
VRM Overview (T2G).....	30
VRM + Browsers (T2G) .....	32
The line between public and private Internet ID (T2H).....	33
Users Managed Access (UMA) (T2I) .....	34
How many IDPs do we need? (T2P) .....	37
Session 3 .....	38
Verified ID in the browser (T1A) .....	38
Secure Cloud Interlop Using JWT + OAUTH (T3B) .....	39
An architectural approach to harmonizing data between personal data stores (T3C) .....	40
URL:.....	40
Convener:.....	40
Note-Taker(s):.....	40
Reputation Systems (Wuffie) (T3D).....	41
OpenID Session Management (T3E).....	43
PuSHee talk with Mitre team (T3F).....	44
Can Banks be IDP Providers (T3G).....	45
Portable Contacts 2.0 (T3H) .....	48
Security Measures Open Identity Protocols (T3J) .....	49
Session 4 .....	51
W3C Identity in the browser topic gathering session/Info Card (T4A) .....	51
New UMA Solutions for Scoped Access and Centralized AUTHZ (T4B) .....	52
How to coordinate digital identity efforts between Europe and the U.S.? In collaboration with “SSEDIC” European Project (T4D).....	54
OpenID User Info Endpoint (T4E).....	56
JSON activity stream spec (T4F) .....	59
System Factors for Fourth Party User Agents (T4G).....	60

When SaaS apps exchange data, what protocol should they use? OpenID, OAuth, SAML?	
What are the best practices? (T4H).....	68
Higgins 2: Open Source Personal Data Service (T4I).....	70
Bizzaro ID revenue from user purchased ID services (T4J).....	71
Open ID 2.0, OAUTH 2.0, Open ID ABC Where are we going? (T4L).....	72
Do Not Track, It Won't Work (T4N).....	73
<b>Session 5.....</b>	<b>75</b>
What is the State of Personal Data Today? (T5A) .....	75
Getting rid of usernames & passwords – for real? (T5C).....	77
OAUTH 2.0 Device Profile (T5E).....	78
Open XDI OX (T4F) .....	80
Data portability for trust framework (T5G) .....	81
Pros and Cons OAuth and Online Banking (T5H).....	82
Portable Context (T5I) .....	83
Ostatus (Federate the social web) (T5J).....	84
<b>Day 2 – Wednesday, May 4<sup>th</sup> .....</b>	<b>85</b>
<b>Session 1 .....</b>	<b>85</b>
Beyond the Nascar UI Google's Account Chooser (W1A).....	85
Chained Identity in Online Entertainment (W1B) .....	86
Information Sharing Agreement (W1D).....	87
Virtual Problems (W1E) .....	91
SCIM Use Cases (W1F) .....	92
Different IDP Business Model (W1I).....	93
<b>Session 2 .....</b>	<b>94</b>
Packaging RP Best Practices Google Identity Toolkit (W2A).....	94
Identity in the Browser: Open ID for Firefox (W2C) .....	96
UMA SMART AM Demo (W2E) .....	97
Public Policy around Identity (W2F) .....	98
How do we publish from our Personal Data Stores? Save the RESTful web! (W2G) .....	100
Trust, Identity, Commerce & Journalism (W2H).....	102
<b>Session 3 .....</b>	<b>104</b>
NISTIC. (W3A) .....	104
Proxy Auth for Native App Hosts (W3B).....	105
Respect Trust Framework 2 (W3C).....	107
User-Managed Access Authorization Manager UX Study (W3E).....	108
SCIM Core Schema (W3F).....	111
Reputation System (W3G) .....	112
Beautiful Payments with OATH (W3I) .....	116
<b>Session 4 .....</b>	<b>117</b>
UserAgent flow based on Windows Post Message (W4A).....	117
What's available for the shared user profile? Is Poco end all answer? (W4B) .....	119
Adapting Levels of Assurance for NISTIC (W4C).....	120
Building a Trust Framework for Multiside Markets (W4D).....	121
VRM and CRM (W4E) .....	122
SCIM Bindings (W4F).....	123
Two Legs Good? "Client-Server" OAUTH Usage (W4G).....	124

Extended Demo: UI for personal data store + data sharing on mobile device cubicon (W4I)	128
.....	.....
<b>Session 5</b> .....	<b>129</b>
Backplane Spec (W5A).....	129
Oauth and OpenID on mobile native UIs. How should it work? (W5B).....	130
How to Manage Digital Multiple Identities Securely and Assuring Privacy on the Internet (W5C).....	134
Payment Card Industry Trust Framework (W5D).....	135
VRM @ Work (W5E).....	138
ID Legal (W5F).....	139
Data as Currency (W5G).....	140
How Yahoo! Became RP: A Large Scale Implementation Study (W5I).....	144
Open Architecture for Step Up Authentication (W5N).....	145
<b>Day 3 – Thursday, May 5<sup>th</sup></b> .....	<b>146</b>
<b>Session 1</b> .....	<b>146</b>
For Public Consumption. Choose Wisely: Identity as Selective Pressure on Biology (TH1A)	146
.....	.....
Respect Trust Framework Q+A (part 3) Become a trust Anchor (TH1C).....	147
Data Portability for Trust Frameworks (TH1E).....	148
OpenID Specificatin Work (TH1G).....	149
Internet Bill of Rights for “Vegas” Model (TH1I).....	150
<b>Session 2</b> .....	<b>151</b>
IETF OAuth: Status & Next Steps (TH2A).....	151
MYDEX CIC (TH2D).....	152
NSTIC Attributes (TH2E).....	153
Purpose Binding (TH2F).....	154
Personal Data Ecosystems (TH2G).....	155
<b>Session 3</b> .....	<b>156</b>
What Part Is Identity and What Part is Personal Data? (TH3A).....	156
Open ID Specification Work (TH3&4B).....	158
Bill O’ Rights O Rama (TH3D).....	161
Strategies for Ubiquity (TH3E).....	163
NSTIC Risks Legal Liability (TH3F).....	164
News personalized by inference or expression... managing the users persona (TH3G) ..	165
The Locker Project (TH3H).....	166
<b>Session 4</b> .....	<b>167</b>
What part is Identity? What part is Personal Data? (TH4A).....	167
Open ID Specification Work (TH3&4B).....	168
How is it that the legal structures don’t have the right terms/approach for identity + data + What do we do about it? (TH4C).....	171
Personal Data Ecosystem (TH4D).....	172
Square Tag (TH4E).....	174
Red Teaming Trust Frameworks (TH4F).....	175
Give me tips on creating persona (TH4G).....	176
Field Guide to Real World Trust Frameworks (TH4H).....	177
Start-ups table (TH4M).....	178

<b>Session 5</b> .....	<b>179</b>
<b>OPEN ID Specification Work (cont) (TH5B)</b> .....	<b>179</b>
<b>Is There Value In An Open Reputation Framework, If So Where Should it be Standardized? (TH5C)</b> .....	<b>181</b>
<b>Digital Death (TH5D)</b> .....	<b>183</b>
<b>Real world VRM example + code for VRM App (TH5E)</b> .....	<b>184</b>
<b>Make OAuth Easy for REST Developers (TH5F)</b> .....	<b>185</b>
<b>Certified Identity (TH5H)</b> .....	<b>186</b>
<b>About IIW Events</b> .....	<b>188</b>

# Day 1 - Tuesday May 3<sup>rd</sup>

## Session 1

### *JSON SPECS Suite & OpenID ABC (T1A)*

URL: [http://iiw.idcommons.net/Introduction to the JSON Spec Suite](http://iiw.idcommons.net/Introduction%20to%20the%20JSON%20Spec%20Suite)

Convener: Mike Jones

Notes-taker(s): Nat Sakimura

Tags for the session - technology discussed/ideas considered:

JSON, Signature, Encryption, Token, OpenID

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

Topics Today

=====

Token: JWT

Signature: JWS

Encryption: JWE / JSMS

Key: JWK

Simple Web Discovery (JWS)

OAuth 2.0 spec

OpenID AB/Connect

Some depends on others. e.g, OpenID ABC depends on all the above.

JWT

===

- Consolidated several spec proposals.
- No canonicalization
- Common sets of registry would be useful?
  
- Main Goal: JSON Representation for claims to support signature securely.
- Schema? -- Binding specific.

JWS

===

- Algorithms: 3 HMACS, RSA, ECDSA.
- HS256 is mandatory.

## JWE

===

- Again, several proposals, e.g., draft-rescorla-jsms.
- Sitting down this week to come up with the JWS like spec.

## JWK

===

- Not a replacement to X.509 but for the cases that requires just public key representation.

## SWD

===

- Modular very simple disco spec.
  - OpenID ABC depends on it.
- No current draft to "push" content into discovery service.

## OAuth

=====

Currently, the followings are discussed in IETF.

- OAuth 2.0 Framework Spec.
- OAuth 2.0 Bearer Token Spec.
- SAML Grant OAuth 2 Profile
- JWT Grant OAuth 2 Profile (Private Draft)
- MAC Signature OAuth 2 Profile (Private Draft)

## OpenID ABC

=====

Spec are in three layers: Building Blocks, Protocol Bindings, Profiles.

- Goto OpenID blog. <http://openid.net/2011/04/29/a-map-for-openid-abc/>
- Open Spec Issues
- Kinds of identifiers supported
- Permissioning distributed attribute providers
- Claims specification and integration
- Trust metadata formats and transport
- OAuth 2 spec completion.

Q. Why so complex?

A. Being modular does not mean complex. Being a single spec does not mean simple.  
Not everybody needs to read crypto spec. Most should use libraries.

## ***Yahoo! DAA DNT Hybrid from W3C webtracking & user ID (T1B)***

URL: [http://iiw.idcommons.net/Yahoo!\\_DAA\\_DNT\\_Hybrid\\_from\\_W3C\\_webtracking\\_%26\\_user\\_ID](http://iiw.idcommons.net/Yahoo!_DAA_DNT_Hybrid_from_W3C_webtracking_%26_user_ID)

Convener: Wendell Baker

Note-Taker(s): Wendell Baker

Notes in PDF hosted on Wiki.



## ***Google as an OpenID Relying Party Lessons, tips and updates (T1C)***

URL: [http://iiw.idcommons.net/Google%E2%80%99s\\_Open\\_ID\\_Relying\\_Partyr](http://iiw.idcommons.net/Google%E2%80%99s_Open_ID_Relying_Partyr)

Convener: Tzvika Barenholtz <tzvikab@google.com>

Notes-taker(s):

Tags for the session - technology discussed/ideas considered:

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

Website with summary on Google's status as an OpenID relying party:

<http://sites.google.com/site/oauthgoog/UXFedLogin/google-rp-status>

The presentation that was given is at the following URL:

[https://docs.google.com/present/view?skipauth=true&id=ajkhp5hpp3tt\\_87ds3v38fk](https://docs.google.com/present/view?skipauth=true&id=ajkhp5hpp3tt_87ds3v38fk)

Notes on the presentation slides, by slide number:

1. How is OpenID helping Google?

2. 50% of google account users = Gmail users

Other 50% = people with email from yahoo, hotmail, aol, etc...

AOL big in USA

3. Basic and insufficient

4. Google wants to show customized search results (with your permission). Wants more logged in people, better email verification

Want unified across the Web: Google or Yahoo, login box should always look the same

5. 2 groups of people: Those with/without google accounts

What if Google account created already with email address from yahoo? How can we increase retention?

Must not make things more difficult and costly to support.

6. OpenID sample store is a best practices sample when a 3rd party website is delegating identity to 3rd party providers: <http://openidsamplestore.com>

Standard instance of the open source OpenCart package where the login system has been changed to use OpenID

Need to reduce webdesk costs. There are a dozen videos on the sample site that show the scenarios that people get themselves caught into. The sad reality is that there are lots of edge cases that are horrible.

**7.** The vision is to get to opened logging to be as simple as regular login. The prototype federatedux.appspot.com is a preview of what Google would like.

**8.** The approach to RP was gradual. At first, Google verified the email address by doing it inline (instead of sending an email to your inbox). => double-digit increase in the % of accounts verified.

**9.** OIX Trust framework is an additional layer that OpenID providers need to provide so that the whole process becomes smooth (such as language support, etc...). See <http://sites.google.com/site/oauthgoog/>

**10.** The next step after implementing verification was to implement a whole signup flow. With the OpenID process one can give the user a better signup experience. See it live at <http://www.mysears.com>. Click on Google and create an account. It's brand new and allows you to create a Google account using other providers such as Hotmail. Then it uses that account to login to mysears.com.

It's all about making things smoother for users.

Discussion: most people want one profile per email account, which is why Google doesn't have multiple emails per account. If people need to "merge" accounts when they get invites from multiple email addresses, they manually share docs on those accounts in Google Docs for example.

**12.** This schedule could be accelerated if you're starting a website from scratch.

**14-15.** If you're using an email from a supported provider on your Google account, you can "upgrade" to the federated account to get rid of your password and use OpenID. If you leave your password empty when logging in on Google to such a supported account, you're sent to an OpenID signup flow.

Google needs more people to sign up for this and test it.

**16-17.** Unless a company is in a special case where it provides email, using the two-tab login box from the sample site is the way to go to provide OpenID.

Be careful, it's all about reducing the dropoff. Don't try to change something (using password) if it adds steps and makes it worse

**19.** The next step will be the identity selector. There's a full session on the account selection on wednesday.

**21.** Google is recruiting more IDPs and RPs. If you have many people logging in with user/pass and have a helpdesk, this is for you. Use companies such as Janrain and Ping if you can, without reinventing the wheel.

## **RESPECT TRUST Framework (T1E)**

URL: [http://iiw.idcommons.net/Respect\\_Trust\\_Framework\\_%26\\_Founding\\_Trust\\_Anchors](http://iiw.idcommons.net/Respect_Trust_Framework_%26_Founding_Trust_Anchors)

Convener: Drummond Reed, Scott David

Notes-taker(s): [tom.holodnik@intuit.com](mailto:tom.holodnik@intuit.com)

Tags for the session - technology discussed/ideas considered:

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

Intro to Trust Framework: tools and rules; what technology is used? What rules apply in a legal and technical sense? Technical, legal, and Product scope.

OpenIdentity Exchange OIX): [openidentityexchange.org](http://openidentityexchange.org)

- neutral home for open identity trust framework construction
- opened to be used by federal agencies
- not based on Nat'l ID cards
- industry identity providers certified to be IdPs that GAO approves.
- Gov't doesn't bless any IdP
- Kantara, inCommon: trust framework providers created open identity exchange (ICAM) <http://openidentityexchange.org/trust-frameworks/us-icam>

Consider the trust triangle:

Identity Provider - Relying Party - User

User registers and authenticates with IdP; RP relies on the IdP for these assertions; user relies on the RP for essential services.

3 Metrics describe the Trust Framework:

IDP Perspective: Std Levels of Assurance were created for RPs to describe the degrees of identity and authentication that RPs can expect from IdPs.

RP perspective - Level of Protection: what will RPs do to protect any identity information that the IDPs provide to the RPs?

User perspective on the triangle: what privacy and Level of Control do I have as a user?

The 3 metrics operate independently. However, data can be tagged such that they affect one of the metrics or another.

After experience in trust frameworks focused on Authentication and technology, a legal framework and business framework was seen as a need.

OIX is a way for trust frameworks to publish how they operate in a neutral territory. The metadata registry that describes how the trust framework operates is published in a stable and durable location.

Think of ICAM as a procurement specification for Identity Services.

Assurance, Protection, and Control are soft concerns. LoA is machine readable expressions.

Trillions of identity operations are performed every day. Each interaction is governed by rights and duties; there aren't enough resources to enforce the rights and duties involved. This mandates the creation of a contract of sorts. Since each party has balancing duties, the relationship seems to be viable as a contract relationship.

- Some alternative to a monetization relationship is needed. A market to allow businesses to adopt trust frameworks that address specific needs is the ultimate outcome of the OIX effort.
- Can't solve all concerns at once.

The RESPECT Trust Framework introduces a Level of Control Metric that's user centered as opposed to IdP or RP-centered.

-- build incentives to do the right thing.

Principles:

Promise, Permission, Protection, Portability, and Proof

Data breaches about every 2 weeks over the last 2 years.

Promise: Respecting digital boundaries - this is a respect for the limits of the scope for anyone to act. "Your right to swing your arm end where my nose begins." (This is the fundamental principle of the trust framework.)

Permission: we don't steal or fool each other online.

Protection: maintain confidencies entrusted in us. First duty commitment to protect against 3<sup>rd</sup> party harm. (Commercially reasonable protections or legally reasonable?)

Portability: we don't hold each other hostage. Don't hold users to any one participant in the trust framework - share identity information.

Proof: Reasonably cooperate for the good of all members. Protect user and peer reputation. Scalable enforcement is by participation in a reputation system.

Trust anchors - people who will vouch for others reputation. Prevent Sybil Attacks. This could be based on Social Networks or other peer-to-peer systems.

Those who want to serve as Trust Anchors should contact Dean Landsman at IIW.

(All duties- no rights so far. Just as we all stop at red lights, participants in this trust framework operate with these principles. These principles don't respond to every problem, but solutions to common problems are consistent with these principles.)

## ***Identity 101 (T1G)***

URL: [http://iiw.idcommons.net/Identity\\_Community\\_101](http://iiw.idcommons.net/Identity_Community_101)

Convener: Kaliya

Notes-taker(s): Jim Epes

### **Tags for the session - technology discussed/ideas considered:**

Hybrid - Federation - Shibboleth - SAML - Terrena - InCommon - AuthN - AuthZ - Verification - Enrollment

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

We have gone from on-premise network centric to cloud based, or integrated between cloud and enterprise. How do you manage the employee on premise when he is also in the cloud.

One solution is to push the identities as a service into the cloud; another is to federate identities using SAML (maintained by OASIS) protocol accompanied by a legal agreement.

However, it does not scale very well since 1:1 for each link. So you could create a hub and spoke system with one ID verifier...this is what education in the U.S. does via In Common; also a Euro solution called Terrena for a master schema of education systems. In Common uses Shibboleth, which is an open source version of SAML.

Authentication (AuthN): act of proving that you are a previously seen entity or device in the system, for return login to system.

Authorization (AuthZ): Once you have logged into system, what you are permitted to do.

Verification & enrollment: Latter is how you get into the system - how you actually register into the system. Verification means the system formally accepts you at the time of id creation.

### **Protocols**

OpenID: Started as blogging protocol at LiveJournal; munged with LID and SXIP into OpenID, which were URL based. Then came 2.0 out of first IIW, which used XRI & i-name based IDs and used XRD (extensible resource descriptor).

A user could either self-register an Open ID account or use a third-party identity provider (OP) and then go to a resource site (relying party) and submit just username, which redirects them back to IdP and asks for password for user to enter credentials

to get the info that you are willing to share with RP to authenticate. The problem is that a malicious RP could redirect user to fake IdP and phish your account. The proprietary Facebook Connect works in a similar manner expect it releases a lot more info.

Identifiers vs. claims: The former uniquely defines who you are, while the latter makes assertions about your membership in a group or a particular attribute but without necessarily identifying you. The first effort to use claims based systems, Information Cards, failed, as will be discussed later.

The problem with identifiers is that they are always “phoning home” and reporting on you, which is not good in the online world and which gives IdP a great deal of power. So desire is to get to claims. IdP would merely assert something about you, like employer saying you’re an employee or govt saying you’re a citizen, and they would generate a claim token and this token would be stored in a digital wallet or ID selector that would store a bunch of cards under your control. You could choose to share them with RPs.

That’s where claims come in.....

Mentioned CardSpace and Info Card and that they failed since it was new SW UI and reluctance to support corporation that wanted to agg.





# ***Simple Cloud Identity Management - Overview and Use Cases (T1H)***

URL: [http://iiw.idcommons.net/Simple\\_Cloud\\_Identity\\_Management](http://iiw.idcommons.net/Simple_Cloud_Identity_Management)

Convener: Chuck Mortimer, Patrick Harding & Darran Rolls

Notes-taker(s): Darran Rolls

Tags for the session - technology discussed/ideas considered:

Simple Cloud Identity Management (SCIM)

Provisioning

LDAP

REST

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

Where can I find more information - charter, use cases etc?

- At <http://simplecloud.info>

What is the licensing & IP model?

- It's initially under the Open Web Foundation Contributor License V 1.0, but there has been some talk of moving it to IETF if the community so desires

Why is this activity not simply taking an explicit AuthN token approach - why move around identities at all?

- Lots of discussion on why accounts are needed outside of the IDP
- Not the same issue - this is explicitly for creating accounts based on direct specific requests and protocol flows

Where are we today?

- Draft core schema doc available for review - please comment
- Draft REST API bindings available for review - please comment
- Draft scenarios (use cases) available for review - please add/comment

What other schema initiatives did you look at?

- inetorgperson
- Portable Contacts
- 8 separate cloud providers
- SPML/DSML
- Eduperson

Will SCIM support OpenID and XRI identifiers

- Yes multiple identifiers are available

How could policy and controls to applied to the exchange?

- There's a space in the draft spec for that - yes you could use IGF

Based on the proposed charter (as read) the following points were made:

- This is federated identity with explicit account creation on the back-side
- There may be issues handling volume sync operation of the front channel
- Just In Time flows are key but the spec hopes to cover batch operations too
- Spec is specifically not addressing AuthZ
- Designed to meet needs for enterprise, consumer and mobile
- If possible make an incentive for implementers to stick to the core schema

# ***Government Regulation, Security Services and Bill of Rights (T11)***

URL: [http://iiw.idcommons.net/Gov't\\_Regulation\\_%26\\_Security\\_Services\\_%26\\_Bill\\_of\\_Rights](http://iiw.idcommons.net/Gov't_Regulation_%26_Security_Services_%26_Bill_of_Rights)

Convener: Carl Hewitt

Notes-taker(s): Carl Hewitt

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

Government Regulation, Security Services, Internet Bill of Rights

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

Smartphones are going to have it all: proprietary business strategies, chiseling on taxes and expenses, Roman Catholic confessions, political activities, abortions, personnel decision making, love trysts, STD, mental illness, and cancer diagnoses and treatments, etc. Stored in data centers this information will have to be tightly regulated with respect to how it can be used in marketing, personnel decisions, etc. Government officials will become increasingly knowledgeable about the treasure-trove of intimate personal information and proprietary business information stored in data centers.

Security officials will be forced to recognize the value of this information for preventing terrorism. Since it is politically necessary to do everything possible to prevent terrorism, means will be developed for security agencies to analyze all this information in real time. (The recent US government WikiLeaks subpoenas and National Security Letters to Twitter and other cloud aggregators such as Facebook have heightened awareness of the threat.) Thus we have reached an existential moment for the fate of our proprietary business and intimate personal information. The next generation will ask “Where were you when this was going down?”

A nation cannot allow its people to be able to be blackmailed or its companies' proprietary information to be taken by foreign security agencies. Before information on a person stored in a company's data centers can be turned over to a foreign government, the company will be required to first get permission from the person's country. (Penalty to be determined.) If necessary, a nation's intimate personal and company proprietary information will be required to be stored in data centers located in the same nation.

Industry is undertaking a major shift in cloud computing strategy to forestall the above threat to their international business. The alternative new cloud business model is:

- perform computation using customer equipment because

o it's less expensive than data center computation because of lower communications, energy, and equipment cost

o many-core architectures will provide plenty of computing capacity, even on smartphones

o response time can be faster than data center computation for new collaborative natural language interfaces (à la Kinect, etc.)

- store private information in data centers that can be decrypted only using the customers' private keys because it's cheaper and more reliable to use multiple data center storage vendors incorporated in different countries. (For efficiency, information will be cached on customer equipment.)

- service advertising using customer equipment because advertising can be better targeted on customer equipment (without violating customer private information) than data centers since customer equipment has complete information as opposed to the partial information of a data center vendor

- perform social computing using customer equipment because it can be more customizable and flexible when not restricted by vendor data centers (e.g. Facebook)

The new cloud business model supports and Internet Bill of Rights as follows:

- Information Disclosure. Clients have the right to receive accurate, timely, easily understood information in making informed decisions about their personal information (including that which could be used to help identify, contact or locate them) held by Internet information aggregators.
- Confidentiality of Information. Clients have the right to communicate with their aggregators in confidence and to have the confidentiality of their personal information protected. Clients also have the right to review and copy their own information and request amendments and deletions.
- Security of Information. Clients have the right to security of their information and to timely disclosure of security breaches. For example, they have the right to the means to reliably remove rootkits, viruses, spyware, and other malware from their own equipment.
- Participation in Advertising Decisions. Clients have the right to participate in the process of being offered advertisements based on their information. Clients who are unable to fully participate in the process of being offered advertisements have the right to be represented by parents, guardians, family members, or other conservators.
- Respect and Nondiscrimination. Clients have the right to considerate, respectful treatment from Internet information aggregators at all times and under all circumstances.
- Complaints and Appeals. Clients have the right to a fair and efficient process for resolving differences with their aggregators, and the institutions that serve them, including a rigorous system of internal review and an independent system of external review

## Session 2

### ***NSTIC, \$, IDPs, Telcos, Banks (T2A)***

URL: [http://iiw.idcommons.net/NSTIC, \\$, IDPs, TELCOS, DANKS](http://iiw.idcommons.net/NSTIC,_$_IDPs,_TELCOS,_DANKS)

Convener: Eric Sachs, Don Thibea

Notes-taker(s): Eric Sachs

Tags for the session - technology discussed/ideas considered:

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

Preso at

<https://docs.google.com/a/google.com/present/view?id=0AWRF6Ca-4HNnYWpraHA1aHBwM3R0XzkzY2ZtNG04ZGs&hl=en&authkey=CK244I0H>

which has been updated with notes from the session

## ***How to meet privacy goals of NSTIC (T2B)***

URL: [http://iiw.idcommons.net/How\\_to\\_meet\\_privacy\\_goals\\_of\\_NSTIC](http://iiw.idcommons.net/How_to_meet_privacy_goals_of_NSTIC)

Convener:

Note-Taker(s):

## ***Yahoo and Relying Party experience (T2C)***

URL: [http://iiw.idcommons.net/Yahoo!\\_As\\_a\\_relying\\_party](http://iiw.idcommons.net/Yahoo!_As_a_relying_party)

Convener: Mike Lee, Andy Wu, Yahoo

Notes-taker(s): Jim Epes

Tags for the session - technology discussed/ideas considered:

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

JIM EPES NOTES:

Last fall piloted on Flickr using OpenID only. To eval UX, engagement, new user acquisition.

Launched global support in q1 11 for OpenID, Google acct, Facebook Connect evaluating engagement performance and impacts from IDP permissions 00 performance, conversion...initial performance is positive; applying changes based on findings. Want to understand user age since some services are age specific. ...

Seeing considerable flow of new users. If I'm providing a service to someone who wants to comment on a blog post, rather than recruit entire new email account, that makes sense.

E2E Flow: Facebook with Hotmail ID...login with non Yahoo address...you want to comment on Yahoo chat but don't have account; today you take them to traditional Yahoo login page, or to sign in with FB or Google. FB renders the credentials pop up and presents what info to present. Some FB info is core to authn, other is asked for. When Yahoo asks for access to FB info it is binary - you either allow it all or deny it all. That's how FB works. The TOS for this is preset within FB but the Yahoo TOS is presented in the next step. This is a one-time event and is replicated the next time you log in. Just before you finish you pre-declare the FB info (name, email, etc.) that is being collected so the user can review. There is opt out for sharing updates from Yahoo to FB. A lot of people choose that.

The one-time admission of info transfer from FB to Yahoo is NOT subsequently editable in Yahoo at next time of OpenID login on Yahoo; you'd have to go into FB and edit permissions on that end.

Conversion performance: From Yahoo to logon page: 34% FB and 55% Google. Full logon completion is 73% each of prior logon visitors, for total completion rate of 25% FB and 41% Google.

IF the user has a Yahoo account, they suggest the user link the OpenID account and the Yahoo account. This creates a second account.

The result is that fewer people complete from logon page: just 46% FB and 30% Google, for lower overall completion to 16 and 17%. Thinks it may be confusing.

3<sup>rd</sup> party auth is what they use: a combo of Open ID and Connect.

Metrics: Andy Wu

56% of Goog signed in UU's access Flickr (then Sports, Frontpage, Answers, Groups)  
39% of FB signed in UU's access Flickr, followed by mail, front page, Sports, Answers, Groups

3PA Metrics: "Considerable" % of WW good registrations driven by 3PA. US Properties drive highest % of registrations. ("Good" = total reg-obvious abuse)

A Majority of all new user registrations for Flickr is driven by 3PA, and sizable referrals rates for Groups, Sports, Answers, Games.

Largest referrals to 3PA new user registrations referral comes from Flickr

Not seeing significant cost impact in terms of compromised accounts, customer support calls.

3PA engagement depends heavily on which Yahoo property you're looking at.

The non-mail services have 65% conversion for FB and 77% Google for getting to Yahoo login return from FB/Goog  
41% FB and 43% Goog on Front Page/My Yahoo  
22% FB and 17% Goog on Yahoo mail. Not surprising since these folks actually HAVE a Yahoo account so they might have just been checking this service out.l.

Completed conversion is 83/84% for non mail services  
So...Property is most critical driver for conversion and usage. Mail is NOT a driver.

Lessons: engagement call to action needs to be more prominent in the referring service

3<sup>rd</sup> party account creation engagement is on par with traditional Yahoo ID reg

Existing Yahoo users are not feeling compelled to use 3PA; confirms goal to reach new users.



KAREN P. LEWISON NOTES:

A high-level architecture designed to meet the privacy goals of NSTIC in the short term was outlined, including 3 use cases (see Power Point at <http://pomcor.com/documents/NSTICProtocolSteps.ppt> and a revised White Paper at <http://pomcor.com/whitepapers/NSTICWhitePaper.pdf> )

Points raised during the discussion period included:

--Identical privacy goals to NIST's were described by the OECD over 30 years ago, but not enforced.

--Also, in Europe, the concept of trust networks to ensure a chain of responsibility for user's data has been important in developing regulations.

--Some audience members from Europe were interested in the exact official formulation of NSTIC's privacy goals; they were directed to the official website at [http://](http://www.nist.gov/nstic/news.html)

[www.nist.gov/nstic/news.html](http://www.nist.gov/nstic/news.html)

--Other issues with the proposed architecture were the resultant increased costs (which would lead to cost redistribution to users), and decreased access speed.

--The proposed protocol is best seen as an enabling technology tool, to demonstrate to

policymakers a short-term implementation of most of the privacy goals of NSTIC.

--Question whether this is a possible building block to fit into OAuth 2.0, versus an OAuth killer? Answer is: likely neither.

--Audience members raised the issues of whether the UMA protocol, or a browser-based authentication app from the group at Newcastle University have already solved these problems.

--Another acknowledged objection was that this architecture requires extensions of the HTTP protocol to enhance the role of the browser in increasing privacy of double-redirection log-in protocols (possibly to be discussed later this month at the W3C Workshop on Identity in the Browser).

--As pointed out by Kim Cameron at the end of the discussion, if the RP and IdP collude, they could find out the identity of the user. On subsequent consideration, this

is not an issue in social log-in, but is a shortfall in other use cases. Hence, this is more of an interim short-term solution, outside of social log-in, and the definitive solution likely

lies in using anonymous credentials based on zero-knowledge proofs.

## ***Open ID ABC Identifier + Discovery (T2E)***

URL: [http://iiw.idcommons.net/Open ID ABC Identifier %26 Discovery](http://iiw.idcommons.net/Open_ID_ABC_Identifier_%26_Discovery)

Convener: John Bradley

Notes-taker(s): Nat Sakimura

Tags for the session - technology discussed/ideas considered:

Discovery, Identifier, openid

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

Title: OpenID ABC Identifiers and Discovery

Date&Time: May 3, 2011, 12:00

Session Number / Space Letter 2-E

Covener: John Bradley

Two types of Identifiers

\* Input Identifiers (User provided Identifier)

\* Canonical Identifiers

Input Identifiers

=====

Requirements:

- 1) User is likely to type in
- 2) Stability and Portability of the registration

Candidates

-----

\* URL

\*\* domains

\* Email/Acct

\* Phone Numbers

Canonical Identifiers

=====

Two competing proposals.

\* Single Principle Name

\* ProviderID / UserID pair 11

where ProviderID is scheme://authority:port/

UserID is path/url-safe-name

## ***Federated Identity for Non-Web Applicants (T2F)***

URL: [http://iiw.idcommons.net/Federated\\_Identity\\_for\\_non-web\\_apps](http://iiw.idcommons.net/Federated_Identity_for_non-web_apps)

Convener: Klaas Wierenga

Notes-taker(s): David Robinson

Tags for the session - technology discussed/ideas considered:

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

There were two separate topics under this same session title.

One discussion was around native applications running on mobile devices and how they interact with providers.

The other discussion was on the IETF Application Bridging for Federated Access Beyond web (ABFAB) technology.

Details:

Use Case To Start Discussion: Company A is a contractor to Company B. Identities are federated between the two companies. User from Company A performs an activity that requires Company B to contact Company C for data. How does this work?

The statement was made that "simple service chain is not solved by the federated identity solution". The military as worked for 7 years on this chaining problem and has not solved it. Federating identities across trust domains may not be the best solution. Instead, tokens should be considered as a way of solving this problem - something like bearer tokens.

The same use case was applied slightly differently for the next part of the discussion. Assume the use case is a person accessing pieces of their personal data from the government and a health provider - but they want to pull attributes from different places into a coherent picture. It was stated that current technologies assume browser redirection for this use case which doesn't work well with a native phone

application. The premise of this statement was a user is forced into a browser in order to solve the federated identity problem - they cannot stay in a mobile native application because the protocols assume browser redirection.

Further the problem was stated to be bigger than protocols that require redirection...that federation between downstream providers does not work effectively.

It was mentioned that personal data stores are an approach to solving the described problem and that UMA had solutions that addressed the use case described. Delivery of data can be via OAuth and there is no technical reason that browser redirection has to happen. It was suggested that the government of British Columbia had solved the use case being discussed using existing technologies. BC used tokens to restrict access/authorization and used signatures to prove where the data came from. It was mentioned that various services also have different API interfaces which makes downstream federation difficult.

It was mentioned, as an example, that Chrome makes the browser the operating system and addressed the "native application" concerns in some ways - and that in general, discussions about tighter integration between browsers, operating systems and hardware might address concerns with browser redirection (not necessarily chaining).

There was also discussion about what information each downstream provider has. Some have authentication information but they lack the meta data to effectively tie information together from downstream providers. Downstream providers may have more meta data...but since they are downstream and don't control the federation, the "tying" is left to the mobile application - which is not tenable.

Browser cookies may help provide useful information that ties these chains together...but it was stated this was not available in native mobile apps.

There was a brief side discussion on if users' actually like federated identities. One point of view was user's prefer to have their information with one or a small number of providers so they can understand under what conditions others can access their information. There was concern that with federation, undesired correlation can take place on a user's information.

The conversation completed shifted to IETF Application Bridging for Federated Access Beyond web technology (ABFAB).

With this architecture and set of technologies, it is possible for a university student at one university to use a non-web based application at another university. The idea is that universities can federate identities of students as well as authorization levels to control access to the applications.

ABFAB technology is based on the Extensible Authentication Protocol (EAP), with attribute assertions carried over SAML. It also uses GNU Generic Security Service Library (GSS) and RADIUS. See the IETF web site for more details.

It was stated that ABFAB combines the best of "both worlds". It uses a federation fabric based on RADIUS, authentication based on EAP, attribute assertion based on SAML and application integration based on GSS. It was stated that most Microsoft applications use the GSS API. SAML assertions are carried over RADIUS and EAP is used for user authentication.

"EAP is logically through the entire thing and goes end to end to itself".

The two organizations agree ahead of time on what attributes/authorization is available - and this is an NxN set up problem with partners, but one universities are willing to handle for now.

## **VRM Overview (T2G)**

URL: <http://iiw.idcommons.net/VRM + Browsers>

Convener: Doc Searls

Notes-taker(s):

Tags for the session - technology discussed/ideas considered:

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

(Disclosure: This was fast and deep. Notes are a little scattered.)

Tools that equip individuals to be better able to engage.  
Individuals bringing more to the table than they are allowed to now.

The Cookie created a subordinate / dominant relationship.  
We exist within their context  
Calf/Cow relationship - Animal Husbandry

VRM empowers Users to have their own context.  
Free customer is more valuable than a captive one.

Introduction to the R-Button.  
ListenLog data - Mashup with Kynetx.

How can we symbolize the user bringing context within the browser?  
What do we need to build worthy of permanent space in the chrome of the browser by the browser teams?

The user needs to be the point of aggregation of their own data, and the point at which things are done with that data.

Mike Hansen with Mozilla-

AwesomeBar HD - Search/Location in same bar, similar to Chrome.

[wsj.com/wtk](http://wsj.com/wtk)

[lsharedwhat.com](http://lsharedwhat.com)

[showmefirst.info](http://showmefirst.info)

Mozilla uses a Door Hanger with Disclosure process and a Consent step.  
example: site wants your location.

Visual Language - passive

web content can request access to a service.  
example: get profile method

reverse invocation.

User causes a message to be sent to the app/site, instead of a site always requesting the information.

A request to allow lying.

Mozilla sends the Do Not Track header, but does not yet require an ack response.  
Mozilla is considering sending terms of service with sent data.

Discussion of user flow for a Terms of Service mismatch. - Website cannot serve user because of inability to match ToS.

Disclosure should always require an explicit connect transaction.

Mozilla wants to be the transport in this user data transfer, not define the formats or standards for transfer.

Enabling this in the browser requires a protocol agreement between source and sink.

Access to data must be purpose bound.

UMA Authorization Manager right in the browser.

User agents have lost user agency.

Current UMA is in frame based, but can work well in a browser chrome based interface.

Tyler Close - Introducer - App asking for introduction to service.  
Dashboard to select between sources.

## ***VRM + Browsers (T2G)***

URL: [http://iiw.idcommons.net/VRM\\_%2B\\_Browsers](http://iiw.idcommons.net/VRM_%2B_Browsers)

Convener:

Note-Taker(s):



## ***The line between public and private Internet ID (T2H)***

URL: [http://iiw.idcommons.net/The\\_line\\_between\\_public\\_and\\_private\\_internet\\_ID](http://iiw.idcommons.net/The_line_between_public_and_private_internet_ID)

Convener:

Note-Taker(s):

## ***Users Managed Access (UMA) (T2I)***

URL: [http://iiw.idcommons.net/Users\\_in\\_control\\_of\\_their\\_data\\_UMA](http://iiw.idcommons.net/Users_in_control_of_their_data_UMA)

Convener: Eve, Maciek, Lukas

Notes-taker(s):

Tags for the session - technology discussed/ideas considered:

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

Introduction: reasons for user centric privacy management

Current situation: why UMA gives a better solution.

Digital identity management

Online social networking

Vendor relationship management

How to control your data

What is uma

A web protocol

UMA group

Introducing a new standardised solution

OAuth themes

Password anti-pattern

Access tokens

User managed access

Architecture and protocol

Uma players explanation: user, host, am, requested

Uma protocol steps

Trusting a token - OAuth workflow, host acting as a client

End points

Q: Who's reliable for the trust relationship?

A: You have to believe that host will use your AM

Two parties host and AM establish a relation.

Scenarios:

Alice to Alice sharing

Alice to Bob sharing

Alice to a company sharing

Mapping transactions and transparency of the protocol

Why avoidance of encryption is a design principle?

Trusting a token - establishing a trust relationship.

Requested application getting a token.

Accessing requested resource - token validation.

Smart AM - static layout

Defining available permissions by host.

Accessing a resource through requester

Issue of displaying permissions. Circles of trusts eg in small business companies. Vertical data. Low assurance for web.

Restful policy making

In the open web. Making sure to get users simply and quickly.

Market different shares for different AMs

Architectural challenge:

separating hosting the data from authorising the data.

Good feature of triggering the workflow by users themselves. If one user have access to e.g. particular folder he or she may also be interested in accessing also other resources and asking the owner of the data to grant them with access.

OAuth Leeloo and UMAj framework

## ***How many IDPs do we need? (T2P)***

URL: [http://iiw.idcommons.net/How\\_many\\_IDPs\\_do\\_we\\_need%3F](http://iiw.idcommons.net/How_many_IDPs_do_we_need%3F)

Convener:

Note-Taker(s):

## Session 3

### *Verified ID in the browser (T1A)*

URL: [http://iiw.idcommons.net/Verified\\_ID\\_in\\_the\\_browser](http://iiw.idcommons.net/Verified_ID_in_the_browser)

Convener:

Note-Taker(s):

## ***Secure Cloud Interlop Using JWT + OAUTH (T3B)***

URL: [http://iiw.idcommons.net/Secure\\_Cloud\\_Interlop\\_using\\_JWI\\_+\\_OAUTH](http://iiw.idcommons.net/Secure_Cloud_Interlop_using_JWI_+_OAUTH)

Convener: Eric Sachs, Jian

Notes-taker(s): Eric Sachs

Tags for the session - technology discussed/ideas considered:

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

The notes from this session are at:

<https://sites.google.com/site/oauthgoog/authenticate-google-app-engine-app>

## ***An architectural approach to harmonizing data between personal data stores (T3C)***

URL:

[http://iiw.idcommons.net/An\\_architectural\\_approach\\_to\\_harmonizing\\_data\\_between\\_personal\\_data\\_stores](http://iiw.idcommons.net/An_architectural_approach_to_harmonizing_data_between_personal_data_stores)

Convener:

Note-Taker(s):



## **Reputation Systems (Wuffie) (T3D)**

URL: [http://iiw.idcommons.net/Reputation\\_Systems\\_\(whuffie%3F\)](http://iiw.idcommons.net/Reputation_Systems_(whuffie%3F))

Convener: Ratha Grimes

Notes-taker(s): Mark Atwood

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

reputation, wuffie, currency, money, trust

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

What problem are you trying to solve?

example LinkedIn,

example eBay, transaction history

reputation is contextual

events lead to reputation

events have duration, number, size of transactions

what is appropriate cross information between reputation contexts

get the information you can control about yourself correct

there has to be some information about yourself you cant change to get this right

reputation is almost the inverse of personal information

Facebook Like is a reputation point for a web page

getting reputation right is how StackOverflow works

that reputation is now driving "Careers 2.0"

reputation is the future of media

reputation is needed for getting answers to questions

employers are now looking at stackoverflow and github reputation

an identity acquires a reputation

the story of Wuffie, from Doctorow's "Down and Out in the Magic Kingdom"

other books Daemon and Freedom(tm) by Daniel Swarez

reputation breaks down into 2 large catagories: skills reputation, trust reputation

OASIS project Open Reputation Manager seems defunct

we wont have good collaboration systems until we have open reputation systems

reputation is a factor of the size and timeline of a community

privacy is "what can be known" about you

reputation is "what is known" about you

klout & empire avenue are exmaples of social media reputation systems

can i see my score, can other people see your score, can i dispute my score

when do scores affect peer to peer interactions

gaming the system is a big big issue

anti-gaming efforts never stops

people dont like giving negative reviews

badges and leaderboards are very good at incenting people  
badges taht do not have a "game impact"  
gameification is a popular term  
book "Reality is Broken"  
designing systems that are good for people and good at incenting people  
Paul Reznik & School of Information at Michigan  
Slashdot reputation system has been analyzed  
Garcia Mendez at Stanford, math of incentive systems  
Wuffie means "reputation as currency"  
Quora uses "bounty system"  
Slashdot uses "meta moderation"  
has there been any research done on how satisfied people  
book "Web Reputation Systems" from O'Reilly  
book Dan Solve "Reputation"  
academic reputation: given, 3rd parties are granting it  
social reputation: commanded, you are trying to get badges  
much of the work is splitting down those two tracks  
negative interest, give it away,  
positive interest, hoard it,  
why are you creating a reputation? to generate influence to do something  
bitcoin as a distributed currency  
bitcoin trading has its own repuation systems  
would wuffie have to look like bitcoin  
is money reputation? can reputation beocme money? not really  
what is wuffie vs money?  
maybe money becomes reputation at certain level, such as founding a company  
trust is "will i be defrauded"  
reputation is "will you build a profitable business"  
reputation will drive what you can demand for salary

## ***OpenID Session Management (T3E)***

URL: [http://iiw.idcommons.net/Open\\_ID\\_ABC\\_session\\_management](http://iiw.idcommons.net/Open_ID_ABC_session_management)

Convener: Breno de Medeiros, John Bradley

Notes-taker(s): Mike Jones

Tags for the session - technology discussed/ideas considered:

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

Breno introduced the id\_token and went through session establishment procedure.

Id\_token:

- Is a JWT
- Identifies provider
- Identifies user
- Contains an audience restriction
- Has limited duration

In the AB/C spec, the id\_token is called “openid”. It is the identity assertion for OpenID AB/C.

Breno raised the question about whether the JWT should contain an authorization context.

George Fletcher questioned of whether having an authorization context is a good use of space.

John Bradley stated that we don't want to add every feature of SAML tokens to JWTs.

We discussed that we could define extensions to convey information about the user's login state.

George raised the question of whether the PAPE information should be in the token.

We discussed using the equivalent of a “checkid\_immediate that doesn't give you an access token” to extend the current session or revive an expired session. In either case, the authentication quality may have changed, so the id\_token may need to contain the PAPE state.

If the user signs out at the provider, within a few minutes the user should be signed out at the RPs.

Session management is different for the user agent flow.

Our security considerations will work to prevent leaking id\_tokens.

## ***PuSHee talk with Mitre team (T3F)***

URL: <http://iiw.idcommons.net/PUSHEE>

Convener: Justin Richer

Notes-taker(s): Monica Wilkinson

Tags for the session - technology discussed/ideas considered:

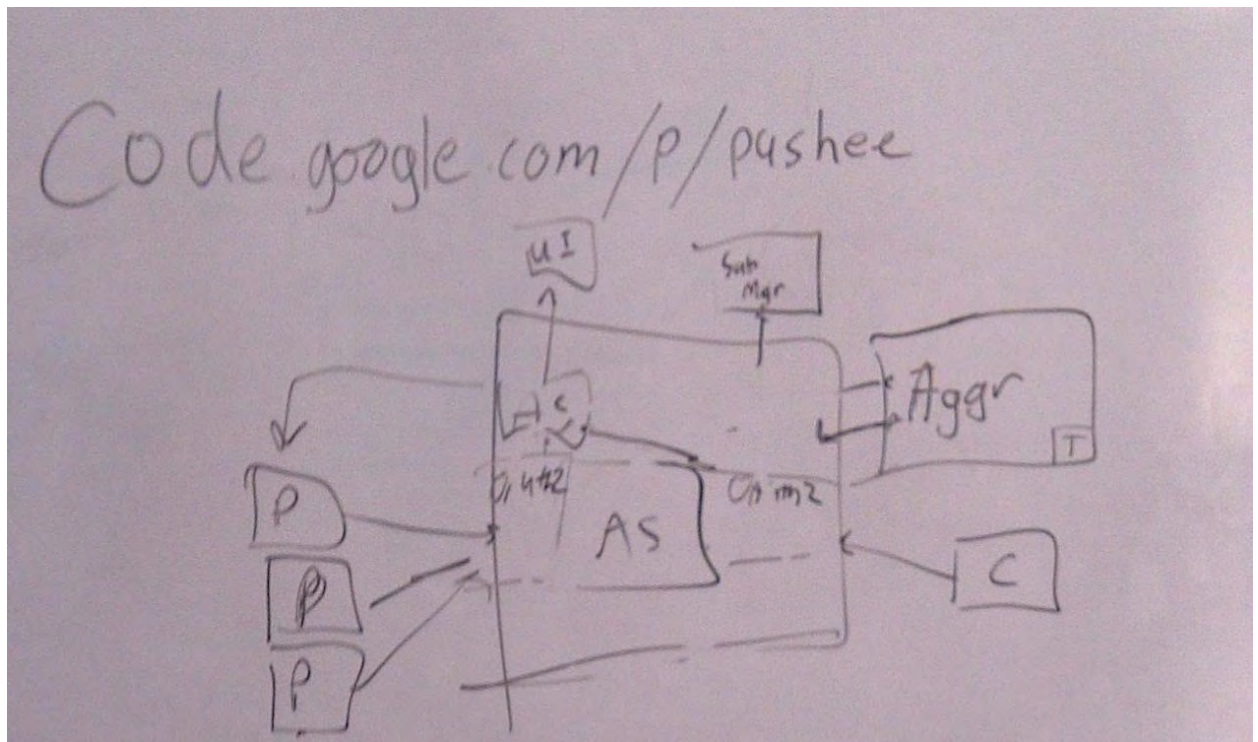
Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

Requirements: Providing calls to action for users in the enterprise based on a variety of business data sources

Methodology: PubSubHubbub and Activity Streams using OAuth 2.0

- Url: <http://code.google.com/p/pushee>.. Java Spring
- Not everyone likes Java in the room but Jason mentions that is a solid enterprise framework and they have added unit testing and monitoring components
- Jason described PubSubHubbub highlighting the PubSub aspects
  - PuSHee = Pubsubhubbub Hub with oAuth 2.0 for Pub and Sub
  - PUSHee Includes an authorization server with UI to manage keys/secrets
  - Subscription rules are managed via UI instead of independently for each resource
- Use case: PubSub for Medical. Justin asks to checkout the hdata project
- Use case is one generic notification engine which is surfaced on intranet
- Audience asked: What happens to late subscribers ?
  - One idea publishing to a topic and then have the topic support or not support late subscribers

- Justin mentions that he wants any publisher and client to be able to use PuSHee
- Clients needs to know url of resource, have a POST end point and support verification of the request via oAuth or JWT.
- One of the principles TOFU = Trust On First Use
- Open Source Project anyone can join includes aggregator
- Clients need to have a web server
- What about having multiple subscribers asks the audience
- The client in PuSHee is really the Activity Stream engine that users would subscribe to



## Can Banks be IDP Providers (T3G)

URL:

[http://iiw.idcommons.net/Can\\_Banks\\_act\\_as\\_digital\\_ID\\_providers%3F\\_Is\\_there\\_money\\_to\\_be\\_made%3F](http://iiw.idcommons.net/Can_Banks_act_as_digital_ID_providers%3F_Is_there_money_to_be_made%3F)

Convener: Peter Van Swift  
Notes-taker(s): Sid Sidner

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

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

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

SWIFT is wanting to issue certificates

USB cert token

Another project with an anonymous USB cert  
that can be used anywhere

Recent innovation contest winner: eMe was 2008

Couldn't get it funded

2011 visited digital ID providers

Started a digital ID innovation project - well funded

Research phase: how far should Swift go? Should Swift be a trust broker  
focusing on VRM

with a federated ID approach

The Digital ID Tuner: tunes across your identity, by both attribute and time

Use case: credit rating

Peter sees it as a sphere

David Segal "Pull"

belgian id system - one id for everything doesnt feel right

do consumers want this?

canadian banks tried it and failed

Pter this is not a consumer idea

What about telcos?

What about EMV?

Scott David but there is a problem with scaling up a system to Internet scale. How can we extend the Swift trust to a larger context.

if this is a new business for a bank or telco offers IDP, and then something goes wrong, what about brand damage.

Scott: pool the risk among many players

-----

new topic know your customer

NIST LOA 4 ( or maybe three)

Scott: you are already kyc on corporations, a non real entity. This is similar to vetting virtual identities.

kyc is not shared between banks

## ***Portable Contacts 2.0 (T3H)***

URL: [http://iiw.idcommons.net/Portable\\_Contacts\\_2.0](http://iiw.idcommons.net/Portable_Contacts_2.0)

Convener:

Note-Taker(s):



## ***Security Measures Open Identity Protocols (T3J)***

URL: [http://iiw.idcommons.net/Security\\_measures\\_identity\\_protocol\\_flows](http://iiw.idcommons.net/Security_measures_identity_protocol_flows)

Convener: Cordny Nederkoorn

Notes-taker(s): Cordmy Nederkoorn

Tags for the session - technology discussed/ideas considered:

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

This session started with the saying that the less we give in the cloud, the better.

Microsoft added that Office 365 is more user-centric in this, but still using Open Identity protocols like OpenID in enterprises is still a No Go.

The same is for Banks holding other data than banking, like health data.

What does the customer want? It's scary to see they still want to use username and password. Enterprises react to this with password-managers, but if these password-managers use all these passwords in 1 place, this is a No No.

Enterprises like AT&T think more about interoperability frameworks and with Microsoft they want to develop a standard way to link their info for the benefit of them and their customers.

To use information cards here is possible, but it spikes dramatically with every parameter added, which will scare customers and scare them away.

What about webservices? Concerning the legal liability, 2 of a 100 have a high liability, making it necessary to use a higher form of authentication here than username and password, contrary to the other 98.

To make webservices safer, a validation of the parameters can be done by using a token in a structural way to meet the customer's info, masking the real info, therefore securing it. Mapping here is still a difficult process, because of documentation and use.

IT&T proposes, next to the 3A's (Authentication, Authorization and Audit) a 4<sup>th</sup> one: Assurance. This is time-dependent, illustrated by ending a subscription where the expiry date is not the end of subscription-date, making it possible for a customer to get subscribed again for the same conditions.

Necessary here is the use of the same semantics and syntaxis between the parties involved, otherwise the dates can be mixed up.

This semantics also holds for error handling, which is a big hassle for support.

Just a few thoughts about keeping data secure in the cloud.

## Session 4

### *W3C Identity in the browser topic gathering session/Info Card (T4A)*

URL: [http://iiw.idcommons.net/W3C\\_Identity\\_in\\_the\\_browser\\_topic\\_gathering\\_session/Info\\_Card](http://iiw.idcommons.net/W3C_Identity_in_the_browser_topic_gathering_session/Info_Card)

Convener:

Note-Taker(s):

## ***New UMA Solutions for Scoped Access and Centralized AUTHZ (T4B)***

URL: [http://iiw.idcommons.net/New\\_UMA\\_solutions\\_for\\_scoped\\_access\\_and\\_centralized\\_AUTHZ](http://iiw.idcommons.net/New_UMA_solutions_for_scoped_access_and_centralized_AUTHZ)

Convener: Eve Maler, Maciej Machulak

Notes-taker(s): Eve Maler

Tags for the session - technology discussed/ideas considered:

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

. We shared and discussed the User-Managed Access (UMA) draft solution for loosely coupling an OAuth authorization server and resource server to solve for externalized authorization and interoperable scoped access.

UMA is:

- A web protocol that lets you control authorization of data sharing and service access made on your behalf
- A Work Group of the Kantara Initiative that is free for anyone to join and contribute to
- A set of draft specifications that is free for anyone to implement
- Undergoing multiple implementation efforts
- Being contributed to the IETF, in pieces (over the next few months)
- Striving to be simple, OAuth-based, identifier-agnostic, RESTful, modular, generative, and developed rapidly

UMA has three phases:

### 1. Protect a resource (NEW protection model)

- Alice introduces her Calendar host to CopMonkey: "When CopMonkey says whether to let someone in, do what he says" - and then tells CopMonkey her calendar access policies

### 2. Get authorization (NEW authorization model)

- Chase VISA tries to subscribe to Alice's travel calendar for fraud protection purposes; its client has to get authorization first, for which it may have to present claims to meet Alice's policy

### 3. Access a resource

- Chase now has an access token with the necessary scope to use at the Calendar host: “This means Alice thinks it’s okay”

The presented slides can be found at:

<http://www.xmlgrrl.com/publications/IIW12-UMA-ScopedAccess-May2011.pdf>

More information about UMA can be found at:

<http://kantarainitiative.org/confluence/display/uma/Home>

Questions that came up about UMA (the group is working on publishing a FAQ with the answers given during the session) were:

- How can the host be made responsible for incorrect or malicious behavior? In other words, how does host/AM trust work?
- Have there been any usability studies?
- Why externalize authorization?

## ***How to coordinate digital identity efforts between Europe and the U.S.? In collaboration with “SSEDIC” European Project (T4D)***

URL:

[http://iiw.idcommons.net/How\\_to\\_coordinate\\_digital\\_identity\\_efforts\\_between\\_Europe\\_and\\_the\\_U.S.%3F\\_In\\_collaboration\\_w/the\\_%E2%80%9CSSEDIC%E2%80%9D\\_European\\_project](http://iiw.idcommons.net/How_to_coordinate_digital_identity_efforts_between_Europe_and_the_U.S.%3F_In_collaboration_w/the_%E2%80%9CSSEDIC%E2%80%9D_European_project)

Convener: Christian Schunck

Note-Taker(s): Christian Schunck and Allen Friedman

Tags for the session - technology discussed/ideas considered:

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

Both the US, Canada and Europe undertake great efforts to create the infrastructure for a digital identity ecosystem.

SSEDIC is a think tank preparing an actionable roadmap towards a proposed Single European Digital Identity Community as envisaged by the Digital Agenda for Europe.

The SSEDIC network comprises 35 core partners and more than 60 associated partners from across Europe. US and Canadian organizations and businesses can join the network as Associated Partners.

How may the EU & the US play together? AND How do the EU member states itself play together?

SSEDIC: [www.ssedic.eu](http://www.ssedic.eu) 3 year project funded by the European Commission Coordinated by Nestor Lab (Italy) EU can't do it alone - international coordination is desired Starting point: what are the needs of sectors & citizens Confidentiality, Privacy, Ease of use/access Cross-border challenges...

EU - 450 million consumers, 27 member states Open if you use paper / post based processes Different states have different tech in built in ID No homogeneous regulatory framework except for e-signature Variations: regulations, liability, legal issues

Many eID uses in the EU are government driven, not user driven BUT - people only interact with their govt in official capacity 1.7 x / year

Who provides Many countries in Europe provide eID using a large variety of technologies. Government issued, ID card-based solutions exist for example in

Germany, Austria, Italy, Spain, Belgium etc. Other states use TAN based systems  
Access varies: citizen, resident, just ask for it

Role of “nationality” in government issued eIDs: just an “attribute”? Claim: if you need to be a citizen to obtain government issued eID, then nationality is moot.  
Distinction: Claim to be Irish for St. Patrick’s day bargain Claim to be Irish for Irish pension

Why not start federating now? There are pilot programs like Stork. But there exists difficulties like implementing LoA (QAA levels) without regulatory framework.  
Federation is going to solve the technical aspects, but the laws and policies need to be harmonized

In the EU exists regulation for e-signature exists (qualified electronic signature)  
Electronic models: Person (who is) vs. signature (what role) Some one has to validate  
Who can prove that person is X Birth certificate / record (local) Government ID (national)

Importance of contracts: French person can bind contract with an American w/out either govt  
What does the government demand? Standards (levels of assurance) What does this imply for digital identities and liabilities?

Claim: key challenges are legal & organizational Need accountability before you can have liability

## ***OpenID User Info Endpoint (T4E)***

URL: [http://iiw.idcommons.net/User\\_info\\_end\\_point\\_of\\_Open\\_ID\\_ABC](http://iiw.idcommons.net/User_info_end_point_of_Open_ID_ABC)

Convener: Nat Sakimura

Notes-taker(s): Mike Jones

Tags for the session - technology discussed/ideas considered:

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

Nat displayed the notes from the working group meeting at RSA containing notes on the UserInfo endpoint. Those notes were:

### UserInfo endpoint

Basically what registration widget would need

Facebook UserInfo

full\_name, first\_name, last\_name (no display name)

birthday

e-mail (verified)

gender

location - array of name and ID

link(s)

hometown

bio

work

sports

interested\_in

meeting\_for

significant\_other

religion                      political

timezone

locale

languages - array of id, location

website

update\_time

verified

Can also ask for

captcha



password  
Facebook phone number retrieval in a specialized scope  
Want

display\_name  
user\_id  
e-mail verification status  
locale  
image  
client\_id  
last\_auth\_time or issued\_at

David also has

profile\_url  
domain  
OpenID2

UserInfo provides a default set of claims

Other claims can be asked for

Use short names in JSON representation

High level goal to make RP registration easy

Can also agree on additional scopes (such as "address")

No\_pii scope?

Can disable default, ask for specific fields

Space delimited scope identifiers in OAuth2 scope parameter

OpenID scope

We discussed whether authentication context parameters should be scopes

first\_name#ja\_homi\_JP - can put in scope

We started down the road of discussing a general claims mechanism and agreed that that is a different discussion for a different session.

We debated how granular we want the information provided to be and permissioning issues.

Paul Madsen raised the question of whether all the claims must be sent.

We agreed that the permissioning and business models are out of scope for this session.

John Bradley asked whether the UserInfo endpoint should always contain the userid.

Phil Hunt asked what security context the request for the UserInfo data occurs in. In particular, does the IdP know to what RP the data is being released to? In general, the answer is "yes".

Justin Richter asked whether we can use Portable Contacts data structures.

Chuck Mortimore said that JanRain has mapped about 20 providers' user info data into PoCo data structures.

Breno made the point that the baseline needs to be simple and predictable.

The business goal is to provide an open equivalent to Facebook Connect.

We didn't get to actually discussing the specific claims list in the default set. We agreed that we need another session just to go over the set of claims in the default set.

Breno (in closing) - this is the absolute minimum set to minimally supply a majority of use cases

- Display Name
- Full Name
- Photo
- e-Mail Address
- Profile URL
- Data of Birth

It's the lightweight registration widget that we need to implement.

.

## ***JSON activity stream spec (T4F)***

URL: [http://iiw.idcommons.net/JSON\\_activity\\_streams\\_spec](http://iiw.idcommons.net/JSON_activity_streams_spec)

Convener:

Note-Taker(s):

## ***System Factors for Fourth Party User Agents (T4G)***

URL: [http://iiw.idcommons.net/Success\\_factors\\_for\\_fourth\\_parties/user\\_agents](http://iiw.idcommons.net/Success_factors_for_fourth_parties/user_agents)

**Convener:** Gam Dias

**Notes-taker(s):** Gam Dias

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

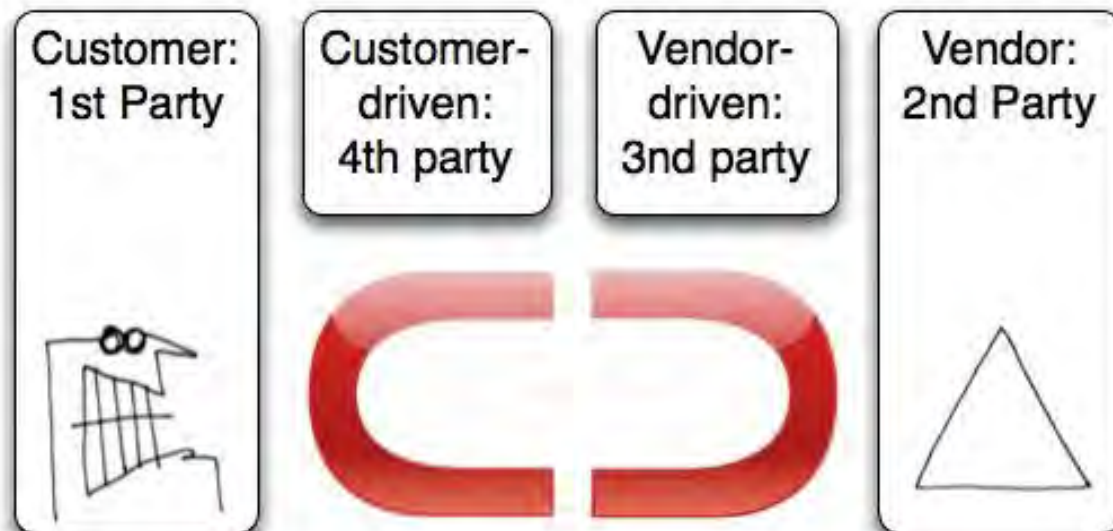
**Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:**

NOTE: the original meetings notes were in the form of a mind-map that is also included as part of this document. The text below represents a transcription a week after the event - so it may be somewhat enriched by additional thoughts that I had subsequently.

### **Defining the Fourth Party**

As an individual, I need a representative to whom I can submit my personal RFP to - with the knowledge that they will not only find what I am looking for with some degree of accuracy from the entire available market, but that they will represent me who is buying rather than a seller who may be paying them a commission on the sale.

The basic description can be found on the post on the VRM blog and was drawn up on the board by Drummond Reed:



In a Corporate Purchasing function, the 'agent' truly represents the buyer - in the manner defined above.

The agent or if there is technology involved, allows the buyer to specify a highly attributed RFP - essentially to make a very specific offer with tightly specified parameters. Not vital, but it makes for a more useful fourth party.

For the 2<sup>nd</sup> Party or Vendor, this provides a very highly qualified set of leads.

Somewhere, where these things come to pass, a new name was mooted for Fourth Party - 'User Agents'. Is this a term with different connotations and therefore different technical, legal and market implications?

### **What Makes a Fourth Party**

There were two proposals put forwards - a Legal obligation or a Technical Infrastructure

Do Fourth Parties have a fiduciary duty to the individuals that they represent? In Real Estate, there is a legal definition of the 'Buyers' Agent' and this is distinct from the 'Sellers' Agent'. (Definitions at [MortgageNewsDaily](#) and [Moving.com](#).)

### **Examples of Fourth Parties / User Agents**

The list of services suggested was as follows:

[Zaarly](#) - peer to peer request service (mobile)

[MyforBuy](#) - peer to peer request service

[Ebay Want It Now](#) - product requests

[Craigslist Wanted Ads](#) - straightup wanted ads

[Kynetx](#) - browser application platform

[Connect.me](#) - person to person connector

[Fancyhands](#) - concierge

[GetFriday](#) - concierge

*Urban Radar - I think this was a concept rather than an actual service because I couldn't find anything*

*Autoplanet - another one that I couldn't find*

[Microsoft Cars](#) - automotive portal

### **What is going to make a Fourth Party Successful**

#### **Contractual Infrastructure**

If 3<sup>rd</sup> and 4<sup>th</sup> parties are carefully defined and their obligations to the parties they represent and to each other - the relationship stands a better chance of succeeding because expectations can be set that define the actions.

## **Economics of the Transaction**

The economics of the transaction now has to be win-win-win-win. Only then will such a set of relationships succeed, sustain and grow.

## **Business Environment**

Parallels to the credit card network - of how adoption needed to work for both parties and then to hit critical mass.

A degree of buyer power or at least the desire from buyers to unite and regain some control in the process

## **Value Proposition**

How would it be implemented? Personal RFP, Social Search or Priority Messaging

Likely product categories:

Real Estate

Healthcare

Music

Banking

Telecoms

Insurance

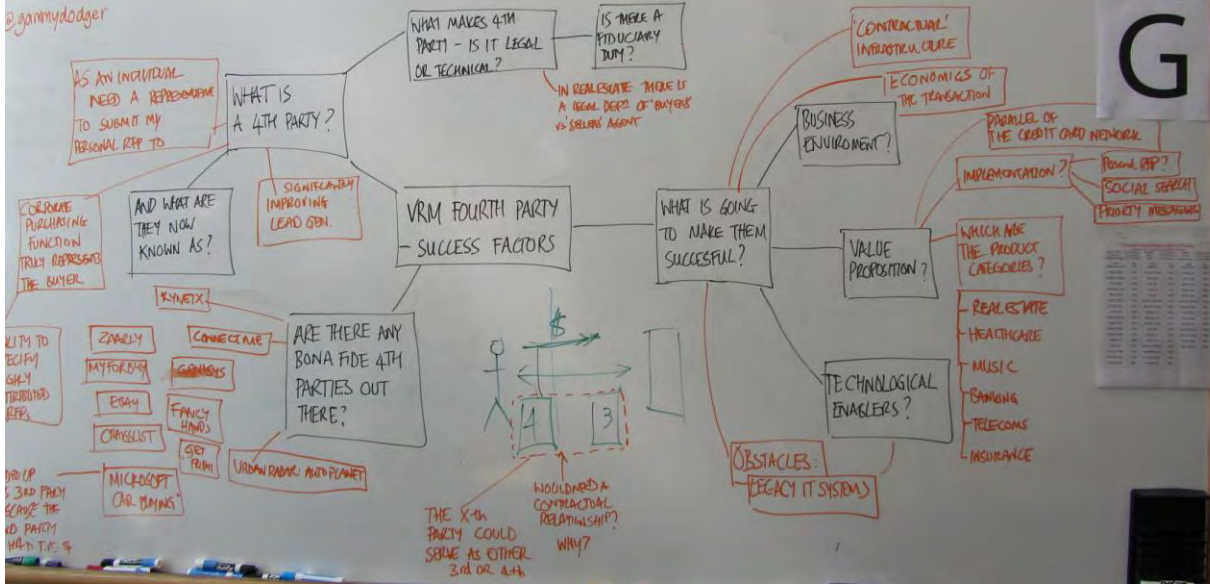
## **Technological Enablers**

Various elements of infrastructure are required to allow buyers to identify and define themselves, then to make a specification and then for those specifications to be presented at scale to potential sellers.

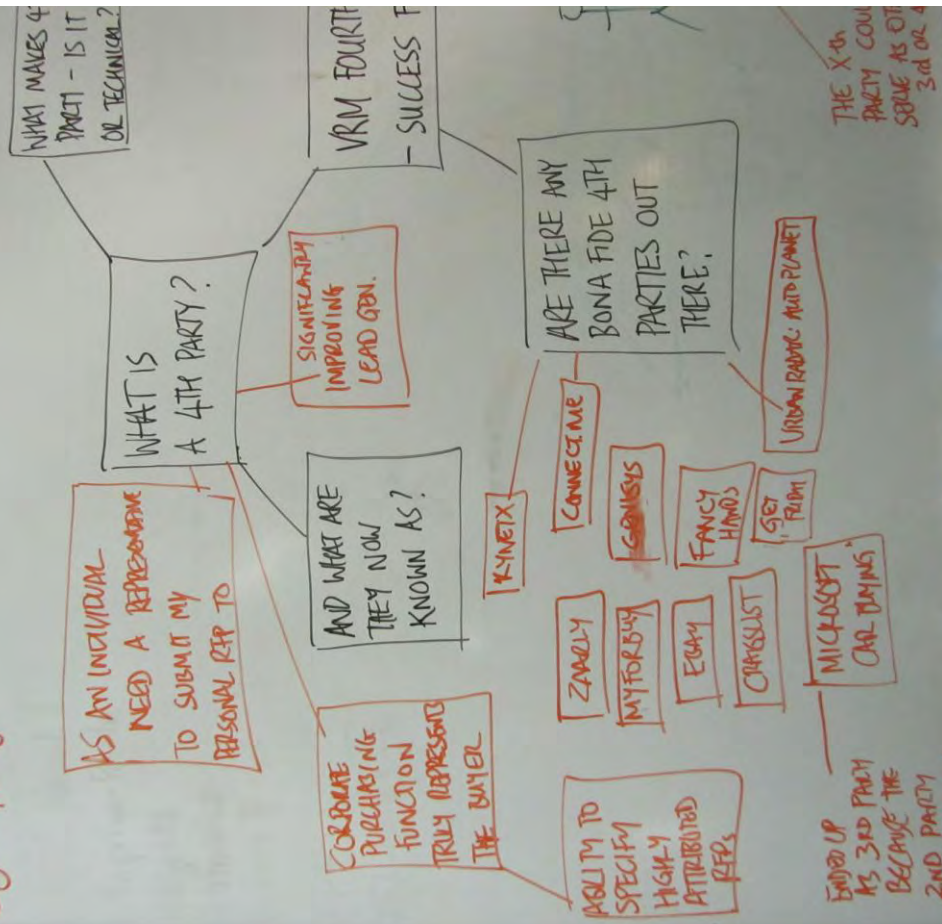
Sellers markets are as old as history and are well established (from the Bazaar to the Shopping Mall to the Aggregator Website). Buyers markets are more rare - confined to specific transaction types such as stock trading, commodities markets and currency speculation.

An obstacle to process in this space will be the legacy IT systems that many organizations rely on, providing a degree of inflexibility that will inhibit the effective operation a Fourth Party system.

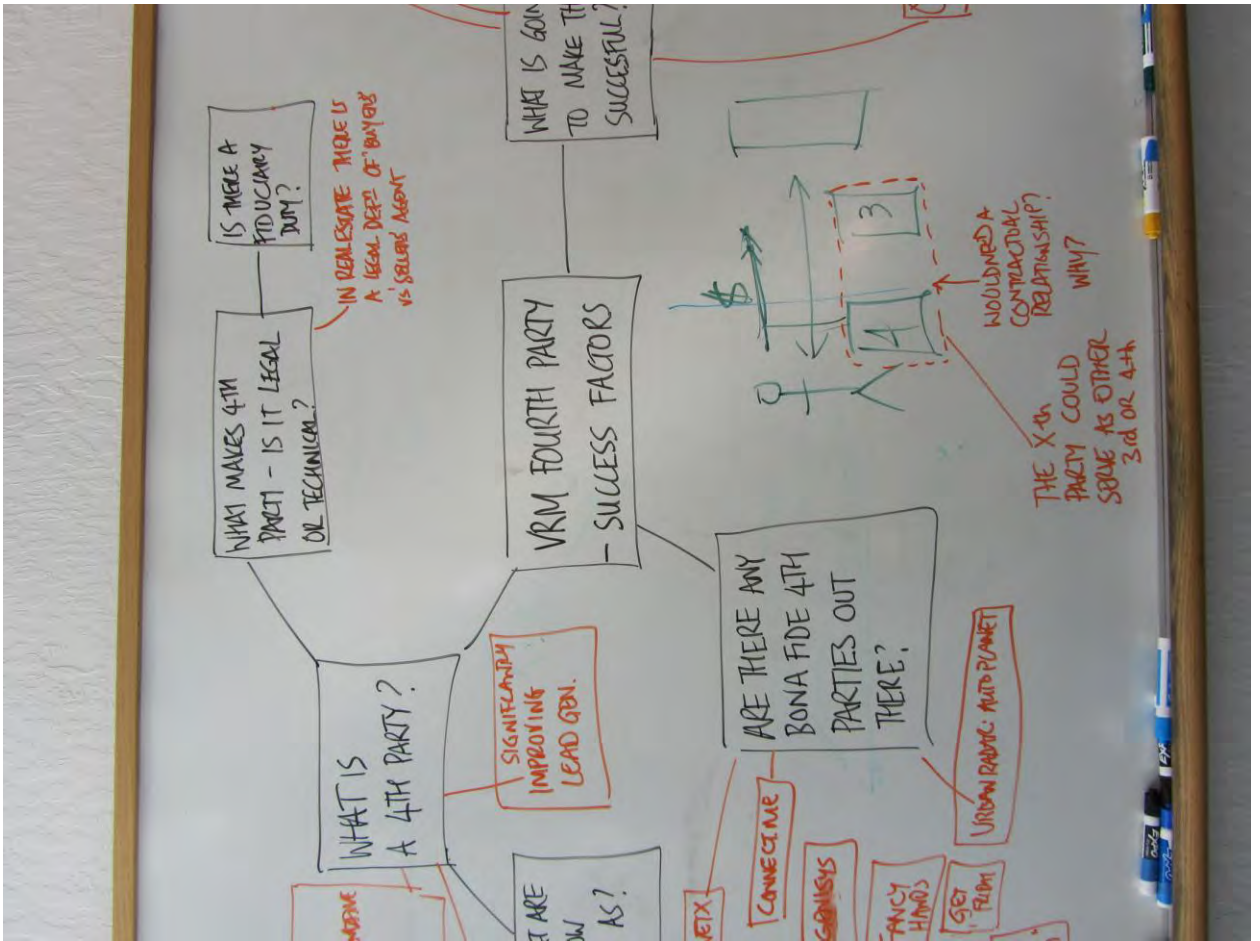
GAM DIAS  
Bjannydodger

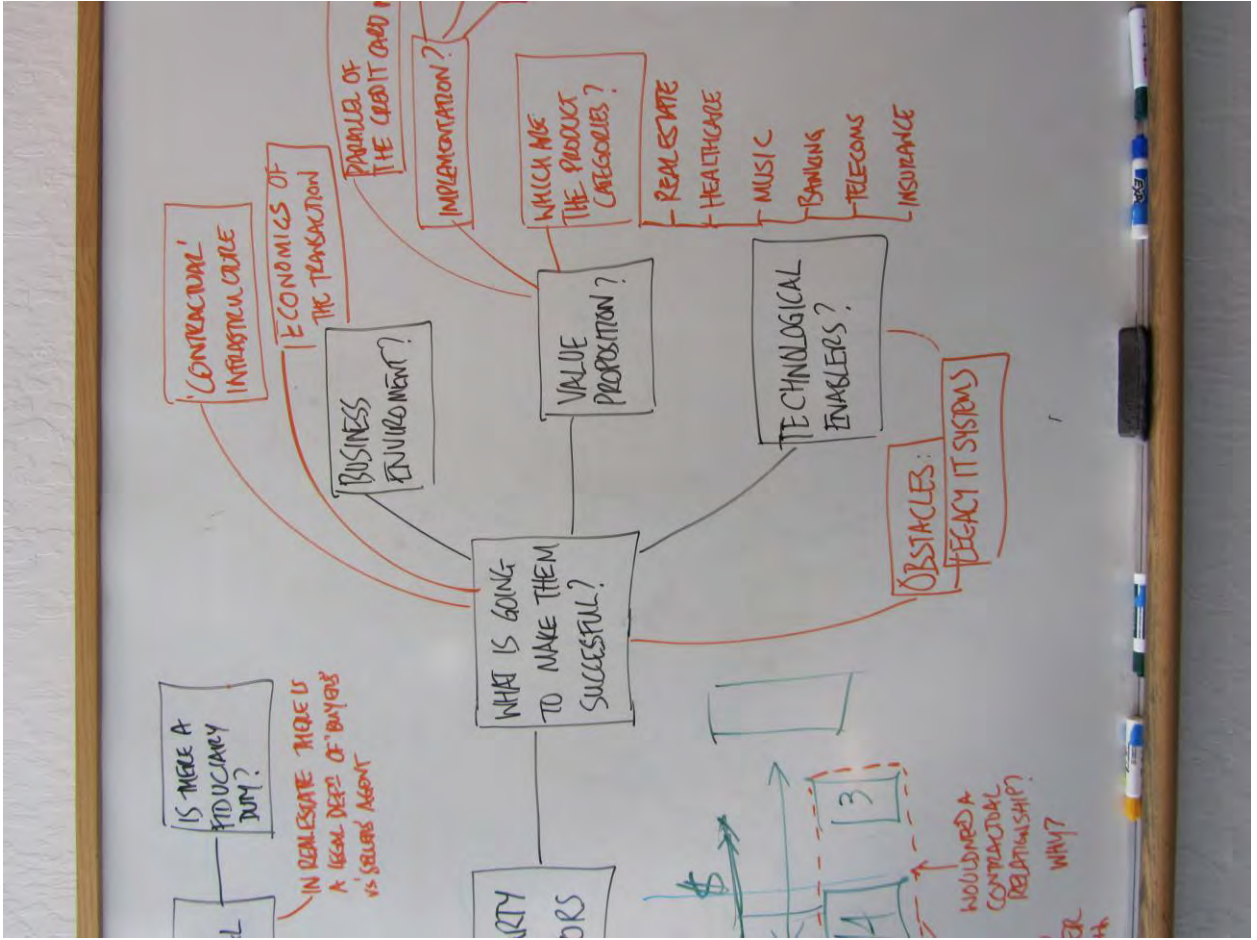


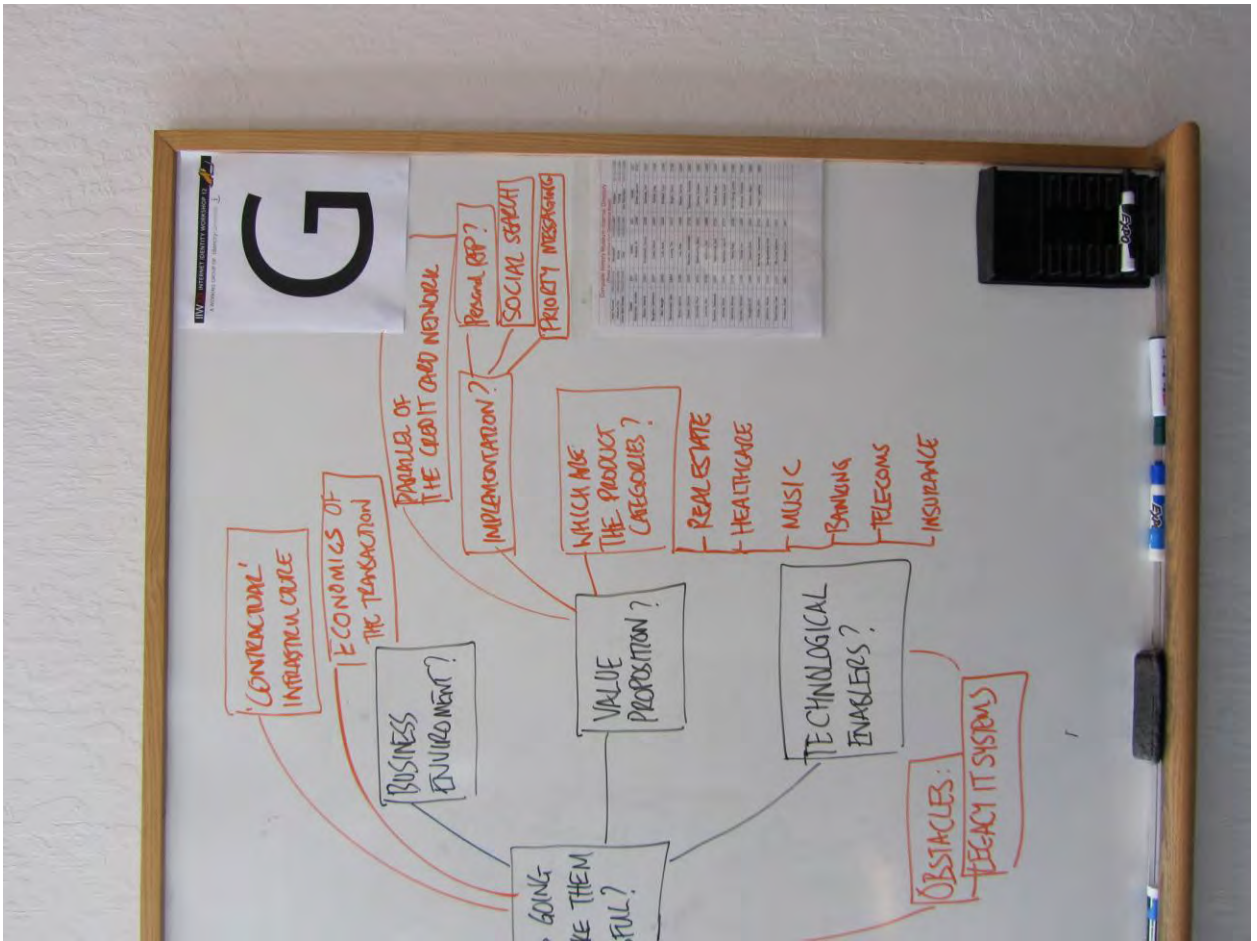
GAM DIAS  
@gammidodger











## ***When SaaS apps exchange data, what protocol should they use? OpenID, OAuth, SAML? What are the best practices? (T4H)***

URL:

[http://iiw.idcommons.net/When SAAS apps exchange customer data should they use OAUTH, Open ID, or other \(SAML\) protocols to access the data](http://iiw.idcommons.net/When_SAAS_apps_exchange_customer_data_should_they_use_OAUTH,_Open_ID,_or_other_(SAML)_protocols_to_access_the_data)

Convener: Jeff Collins

Notes-taker(s): Jeff Collins

Tags for the session - technology discussed/ideas considered:

OAuth  
Backplane  
OpenID  
IdP  
RP

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

- SaaS apps providers are exchanging data on behalf of customers at an increasing rate.
- Vendors like Salesforce.com, Google, Intuit, Microsoft, FreshBooks are creating ecosystems of apps
- For small businesses who buy a set of apps, how do they make sense of the identity problems among apps - where each app may have a different subset of employees registered
- What is the role of OAuth? It's the best way to use identity so that data is transferred safely with standard protocol.
- What is the identity of the unattended OAuth access token between the offerings? Could be a "user" in the source app, a "user" in the destination app, or a "robot account"? What is most appropriate - from a security perspective, and from an auditing example?
- When a 3<sup>rd</sup> party data integrator tool (Pervasive, Boomi, etc.) is used to transfer data between applications, what standards govern how the data integrator stores

credentials? What's a standard policy for how those tokens are granted and managed? Seems like OAuth can support most of the use cases.

- What about when SaaS apps have data integration technology between them with data flowing in both directions? There's a mutual sharing of OAuth tokens in the integration. Should we have a different standard for this kind of mutual authentication? Especially since from the user perspective, it may be important for them to turn off the open connection once and not from multiple points. For example
  - is there such a thing as an OAuth access token that represents authentication to more than one service at a time? Yes - maybe there is a need for something there.
- What kind of standard could work for this? Open question.

## ***Higgins 2: Open Source Personal Data Service (T4I)***

URL: [http://iiw.idcommons.net/Higgins\\_2:\\_Open\\_Source\\_personal\\_data\\_service](http://iiw.idcommons.net/Higgins_2:_Open_Source_personal_data_service)

Convener:

Note-Taker(s):

Notes in PPT hosted on Wiki.

***Bizzaro ID revenue from user purchased ID services (T4J)***

URL: [http://iiw.idcommons.net/Bizzaro\\_ID\\_revenue\\_from\\_user\\_purchased\\_ID\\_services](http://iiw.idcommons.net/Bizzaro_ID_revenue_from_user_purchased_ID_services)

Convener:

Note-Taker(s):

***Open ID 2.0, OAUTH 2.0, Open ID ABC Where are we going?  
(T4L)***

URL:

[http://iiw.idcommons.net/Open\\_ID\\_2.0,\\_OAUTH\\_2.0,\\_Open\\_ID\\_ABC\\_Where\\_are\\_we\\_going%3F](http://iiw.idcommons.net/Open_ID_2.0,_OAUTH_2.0,_Open_ID_ABC_Where_are_we_going%3F)

Convener:

Note-Taker(s):



## ***Do Not Track, It Won't Work (T4N)***

URL: [http://iiw.idcommons.net/Do\\_not\\_track!\\_It\\_won't\\_work!](http://iiw.idcommons.net/Do_not_track!_It_won't_work!)

Convener: Kaliya

Notes-taker(s): Mark Atwood

Tags for the session - technology discussed/ideas considered:

privacy, tracking, advertising

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

wont work, why?

David Forbes: a simple matter of practicality

cant think of a business model, where nobody can track  
the liability is too great

we cant control application providers in an ecosystem

we can't pay for these things without advertizing

if you removing advertising, there will not be the money to biuld things

if behaviorial tracking is 5% of advertising now, why not 0%

say you're a high quality content site, and doing internal tracking  
keeping track of behaviorial data, say i keep going to the health  
content.

q Kaliya, wants to know from the technology side why it wont work  
a companies will take it to the limit

a where is the limit, where do we stop logging

q what does Do Not Track mean?

in one session

over time, in the same website

q what will the default be?

differnece between in-browser, cookie whitelist, vs 3rd party do not track  
how does this relate to deep packet inspection?

self regulatory model, different advertising networks

legal model, with FTC dictation

do not call - most successful FTC action in history

85% of US household numbers opt'ed in their landlands

this is the inspiration for Do Not Track

but its very clear, its a phone number

on the web, its much more amorphous.  
mutliple devices, accounts, browsers  
world of warcraft?

what have we done that pissed off so many consumers?  
consumers are more aware  
enough people feel this is creepy that congress is aware of the issue

this is the business model that the net was built on?  
so what?

how can we make "do not share with 3rd parties" work for users?

The Personal Data Ecosystem, asked FTC for everything  
beccones, cookies, fingerprints, spyware - gone  
the data doesnt go outside the business  
the users gets access to their own data  
companies have to ask me for my data, instead of stalking me

how do we stop people from just going offshort  
bad actors could be put on google's malware list

users want visibility and correctiblity into their data trail  
good advertisers will want it to, because they get better data  
data lockers can anonymize the users  
advertisers ARE interesting in identity, for conversion tracking

what does "identity" mean, anyway?  
what is the impact of AdBlock

is is the problem "do not track" is trying to solve

the harm argument is the wrong argument  
but stalked women would disagree

its asserted that a completley transparent society is not good  
its good for the very privilaged, bad for everyone else

"I live in Tennessee, if my neighbors learn I'm Buddhist, nobody will talk to me".

## Session 5

### *What is the State of Personal Data Today? (T5A)*

URL: [http://iiw.idcommons.net/Personal\\_Data:\\_what's\\_the\\_state\\_of\\_things\\_today%3F](http://iiw.idcommons.net/Personal_Data:_what's_the_state_of_things_today%3F)

Convener: Mary Hodder

Notes-taker(s): Mary Hodder

Tags for the session - technology discussed/ideas considered:

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

The State:

- \* mostly controlled by companies
- \* inaccurate
- \* shallow or poor approximation
- \* undervalued / undermonitized
  
- \* higher education sorts of customers: students, professors, staff - biz practices ?
  - preserving work of scholars
  - piles of paper
  - science works has 1000 author papers now

Do we have something we can do about encrypted data being passed between say EX: yelp and facebook.. when they are passing our data and yet we don't have transparency into it

Do we have a right to know what is there?

WHAT WOULD WORK:

- \*future value - share potential
  - potential
  - market value.. quantified leads
  - predictive
  - intentions of people
- \* patterns
- \* symbols

WHAT DO WE NEED:

- \* more user research (usability)
- \* visualization methods for data
- \* metrics
- \* transparency
- \* tools, technology & law

- \* strategies on minimization of impact
- \* user control
- \* context management
- \* data sharing standards
- \* trust frameworks (lots of little ones)

#### USER PERSPECTIVES ON PERSONAL DATA ONLINE:

- \* irrational
- \* depressed
- \* in denial
- \* hopeless
- \* no where to hide
- \* angry "shoot the messenger"

#### STRATEGIES OF MINIMUM IMPACT:

- \* cookie canceling
- \* simple concrete, meaningful, visual
- \* common data leakage models - how much, from where, etc
- \* where is research
- statistical analysis == privacy
- combinatorial insights

#### NOT WORKING:

- \* scare tactics to make users more aware (privacy advocates do this)

## ***Getting rid of usernames & passwords - for real? (T5C)***

URL:

[http://iiw.idcommons.net/Getting\\_rid\\_of\\_usernames\\_%26\\_passwords\\_%E2%80%93\\_for\\_real%3F](http://iiw.idcommons.net/Getting_rid_of_usernames_%26_passwords_%E2%80%93_for_real%3F)

Convener:

Notes-Taker(s):

## **OAUTH 2.0 Device Profile (T5E)**

URL: [http://iiw.idcommons.net/OAUTH2\\_Device\\_Profile](http://iiw.idcommons.net/OAUTH2_Device_Profile)

Convener: Marius Scurtescu

Notes-taker(s): Andrew Wansley

Tags for the session - technology discussed/ideas considered:

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

What is the device profile?

- Similar to netflix pairing
- Device has a display, but no or a painful input
- Device gets a user code and device code
- Device says "go to URL and enter <user code>"
- User goes to browser, enters code at URL, sees a consent page, approves
- Device meanwhile polls AS, gets a code, refresh token

Use a QR code?

- Possible, but UX issues
- People may not have active sessions on their phone, so browser might be easier

Implementation issues

- Google ended up creating separate endpoints
- Devices poll today @FB/G, could just check once
- one URL/client\_id vs generic URL and globally unique codes
- 30m user code expiry time
- Session fixation attack theoretically possible, odd UX mitigates
- Client apps could use this flow

How is it modeled?

- grant\_type=device\_code

Mis-binding

- Devices could show the user id

Account sharing

- other ways of solving

Spec

- Probably refresh Recordon's spec

Code length

- 6-8, variable
- could use words

## ***Open XDI OX (T4F)***

URL: [http://iiw.idcommons.net/Open\\_XDI\\_OX](http://iiw.idcommons.net/Open_XDI_OX)

Convener:

Note-Taker(s):



## ***Data portability for trust framework (T5G)***

URL: [http://iiw.idcommons.net/Data\\_portability\\_for\\_trust\\_framework](http://iiw.idcommons.net/Data_portability_for_trust_framework)

Convener:

Note-Taker(s):

## ***Pros and Cons OAuth and Online Banking (T5H)***

URL: [http://iiw.idcommons.net/Open\\_Identity\\_protocols\\_and\\_banking](http://iiw.idcommons.net/Open_Identity_protocols_and_banking)

Convener: Cordny Nederkoorn

Notes-taker(s): Cordny Nederkoorn

Tags for the session - technology discussed/ideas considered:  
OAuth, Open Identity protocol, online banking security

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

A session for discussion Pros and Cons Use OAuth in online banking

Pros OAuth use in online banking

- Secure provisioning Api's used everywhere
- Scoped Access
- Reduce friction customer registration -> bank as IdP
- Online banking : SAML assertion can insert OAuth access token, resulting in less user interfaces

Cons use in online banking

- Compromised tokens by unauthorized use OAuth access tokens
- Issues usability for end-users
- Cutting edge means you do not know what we do not know
- Limited vendors
- Limited OAuth expertise
- Less defined security options (also encryption) in OAuth
- SAML provisioning is mandatory
- Possible phishing by using non-used OAuth tokens

Conclusion session:

We are going to use OAuth in online banking, but optimization is necessary to ensure a safe use.

## ***Portable Context (T5I)***

URL: [http://iiw.idcommons.net/Portable\\_contexts](http://iiw.idcommons.net/Portable_contexts)

Convener: Joe Andrieu

Notes-taker(s): Joe and Judi

Tags for the session - technology discussed/ideas considered:

Portable Context Search History

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

Site: [portablecontext.org](http://portablecontext.org)

Overview (video on site)

Looking for partnerships (community prototype)

Architecture (browser plug-in, html)

Possible uses: online retail, medical records, pharmaceutical, business intelligence/research

We have a video of this session (link to come)

## ***Ostatus (Federate the social web) (T5J)***

URL: [http://iiw.idcommons.net/Ostatus\\_\(Federate\\_the\\_social\\_web\)](http://iiw.idcommons.net/Ostatus_(Federate_the_social_web))

Convener:

Note-Taker(s):

Day 2 - Wednesday, May 4<sup>th</sup>

## Session 1

### ***Beyond the Nascar UI Google's Account Chooser (W1A)***

URL: [http://iiw.idcommons.net/Beyond\\_the NASCAR UI Google's Account Chooser](http://iiw.idcommons.net/Beyond_the_NASCAR_UI_Google's_Account_Chooser)

Convener: Andy, Eric

Notes-taker(s): Eric Sachs

Tags for the session - technology discussed/ideas considered:

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

Preso that was used

[https://docs.google.com/a/google.com/present/edit?id=0ASzF\\_8krG57FZGhyNHhqZHfMTM1Zjk5c2d0NjU&hl=en](https://docs.google.com/a/google.com/present/edit?id=0ASzF_8krG57FZGhyNHhqZHfMTM1Zjk5c2d0NjU&hl=en)

Still writing up notes

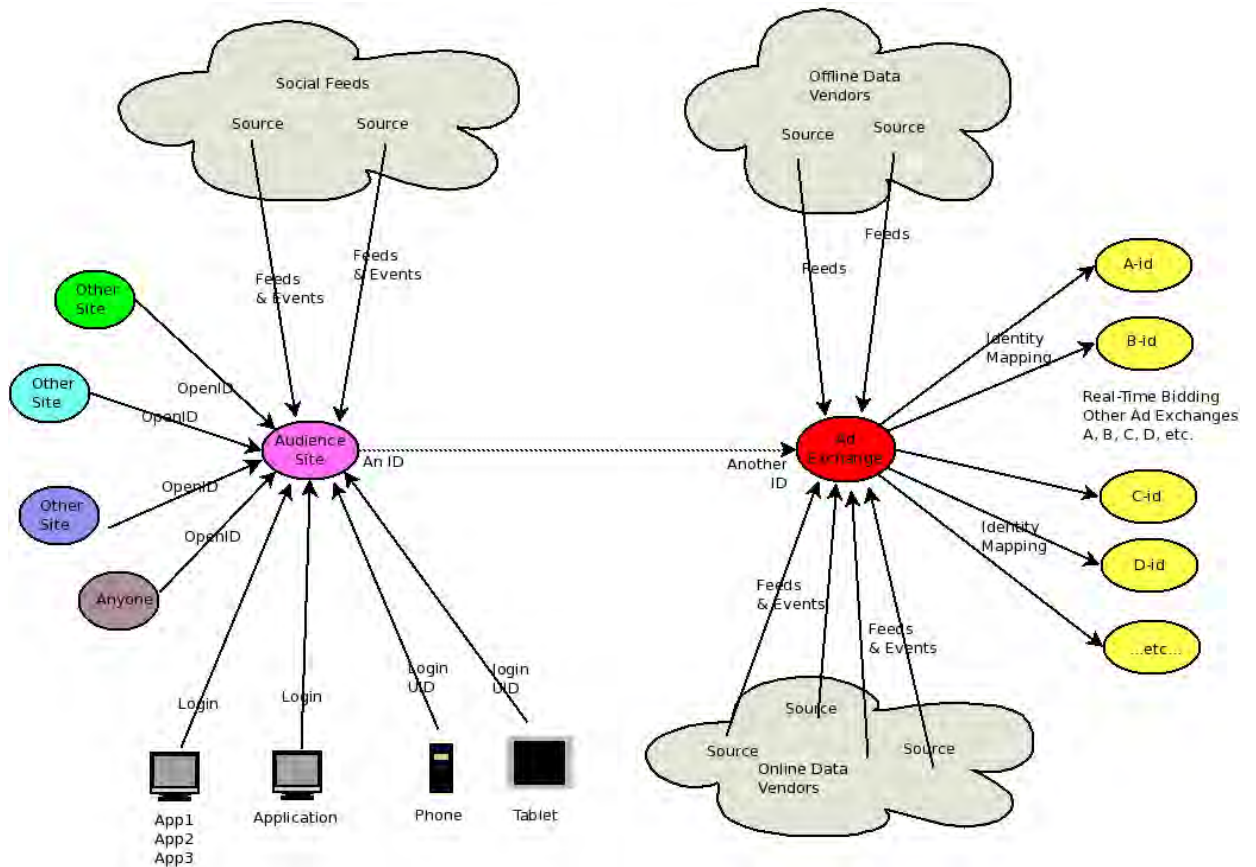
# Chained Identity in Online Entertainment (W1B)

URL: [http://iiw.idcommons.net/Chained\\_Identity\\_in\\_Online\\_Entertainment](http://iiw.idcommons.net/Chained_Identity_in_Online_Entertainment)

Convener: Wendell Baker

Notes-taker(s): Wendell Baker

Tags for the session - technology discussed/ideas considered:



## ***Information Sharing Agreement (W1D)***

URL: [http://iiw.idcommons.net/Info\\_Sharing\\_Agreement](http://iiw.idcommons.net/Info_Sharing_Agreement)

Convener: Joe Andrieu

Notes-taker(s): Joe Andrieu

Tags for the session - technology discussed/ideas considered:

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

Kantara, information sharing, VRM, personal data stores, UMA, ISWG (information sharing work group)

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

Key Concepts behind ISWG -

My Data, Your Data, Their Data, Everybody's Data

Customer Supplier Engagement Framework

Engagement Model

Trust Framework

Data Host, Data Recipient, Individual

Master Agreement & Data Transaction Agreements

Key Idea: before sharing information, establish a contract covering the use of that data

Quadumvirate used to describe key terms for information sharing

\* Recipient

- \* Scope
  - What Data
  - How do they get it
  - When do they get it
- \* Purpose
  - Specific value creating activity
  - Duration of use
- \* Response Channel
  - Authorized communications for output of purpose

Eg: Google Search

- \* Recipient : Google
- \* Scope
  - What Data : Search Keywords
  - How do they get it : Form data posted to URL
  - When do they get it : When form is submitted
- \* Purpose
  - Specific value creating activity : Recommend related websites
  - Duration of use : once
- \* Response Channel
  - Authorized communications for output of purpose : web page resulting from post

Eg: Google Alerts

- \* Recipient : Google
- \* Scope
  - What Data : Search Keywords
  - How do they get it : Form data posted to URL
  - When do they get it : When form is submitted
- \* Purpose



- Specific value creating activity : Recommend related websites
- Duration of use : ongoing (instant/daily/weekly)
- \* Response Channel
- Authorized communications for output of purpose : email

From these, we see two desirable categories of terms.

1. Terms that all sharing scenarios have in common.
2. Terms that distinguish different scenarios.

The Master Agreement covers #1. Data Transaction covers #2.

Master Agreement:

- \* Termination at will
- \* No redistribution without permission, except to third parties who have agreed to this agreement and to not correlate this data with data from other contexts.

Data Transaction Elements

- \* value added
- \* freely redistribute (permissions otherwise are part of master agreement)
- \* use data: once/session/ongoing
- \* read/write/update data: once/session/ongoing
- \* derivative with editorial approval
- \* consideration
- \* statistical aggregation (statically anonymous)
- \* Power of attorney/agency

First four patterns combining those elements

- \* Pattern 1: Personal RFP: pRFP, value added, read & use for

lifetime of pRFP, statistical aggregation, communications via service broker, statistical aggregation

\* Pattern 2: Transit Authority: geolocation data, read & use indefinitely, no value added, no communications channel, statistical aggregation

\* Pattern 3: Road Warrior Program: geolocation data, read & use indefinitely, value added, communications channel: device specific (GPS interface)

\* Pattern 4: Usage optimization: use data, read & use indefinitely, value added (advice), communications channel: notification (SMS, email), power of attorney

Added during session: need for element specifying data host location.

Work in progress. Participation invited.

<http://kantarinitiative.org/confluence/display/infosharing/Home>

## ***Virtual Problems (W1E)***

URL: [http://iiw.idcommons.net/Virtual\\_Problems](http://iiw.idcommons.net/Virtual_Problems)

Convener:

Note-Taker(s):

## ***SCIM Use Cases (W1F)***

URL: [http://iiw.idcommons.net/SCIM\\_Use\\_Cases](http://iiw.idcommons.net/SCIM_Use_Cases)

Convener:

Note-Taker(s):

## ***Different IDP Business Model (W1I)***

URL: [http://iiw.idcommons.net/Different\\_IDP\\_Business\\_Model](http://iiw.idcommons.net/Different_IDP_Business_Model)

Convener:

Note-Taker(s):

## Session 2

### *Packaging RP Best Practices Google Identity Toolkit (W2A)*

URL: [http://iiw.idcommons.net/Packaging RP Best Practices: Google Identity Toolkit](http://iiw.idcommons.net/Packaging_RP_Best_Practices:_Google_Identity_Toolkit)

Convener: Youlin, Evie

Notes-taker(s): Eric Sachs

Tags for the session - technology discussed/ideas considered:

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

Preso at

[https://docs.google.com/a/google.com/present/edit?id=d9dd5k9\\_28w47kk2d4&authkey=CKWxiewN](https://docs.google.com/a/google.com/present/edit?id=d9dd5k9_28w47kk2d4&authkey=CKWxiewN)

Raw discussion notes below

Red parts are not sure.

-----

- Any means for RP to not call google apis directly?

Yes, use js widget.

- What states are maintained by google in the GIT server?

GIT 1.0: no state. 1.5: store user account mappings etc.

- Target RPs are those with email users and not plain usernames?

yes

- what attributes are supported?

Depends on IDP, basically email/name/language/ etc.

- Does GIT server store IDP matrixes?

GIT 1.5: yes

- does GIT track user activities in its server?

Most IDPs do. End users don't see google log.

- does GIT support openid providers?

Only email providers. Hotmail is oauthwrap.

- Timeline for GIT release?

Plan is 2-3 months.

- Any integration for cms?

Yes, we already some work on Drupal.

- what is the server of GIT?

It is the same as google openid login server.

- will GIT 1.5 pass all attributes of non-email IDPs (like finance attributes)?

yes.

- If a google apps fires a user, and idp denies a user, RP should reject the user?

Yes

## ***Identity in the Browser: Open ID for Firefox (W2C)***

URL: [http://iiw.idcommons.net/Identity\\_in\\_the\\_Browser:\\_Open\\_ID\\_for\\_Firefox](http://iiw.idcommons.net/Identity_in_the_Browser:_Open_ID_for_Firefox)

Convener:

Note-Taker(s):



## **UMA SMART AM Demo (W2E)**

URL: [http://iiw.idcommons.net/Smart\\_User\\_Managed\\_Access\\_Demo](http://iiw.idcommons.net/Smart_User_Managed_Access_Demo)

Convener: Maciej M. ,Lukasz

Notes-taker(s): Maciej W.

Tags for the session - technology discussed/ideas considered:

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

1. Smart AM, Gallerify, Smart fetch explanation - which party does what and how.
2. Registering an album at Gallerify.me
3. Logging into Smart AM by means of ID provider - Facebook for the purpose of this use case.
4. Smart AM as a predefined AM - granting it access at Gallerify.
5. Explanation of providing sharing permissions to the AM from a Host application (Gallerify.me in this case).
6. Suggestion of introducing a new feature of Import/export permissions from/to another application.
7. Setting up sharing permissions.
8. Posting on the Facebook wall.
9. Accessing data by means of a requester application: [smartfetch.net](http://smartfetch.net) in this case.
10. OAuth flow - notification about the location of the data and allowing saring permissions.
11. Q: Accessing registered resources as a Smart AM non-user. Providing Smart AM only with a proof of identity (by means of Facebook in this case).
12. Revoking access and changin permissions. Accessing data only with an external application.
13. Denying access with host application (Gallerify.me in this case).
14. Redirection problem. Authorising Facebook to be and extension to be also an ID provider.
15. Facebook friends for the purpose of this use case.
16. Future features.
17. Q: Does Gallerify.me know the access request to the Smart AM?

## ***Public Policy around Identity (W2F)***

URL: [http://iiw.idcommons.net/Public\\_Policy\\_Issues\\_in\\_Identity](http://iiw.idcommons.net/Public_Policy_Issues_in_Identity)

Convener: Alan Friedman

Notes-taker(s): Kimberly White

Tags for the session - technology discussed/ideas considered:

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

What are the issues to be faced with NSTIC?

Govt. takeover/Corporate capture -Tension - protect consumer and citizen rights versus business model interests of very large international companies.

Govt. interest:consumer/citizen rights

Navigational globalized e-commerce

Privacy Principles - FIPS - decon value

Scale - proof of concept challenges

Model:

1. Contract
2. De facto
3. De jure - federal solution

All markets model -mechanism - liability - trust - some rules, sometimes written down for laws

Duties - contract or public law - market has combination of govt. law and contract

Market can drive single solution, not the best solution.

NSTIC = catalyst - best word -

Competition mentioned throughout NSTIC

Cases: Canadian health cards - massive fraud issue western most province of the country - authentication process within healthcare delivery system.

VA

PKI - failure case

SSO

Parallel efforts

Metrics

Four quadrant Snowden - Complex - Complicated, Chaos, Simple - (Complex to Complicated)

Eleanor Ostrum - Complicated solutions for complicated problems

Multiple solutions, multiple vectors - everything can function with problems.

Precedence - 1)metaphor/usability, 2)legal, established case law 3) major path  
dependence - once you get the ball rolling...  
Second question - let's go 4 years down the road  
What does that look like? Stable equilibrium -  
Liability  
Market incentives for evaluations  
Complexity is the enemy/entropy  
Future State - Secure, Scoped past techies,  
Data - ownership/property - off the session  
Next steps - take the use case - and explore what world states....

## ***How do we publish from our Personal Data Stores? Save the RESTful web! (W2G)***

URL:

[http://iiw.idcommons.net/How\\_do\\_we\\_publish\\_from\\_our\\_personal\\_data\\_stores%3F\\_Save\\_the\\_restful\\_web.](http://iiw.idcommons.net/How_do_we_publish_from_our_personal_data_stores%3F_Save_the_restful_web.)

Convener: Steve Williams

Notes-taker(s): Steve Williams & Scotty Logan

Tags for the session - technology discussed/ideas considered:

Personal Data Store, Privacy, Unhosted, REST

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

Audio and whiteboard snapshots: <http://sbw.org/iiwxii>

Videos Posted:

Part one (almost 9 mins):

<http://www.chachanga.com/nfb/c.php?c= 1304530699630>

Part two (about 21 mins):

<http://www.chachanga.com/nfb/c.php?c= 1304531262037>

Part three (another 21 mins):

<http://www.chachanga.com/nfb/c.php?c= 1304532591991>

The Personal Data Store is a positive development for user control and privacy. However, the common understanding of web application architecture is that application service providers will have authorized access to the Personal Data Store, so people still are not completely independent of application providers.

In the nascent application architecture @unhosted (<http://www.unhosted.org/>), the application provider serves Javascript to the person's web browser, and all access to the Personal Data Store is from that browser. That is, there is no need and no way for the application provider to know the identity of the person or the location of her Personal Data Store.

Steve believes the Unhosted architecture is a further step forward in user control and privacy, but he is concerned that Unhosted does not provide for publishing information from the Personal Data Store as RESTful, semantic web documents for

consumption by anonymous visitors, robots, and other agents that cannot feasibly run the application's Javascript and, in any case, have no way to obtain authorization to access the Personal Data Store.

Steve asked whether this issue is being discussed and asked the attendees for ideas on how such published documents can be created, when the authoring is done in an Unhosted application.

There were several good suggestions. Steve suggested (but is not completely comfortable with) the application provider serving code that would run on the person's server, under Caja or suchlike.

Phil Windley suggested that the publishing of the RESTful documents would be triggered by events raised by agents. We didn't pursue that idea adequately.

Scotty Logan suggested that the application would include Javascript that runs in the web browser to render the RESTful document and publish it to the person's designated web server.

Scotty also suggested that the application provider would provide Javascript to be stored in the Personal Data Store, and the Personal Data Store provider would provide an "admin console" that would run that Javascript to publish updates to the RESTful documents.

An attendee observed that the above ideas do not address use cases where passive events that should trigger updates of the RESTful documents, because no web browser is involved in such events. For example, when the person's location changes, her phone might push the new location to the Personal Data Store. That should update the map on the person's home page, but no web browser is involved in the update, so there's no opportunity for the application or the Personal Data Store admin console to get involved.

We did not solve that issue. Further discussion is needed.

## ***Trust, Identity, Commerce & Journalism (W2H)***

URL:

[http://iiw.idcommons.net/What's possible at intersection of trust, identity info, commerce and journalism](http://iiw.idcommons.net/What's_possible_at_intersection_of_trust,_identity_info,_commerce_and_journalism)

Convener: Bill Densmore

Notes-taker(s): Vanessa Miemis

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

- atomized content, curation, objectivity, bias, personalization, echo chamber

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

Can news organizations act as information valets? Can they curate the information you want?

What information would you give to a news organization?

- preferences, but not personal identifiers like location

3 different levels of willingness to participate in news

- willing to be involved in the story

- public insight model - willing to be an opt-in resource / subject matter expert in a story

- willing to share demographics, preferences about self in order to get more customized/curated content

do we care about / trust the news organization itself, or just individual journalists?

would we prefer to only receive content from journalists and content creators that we trust or are willing to listen to?

if we only receive content customized to our preferences, are we effectively putting ourselves in an echo chamber, reducing the chances for discovery, serendipity and insight?

do we want objective news, or do we want news that admits it comes from a certain perspective with a certain bias, so that we can judge for ourselves how to weigh the validity/truth of the content.

where do reputation currencies come into play when deciding where to direct our attention and dollars?

## Session 3

### ***NISTIC. (W3A)***

URL: <http://iiw.idcommons.net/NSTIC>.

Convener:

Note-Taker(s):



## ***Proxy Auth for Native App Hosts (W3B)***

URL: [http://iiw.idcommons.net/Proxy\\_Auth\\_for\\_Native\\_App\\_Hosts](http://iiw.idcommons.net/Proxy_Auth_for_Native_App_Hosts)

Convener: John Webb

Notes-taker(s): John Webb

Tags for the session - technology discussed/ideas considered:

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

# Main topic: Smartphones and other devices that have apps that utilize webservices currently require tedious authentication steps even when the user is already logged in elsewhere on the device (either in the OS shell or another app). How can we reduce the number of repeat authentication steps for these services? There is a much better user experience to be had, and possibly some savings in terms of development effort/risk.

# Three main options put out as starting point: - Third party cloud service that aggregates your services and proxies those requests for authentication/authorization - Platform level account manager which handles the auth exchange with the remote service and ensures user consent is handled properly (android model) - Switch to the native app for that device for that service and have it proxy the app-specific auth exchange (facebook on iOS model)

# Discussion:

- George described how AOL delivers long term tokens to the device with a shared secret - Google described the android account manager and how it has a plugin model that allows IDP's to support centralized auth in android - George has concerns that scope is provided by the client app via the account manager in native UI because it means that the plugin and the service need an API with fairly strong credentials that can control user consent -- risky - General concerns also about issuing a long lived token to an insecure device like a smartphone -- Counter-argument is that the long lived tokens can be revoked from the server side and also it may be even more secure in this model because specific client apps can use short lived tokens and re-request them transparently - Dirk described an additional security step whereby the OS can pass some metadata about the client app that requested authorization up through the account manager's conversation - extra assurance that the client app is who he says he is - Talked about the general notion of token exchange or token leverage whereby the user can get a token for a service based on having an existing token - Having a relying party alternative seems to be preferred in all cases, but agreement that we need to support this style as well - Dirk talked about how Android has some "blessed" apps which don't need to ask the user for consent, which is a

potential cause for server confusion. Their solution had something to do with having the client token returned with the consent screen, but I didn't catch the whole thing

Questions:

#1 - Is this mechanism of an account manager a viable model for all "native app hosts"? What about "web platforms?"

#2 - Is there some standard that needs to be developed around this mechanism of having an endpoint for twiddling consent bits?

## ***Respect Trust Framework 2 (W3C)***

URL: [http://iiw.idcommons.net/Respect\\_Trust\\_Framework\\_2](http://iiw.idcommons.net/Respect_Trust_Framework_2)

Convener:

Note-Taker(s):

## ***User-Managed Access Authorization Manager UX Study (W3E)***

URL: [http://iiw.idcommons.net/User\\_Managed\\_Access:\\_User\\_Interface](http://iiw.idcommons.net/User_Managed_Access:_User_Interface)

Convener: Maciej Wolniak, Lukasz Moren (Newcastle University)

Notes-taker(s): Maciej Machulak

Tags for the session - technology discussed/ideas considered:

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

Maciej presented the UX study on the UMA Authorization Manager. First, introduction on UMA, then description of the research study, the description of the 1st version of AM, then research results, then the new AM and conclusions.

Research study:

Learnability, efficiency, memorability, errors recovery, satisfaction  
- this are the usability factors that have been assessed.

34 participants

men and women, age 19-50

questionnaire-based: interviews and online form

sample task

participants' feedback

Study results:

users found the manager complex due to many steps in the process

- confusing colour scheme
- respondents reported the layout to be comprehensible
- they stated it could have been better
- major flaw, confusing headlines
  
- illogical layout - elements do not correspond with the steps of the task
- counter intuitive - drag boxes
- accordion module
- vague form fields
- lack of colours
- more help requested

Based on the initial research study, the following user-required improvements have been defined:

- more intuitive
- more logical
- more visual
- more colours
- more precise form fields

Then, the new Authorization Manager (SMART AM V2.0) is shown - the previously defined sample task is shown using the new UI - there's a small difference in comparison to the earlier task - resources are not registered at the AM but are registered from the Host application (e.g. user clicks the Share button).

Question: Was that the conscious choice to have all the information when defining a policy on a single screen?

Answer: Yes, this was to provide a user with a consistent and easy to use UI. At this point of time, there's only a minimum amount of information that can be managed at the AM. If we wanted to introduce additional features (e.g. calendar to specify that permissions are valid for a certain period of time) then we would probably for a wizard-like screen.

Comment: There's a necessity to evaluate the understanding of the Authorization Manager, not only the usability. The usability might be good but the understanding might be low (because UMA is quite a new model and may be confusing for the users).

Lessons learnt from the UX study:

- keep the UI simple
- emphasise key features
- show only necessary options
- indicate current stage in the cycle

When the user clicks on Share being at the Host then he knows the context of the actions he performs (i.e. in the previous SMART AM the user would register resources from the AM side and not from the Host side).

Newcastle University team plans to continue the work on the Authorization Manager:

- conducting another UX research
- include at least the same number of participants (preferably more)
- perform a new user evaluation study based on the new user interface
- apply the same questionnaire - try thinking aloud method or voice recording

There's a necessity for heuristic evaluation - small number of usability experts assessing the UI (3-4 people).

You can check out <http://www.smartam.net> and comment further.

It would be great to provide more integration points between the host and the AM..

## ***SCIM Core Schema (W3F)***

URL: [http://iiw.idcommons.net/SCIM\\_Core\\_Schema](http://iiw.idcommons.net/SCIM_Core_Schema)

Convener:

Note-Taker(s):

## Reputation System (W3G)

URL: [http://iiw.idcommons.net/Pseudo\\_Anonymity\\_and\\_Reputation\\_Systems](http://iiw.idcommons.net/Pseudo_Anonymity_and_Reputation_Systems)

Convener: Darius Dunlap  
Notes-taker(s): Gam Dias

Tags for the session - technology discussed/ideas considered:

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

### Definitions

Anonymous	Can't be traced
Known ID	Declared, True ID
Obscure ID	Anonymous but traceable
Pseudo-Anonymous	Verified (Authenticated) but not traceable

Pseudo Anonymous - where I want to use a service, but I don't want to necessarily be 'found'

Running a non-profit, we are interested in certain things (e.g. teenage pregnancy). As the non-profit, we want to use sites without revealing the person

For a Federated Reputation system to be able to Authenticate a person without actually identifying the user themselves

Can I visit a site and allow the organization know 'about me' rather than 'of me'

Users would include Organizations who also want to use a service, so organizations that are using services as would a person

Not trying to solve the security problems of the internet

Today ISPs are not allowed to sell the mapping of your IP address to NGOs

What do we do about reputation and how can we separate users different personas that use different sites

Another use scenario - I want to review a hotel.. and the reader wants to know that the reviewer is a person and not a shell

If that pseudonym has got positive reviews on their content, how



This has been discussed at IIWs in the past, when you talk about pseudonymity you need to discuss reputation:

1. I am not a robot
2. I am not a shill
3. I write good reviews

The application can have game attributes (gamification) that will ensure users value their reputation

Pseudonymity should be the default in all Authentication systems (Steve William SBW.org)

[Http://pseud.ony.ms](http://pseud.ony.ms)

In a federated and distributed system, a person can have 5 online personas

Facebook by nature aggregates multiple identities rather than maintaining a separation

Pseudonymity is very difficult to maintain in the real world - online because of the IP address, the ISPs can join these up

We have trained unsophisticated users to not manage separate online personas

EFF has a tool to identify users on a browser

How can we help users to manage their online identity better

Facebook is a good tool for training people to be non-anonymous

The natural most convenient action should have the good online identity management practice for the individual

Are you proposing a building block for helping to solve this?

Solving these problems starts with a good reputation system

As well as segmentation whatever system needs to integrate - so a family id or a company id

Is reputation portable? How can reputation information be transferred between communities

Although two people are acting via pseudonyms, they need to discover each other or not

Reputation as a movable 'currency' when is it transitive (not a fungible currency)

And NOT (so an individual can hide one aspect of their persona from another)

The currency should not be gameable

There should be a granular aspect to the reputation with all the permissions

If the reputation is faulty you should be able to change that

Marketingdouchebag on Twitter has a higher reputation and he maintains the reputation of that persona. He maintains this reputation more than he does the online persona

Even if all we did was to enable pseudonyms to be used in context e.g. Facebook, that would be a step forward

Most people treat their identity as one thing, on the internet, servers are managing

Facebook believe that if you are on facebook as you, you will behave better.

This is isomorphic to what the VRM community is saying a free customer is more valuable than a captive one

The right reputation system will make the internet a better place

Will it take a catastrophe (e.g. Playstation credit card occurrence)

If you want to transfer your reputation and have this follow across personas you end up tying them together

With Whuffie, it works like eCash

Although we are already here with Facebook the emergence of Agent technology will give us the

About 10 years ago, Rich (from data people) build this reputation management - like a roaming agreement for personas. The WTO has a set of global agreements for patents, this brokedown and has been replaced by the ACTA

In the same way each community can see a different view of a person's persona (google "Addapt")

There are practical communities (e.g. distinct private bittorrenting communities) are practicing this today

Drummond is working on a model like this for Connect.me

As I am listening to people talk about the login experience - they don't need to know who I am, they just need to know the IDP I am using

The missing piece is the reputation manager

How do they all link up?

What is the biggest most successful reputation on the internet right now? Google Page Rank for pages

Pseudonymity should be the default, it should be built upon a strong set of building blocks with the right granular permissions on access or usage.

We are not starting from scratch, where do we start from?

We can start from the ID systems - and people need to walk away from everything they currently have?

Anything that a IDP does for you adds value and creates stickiness for users

If you take the argument that 'privacy is dead' and allow the system to track us completely - it allows all acts to be trackable and gives fraud consequences. If one person steps outside of this (because people don't want to be tracked) - then that person cannot be tracked.

What we are training people today harms them, and we should really be stopping those behaviors. Can we build these in to richer experiences.

A system that prevents all evil means that there is no room for an offline experience. A system should be essentially empty for reputation and should be able to rebalance with more information.

## ***Beautiful Payments with OATH (W3I)***

URL: [http://iiw.idcommons.net/Beautiful\\_Payment\\_Systems\\_w/OAUTH](http://iiw.idcommons.net/Beautiful_Payment_Systems_w/OAUTH)

Convener: Tom Brown

Notes-taker(s): Tom Brown

Tags for the session - technology discussed/ideas considered:

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

In “Beautiful Trade: Rethinking E-Commerce Security,” Ed Bellis notes that the fundamental problem in the card-not-present case on the web is that cardholder data becomes a shared secret passed along many parties. Furthermore the incentives to protect the data do not align who with has control.

We discussed a simple OAUTH based protocol called OpenTransact. See <http://opentransact.org> for a simple spec and videos. Using this simple framework, we diagrammed one way payments could be handled across financial service providers (FSP). Also, it was shown that the asset class can be specified using Oauth scope when requesting a token.

Whiteboard snapshot: <http://www.flickr.com/photos/tbbrown/5688317438>

Sid mentioned previous work he had done:

<http://tootallsid.blogspot.com/2006/12/infocard-and-e-commerce.html>

Outstanding Questions: FSP discovery

## Session 4

### *UserAgent flow based on Windows Post Message (W4A)*

URL: [http://iiw.idcommons.net/OAUTH2\\_User\\_Agent\\_via\\_Window\\_Post\\_Message](http://iiw.idcommons.net/OAUTH2_User_Agent_via_Window_Post_Message)

Convener: Breno de Medeiros

Notes-taker(s): Breno de Medeiros

Tags for the session - technology discussed/ideas considered:

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

The section put forward the proposition that using javascript-bound transport mechanisms whenever possible (instead of network/HTTP) leads to an OAuth2 UserAgent profile that has better security, lower latency, and more powerful and flexible mechanisms to customize the user experience.

Participants generally agreed with the proposition to pursue javascript transport bindings for UserAgent in a speclet. (Revisiting OAuth2 core being the alternative option, which was not viewed positively.)

Specific feedback:

\* Backward compatibility:

- Define the javascript binding so that it can be requested in combination with a syntactically valid HTTP-binding so that the client does not need to have logic to special case providers that support the JS-binding; non-JS-binding aware providers will ignore the extension parameters they don't understand and process the request as before in traditional HTTP-binding for UserAgent.
- Define the JS-binding-aware provider behavior to be able to handle

the multiple request by preferring the postmessage variant.

- Have the JS libraries configured to handle either behavior automatically, with minimum configuration of an additional static servlet for providers that require a fixed pre-registered Uri, and very simple additional client side configuration to define the client.

\* Native app extension:

- Allow the redirect URIs to be any scheme that can be securely managed as a javascript origin.
- Extend the postmessage flow to native apps using custom URI schemes.

\* Provide open source javascript libraries and code samples for both server (provider) and client.

\* I was asked to provide a link to a forum for further discussion. I created a Google group where we can start this conversation until we have an umbrella WG in a receptive spec community.

<https://groups.google.com/forum/#!forum/oauth2-postmessage-profile>

***What's available for the shared user profile? Is Poco end all answer? (W4B)***

URL:

[http://iiw.idcommons.net/What's\\_available\\_for\\_the\\_shared\\_user\\_profile%3F\\_Is\\_Poco\\_end\\_all\\_answer%3F](http://iiw.idcommons.net/What's_available_for_the_shared_user_profile%3F_Is_Poco_end_all_answer%3F)

Convener:

Note-Taker(s):

## ***Adapting Levels of Assurance for NSTIC (W4C)***

URL: [http://iiw.idcommons.net/Adapting\\_Levels\\_of\\_Assurance\\_for\\_NSTIC](http://iiw.idcommons.net/Adapting_Levels_of_Assurance_for_NSTIC)

Convener: Jim Fenton, Bob Morgan

Notes-taker(s): Jim Fenton

Tags for the session - technology discussed/ideas considered:

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

Notes are located:

<http://www.employees.org/~fenton/NSTIC-LOA.pdf>



# Building a Trust Framework for Multiside Markets (W4D)

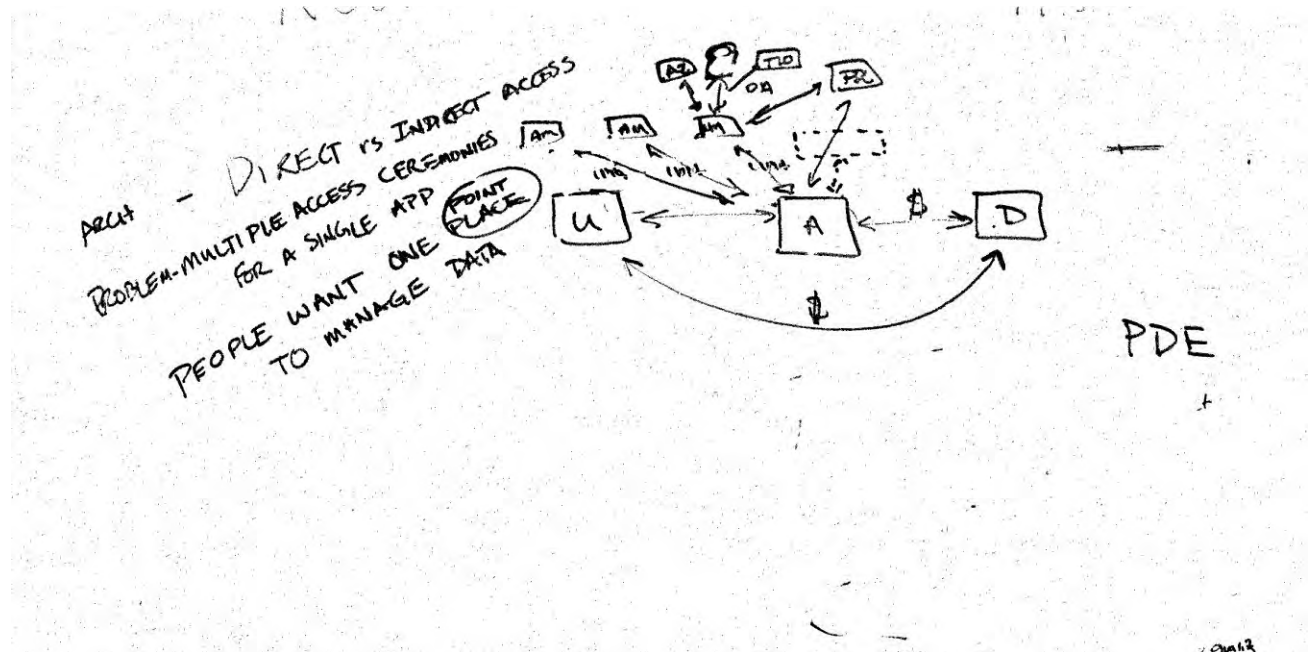
URL: [http://iiw.idcommons.net/Building\\_a\\_Trust\\_Framework\\_for\\_Multi-side\\_Markets](http://iiw.idcommons.net/Building_a_Trust_Framework_for_Multi-side_Markets)

Convener: Phil Windley

Notes-taker(s): Photo Phil Windley

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

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



## ***VRM and CRM (W4E)***

URL: <http://iiw.idcommons.net/VRM + CRM>

Convener:

Note-Taker(s):

## ***SCIM Bindings (W4F)***

URL: [http://iiw.idcommons.net/SCIM\\_Bindings](http://iiw.idcommons.net/SCIM_Bindings)

Convener:

Note-Taker(s):

## ***Two Legs Good? “Client-Server” OAUTH Usage (W4G)***

URL: [http://iiw.idcommons.net/Two\\_Legs\\_Good%3F\\_“Client-Server”\\_OAUTH\\_Usage](http://iiw.idcommons.net/Two_Legs_Good%3F_“Client-Server”_OAUTH_Usage)

Convener: Eve Maler

Notes-taker(s): Mark Atwood, Eve Maler

Tags for the session - technology discussed/ideas considered:

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

It is noticed that OAuth is being used for internal services. It's not being talked about much publicly. What are the good/best/bad practices for doing it?

What is the terminology? "2-legged" vs "client/server"? Though most people detest "2-legged" and "3-legged", they also understand what it means.

2L is being used to replace sending dev API keys across the wire with every request. You can use the signing mechanisms in OAuth 1, or with OAuth 2 you can use the client credentials flow. When using the client credentials flow, using refresh tokens doesn't make sense (SalesForce explicitly disallows it). Usually an access token is considered to be the length of a "session", but this doesn't have meaning in the 2L context. What does "expiration" really mean in 2L flows? In Justin's implementation, the client is brain-dead; it just keeps trying until it gets a 200 OK. We don't want people to think of "cookies".

There are use cases where apps want to do both SAML and OAuth into a service. This still has a user in the mix, but it's still an implicit grant. A 2L authorization grant is implicit in a deeper way; the client represents itself.

(OAuth 1 forced you into a long grant in order to get anything done. Refresh tokens in

OAuth 2 are only good for getting access tokens, so they're safer.)

Torsten has a token revocation draft that lets you submit the token and say "cancel this", but it doesn't have things quite right yet. Salesforce and others are planning to use this revocation model.

There are enterprise customers for whom the term "OpenID" and "OAuth" are negative statements; the words must be avoided. But one customer has a REST API protected by OAuth 1.0a. In that case, they use admin-configured tokens. A defect tracking system needs to be registered across the system against code changes. For a test org and a dev org that are in different identity domains inside an enterprise, they had to tinker with OAuth 1.0a to include user ID and group info.

Removing query string tokens from OAuth 2.0 breaks shipping a signed URL.

Info security control is a mirage. People WILL use Gmail, Dropbox, and Evernote to get their work done. When IT becomes non-innovative because it is the one monitoring, the business units will become innovative because they have to get work done.

Internal use of OAuth is useful for reducing dependency on a central authorization server.

A few Salesforce customers ask for 2L flows in the context of federating for web operations. The user at the customer site has gone through a SAML service, and SSOs into Salesforce. Or, TripIt or Concur wants to connect an app to SFDC's social network, to post someone's flight schedule to people in your network. For Concur itself to tell Chuck that his flight schedule has been updated, the message is literally coming from Concur, so 2L could be used for that. That flow can be preconfigured to have certain permissions. The SAML token would contain the subject.

Google Apps Marketplace has an admin doing the scoped grant at install time, rather than having the user do this at one-time.

One company had a blog service and a picture-storing service that used the OAuth flow. This was in the context of users, but they didn't want the authorization screen to come up between these two services because they were run by the same company. Salesforce has the same thing: If a user tries to connect with an OAuth client that was defined inside the same tenant (company) in the system, the implicit flow is used.

MITRE has a social networking site called Handshake, outside its firewall, along with recommendation services etc.. The service can be used by both MITRE and external people. It's based on a collaborative tool called Elgg. Different data sources contribute to it. For people on the outside, a user agent using the recommendation engine can easily get access to stuff stored outside. The internal recommendation engine shouldn't need to know much about users. So the internal recommendation engine and the external Handshake platform have something like 2L OAuth, and all user-specific authorization decisions are being made by Handshake. Handshake is generating a signed ID, and the internal recommendation engine just has to validate the key and secret. This uses OAuth 1.0 2L, signing the full URL, with no token.

Now that OAuth 2 forces everything to be in authorization headers, they can't use the MAC token profile. This will prevent OAuth 2 from being used widely for this purpose. But they will be switching to client credentials and short-lived tokens for some other use cases.

Net-puncturing in general is done with a trick like Alan Karp used for his "SCOOPS" demo. InfoSec wants control, and when they put up controls, people work around them. It's so much easier to set up services than to even know how to get permission for them. At one company they're allowed to blog and tweet, but they have to go through social media training, and at the risk of being terminated (everything is being monitored), they comply. Alan: "There is another way not to get fired, which is to get

your job done." :-)

Before OAuth, client apps just used a username and password, which is ideally different for each client app but often not.

Some companies have so many loosely coupled apps internally that 2L OAuth is used as a cleaner alternative than a centralized authorization server. It takes away a dependency on a centralized server, so it can't bring your apps down.

Another benefit of OAuth is the constrained delegation: read-only vs. read/write tokens, for example.

AOL has also used OAuth instead of IP ACLs. If only certain sites are supposed to access a certain API, it's nice and clean. It's also good for signing URLs that have redirects in them, to constrain the system from doing open redirects.

## ***Extended Demo: UI for personal data store + data sharing on mobile device cubicon (W4I)***

URL:

[http://iiw.idcommons.net/Extended\\_Demo:\\_UI\\_for\\_personal\\_data\\_store\\_data\\_sharing\\_on\\_mobile\\_device\\_cubicon](http://iiw.idcommons.net/Extended_Demo:_UI_for_personal_data_store_data_sharing_on_mobile_device_cubicon)

Convener:

Note-Taker(s):



## Session 5

### *Backplane Spec (W5A)*

URL: [http://iiw.idcommons.net/Backplane\\_Spec](http://iiw.idcommons.net/Backplane_Spec)

Convener:

Note-Taker(s):

## ***Oauth and OpenID on mobile native UIs. How should it work? (W5B)***

URL: <http://iiw.idcommons.net/OAUTH, Open ID Mobile UX: How should it work%3F>

Convener: George Fletcher

Notes-taker(s): David Robinson

Tags for the session - technology discussed/ideas considered:

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

What is the best way both from a security and from a user flow point of view for native mobile applications to authenticate and become authorized with access tokens?

Details:

Conversation started about how the web flow is fairly well known and understood, even when used on mobile devices, then turned to a discussion of how the AOL mobile applications work, where a user id and password are entered and the application contacts an AOL endpoint in order to get a token which is stored on the device... the user id and password never stored on the device. But how do users expect this to work from a screen flow point of view?

Discussed what a mobile screen might look like for logging in to services.

There might be a button that you click that causes a web view in your own app to load or alternately a web browser could be started and then you are redirected to a URL where you log in.

This screen could have a "default" username/password UI that sends credentials to a well known service provider that you want used for "all" or most of your mobile apps and then have other smaller buttons specific to other IdPs if you don't want to use the "default".

Drawing a different picture, you could have a drop down list where you pick an IdP from the list, and then enter a uid/pwd and press a "sign in" button - and that screen contacts the selected IdP. It was noted this was very similar to the way a wireless hotspot works today in some cases. The potential drawback of this is that the IdP may not support oauth - there are no guarantees. Also this method only really supports username/password credentials and no second factor support.

Facebook supports the ability to do a native client login. They pick particular partners that they allow their log-in to go to...but this is not a good general model

because it makes it difficult for random application developers to let people log into their app using Facebook, AOL, Google, etc. because the app developer has to go to each one to "negotiate" credentials ahead of time. This method basically attempts to use the OAuth2 Resource Owner Credentials grant type.

The "direct" Resource Owner Credentials grant has additional issues. Users are "conditioned" to look for certain chrome and we want to have the ability to do risk based authentication. We also like to do OTP.. Much of this becomes harder or "impossible" when working with pure native application scenarios that do not include any browser type flows. Since so much risk based heuristics are in place, we want to leverage this.

We need some assurance that users are not providing credentials to the wrong site in a phishing attack.

It was speculated that there are "3 modes" for a mobile app ...

1. During installation
2. The very first time the app is run
3. Other times the app is used

There was discussion about whether there are opportunities to take advantage of these "modes" to register the app with an IdP and provide some sort of credentials maybe during these moments that are less obtrusive than others. In particular it was mentioned that installation time might be a good time...but then counter arguments were that this would require Apple and Google to change their installation processes for all applications.

It was also noted that applications can leverage browsers...but web views cannot leverage applications (not sure where that comment was going...)

Is it too awkward to open a browser when a user starts in a native application? It was thought this was a bit awkward if it can be avoided...but for security the log in UI needs to connect directly to the IdP and not go through the native application.

It was mentioned that single sign on (SSO) protocols often "assume" a browser. Based on the need for the IdP to determine if the user is already logged in. There are ways to bootstrap an SSO event from an authentication/authorization token but these aren't standardized.

There was a question about how tokens get into an application when a browser is used to authenticate.

It was mentioned that in smart phones, you can register your own URI schemes and have the browser redirect the user to my application URI passing the token information on the URI, which can then be processed by the application.

Google described Android and it's Account Manager. The account manager handles

authentication/authorization for applications on an android phone. The account manager contacts a special end point for the native app and gets redirected to Google's IdP..which then can redirect the user further to a third party IdP if necessary. The user authenticates and authorizes...and the third party IdP issues a token. This token is flowed back through the Google IdP which then flows back to the original end point that was contacted, which returns a 200 to the account manager..which gets the URI and can strip the token and save it. It is possible to write "plug-ins" for random IdPs for Google's account manager. This allows other IdPs to register the process needed for Android apps to get OAuth tokens for that IdP.

There was a comment that while account manager makes sense for android, this doesn't make sense for all device types or even all mobile platforms. Some platforms like games systems are very constrained and don't really support passing of information between apps during app invocation.

Another concern with account manager is that installation on mobile devices does not allow for pre-reqs, so there is not way to guarantee that your plug-in for an IdP is loaded before your application is installed.

When Applications are installed, it should be up to the particular application whether it uses a separate browser, an embedded browser or handle the authentication/authorization in some other way.

Is it possible to release an IdP SDK for each of the major mobile platform ?

Someone suggested that you really should "always" use a web browser...but the conversation was about native applications.

There was some discussion on how to render log on screens appropriately on different devices so they display "nicely" and fit on the screen. Some IdPs use the OAuth extension for the 'display' parameter to identify which UI the IdP should display. This needs to be re-introduced and standardized.

There was discussion on what grant to use when using oauth on mobile devices. Someone suggested using the regular authorization grant. Someone else suggested that implicit grants were the way to go because they do not want to encourage anyone to put secrets on mobile devices. As a security measure, it was mentioned that callback URLs are custom schemes in some cases ...acting like "magic" URLs and are not regular http URLs. Since native apps have access to the entire HTTP response, it's easy for them to extract the token and other data from the OAuth2 Implicit Grant flow.

Someone stated they are going to continue to use web views until the time when the operating systems can inherently deliver centralized account managers.

There was some discussion of trying to standardize how mobile log ins work -

especially for native applications...then there were questions about where this would be done...not definitive answer...just a discussion at this point.

There was some discussion that you don't want to prompt a user "twice" for uid/pwd and then consent. Once they have installed an app, you may not want to re-ask if they want to grant the application authorization ...because the user just downloaded and installed the application. There was discussions on when/how to suppress the authorization page. There was discussion that this cannot and must not always be suppressed - so the IdP must be able to get specific information before it suppresses this screen.

It was also mentioned that cookies are available in a browser environment and these can also be leveraged for certain suppressions of screens. The key here is to mark the cookie has HTTPOnly so that JS in the browser can not get access to the data. Another solution is to use a custom HTTP header. This works because the native app has full access to all parts of the HTTP response.

If the authorization code is returned in the header, by design, a web application cannot get to it.

There was mention of the Facebook "account manager" - that it does not need to be running when a Facebook app is called...because the mobile OS will wake up the FB app to do its thing.

Finally, it was mentioned that each app is signed and has a special "signature" - called different things on different devices. This signature is passed to the account manager by the operating system when the account manager is called by an application wanting to authenticate/authorize. This adds security such that the account manager can match invoking app with it's client\_id and detect potential abuses.

## ***How to Manage Digital Multiple Identities Securely and Assuring Privacy on the Internet (W5C)***

URL:

<http://iiw.idcommons.net/How to Manage Digital Multiple Identities Securely and Assuring Privacy on Internet>

Convener: Guido Marinelli

Note-Taker(s): Guido Marinelli

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

Multiple Identity, privacy, security, authentication, identity provider, user centric

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

### **Overview**

The user centric identity management means that the user has the possibility to use, in an authentication process, only the attributes that are necessary to define the user profile needed for being authenticated. Moreover, a user can define a different identity credential for any different profile he needs or wishes.

### **Questions**

How to use the identity provider and the “anonymous credential” concepts to support the user in managing his multiple identities and in preserving his personal data privacy.

How to avoid that the multiple identities management becomes boring and unsecure for the users.

### **Demo**

Pip&Pops credential management software has been presented as an example of a tool to declare and manage, in a fast and secure way, user multiple identities.

## ***Payment Card Industry Trust Framework (W5D)***

URL: [http://iiw.idcommons.net/The\\_Payment\\_Card\\_Trust\\_Framework](http://iiw.idcommons.net/The_Payment_Card_Trust_Framework)

Convener: Sid Sidner

Notes-taker(s): Sid Sidner

Tags for the session - technology discussed/ideas considered:

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

Sid:

- Cards now make up over 50% of the the transactions in the USA.
- The process of 4 party model of credit networks (Sid refers to the 5 party model "the evil pentagram" where he breaks out the Network and the Issuer)
- Acquirers, Networks, Issuers, Merchants, Consumer <-- see Sid's blog post for a 12 slide presentation on this topic
- 1. Merchants decide what types of cards they're going to accept (decrease the friction and outsourcing his credit-issuing processes, in exchange they pay the Acquirer a Merchant Discount Rate (1-3%))
- 2. Acquirers aggregate merchants on behalf of the Networks (and they generally mark-up the interchange fee, by layering on a Merchant Discount Rate)
- 3. Networks offer the foreign exchange, connectivity, standards, audit, etc. to the system (They make ~25% of the interchange fee charged to the merchant)
- 4. Issuers (generally banks) issue cards to customers (they and the Network charge interchange to the Acquirers, the issuers make ~75% of the interchange charged to the merchant)
- 5. Customers take cards from Issuers to get access to credit. Sometimes they pay a small fee for the card. This fee is insignificant to the fees generated by the card through the purchases, or through interest on balances.
- "You have rights because of my duties"
- Level of Assurance (ID Service Provider) , Level of Protection (RP), Level of Control (User)



Drummond Reed:

- This Trust Framework was set up to move money.
- The Respect Trust Framework was set up to protect the movement of data, exchange of value.
- VISA: "the largest network to effect the transfer of value" see: "The Birth of the Chaotic Age" a book by Dee Hock, founder of Visa - google search of "Desmore Chaotic Age": <http://www.globalhome.com/news/chaordic/bookreview.html>
- In PAYMENTS: Merchants can't all deal with us to sending cash to them directly, so the payment network acts as a broker/aggregator
- The concept of the Respect Trust Framework is to allow you to manage the process of moving information (personal data) to various parties.
- Using the Trust Framework, the data becomes more valuable, more manageable,
- Cardholders aren't stakeholders in the Payment Network Trust Framework, but they are in the Respect Trust Framework.
- If you join the Respect Trust Framework, you're joining a mechanism for the orderly performing business using personal data. A set of rules, a set of principles, clarity of roles and responsibilities.
- Discussion of the consumer representation / participation in the payment ecosystem vs the Respect Trust Framework. Self-governing aspects. The members of the network have control of the changes to the network.
- Discussion of L3C entities: A low-profit limited liability company (L3C) <http://en.wikipedia.org/wiki/L3C>
- Discussion of how Respect Trust Framework will make money by brokering access to my personal data to entities like Facebook, etc. When challenged on the concerns of "whoever is paying, is the real customer", Drummond referred



to free checking accounts generating revenues for banks by holding the cash, and what they can do with the cash.

Other reading:

1. Doc Searls: sense-of-bewronging <http://blogs.law.harvard.edu/doc/2011/04/02/a-sense-of-bewronging/>
2. [http://users.crocker.com/~newshare/reports/visa\\_founding.html](http://users.crocker.com/~newshare/reports/visa_founding.html)

## ***VRM @ Work (W5E)***

URL: <http://iiw.idcommons.net/VRM @ Work>

Convener:

Note-Taker(s):

## ***ID Legal (W5F)***

URL: <http://iiw.idcommons.net/ID/Legal: Dialogue Collaboration>

Convener: Judi

Notes-taker(s): Judi

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

Law, technology, lexicon, policy, ID Commons, ABA,

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

1/ ID Legal: past and future

2/ connections - what people in the room are doing

3/ architectures and modeling

4/ open questions, uncertainty, liability, mechanisms

5/ thresholds: anonymity/de-identification, sensitivity, legal duties

6/ lexicon (Scott will distribute Global Glossary Grid by next call)

7/ privacy, security, ownership: societal desire, balance

8/ future: join our calls! (next one in June)

## ***Data as Currency (W5G)***

URL: [http://iiw.idcommons.net/Conversation\\_Around\\_Data\\_as\\_Currency](http://iiw.idcommons.net/Conversation_Around_Data_as_Currency)

Convener: Heather Vescent

Notes-taker(s): Vanessa Miemis

Tags for the session - technology discussed/ideas considered:

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

What is data?

- information → collection
- contextual
- timelines
- faded value

What is currency?

- money? fungible? non-fungible?
- exchange of value, store of value
- asset / liability
- deposit / return

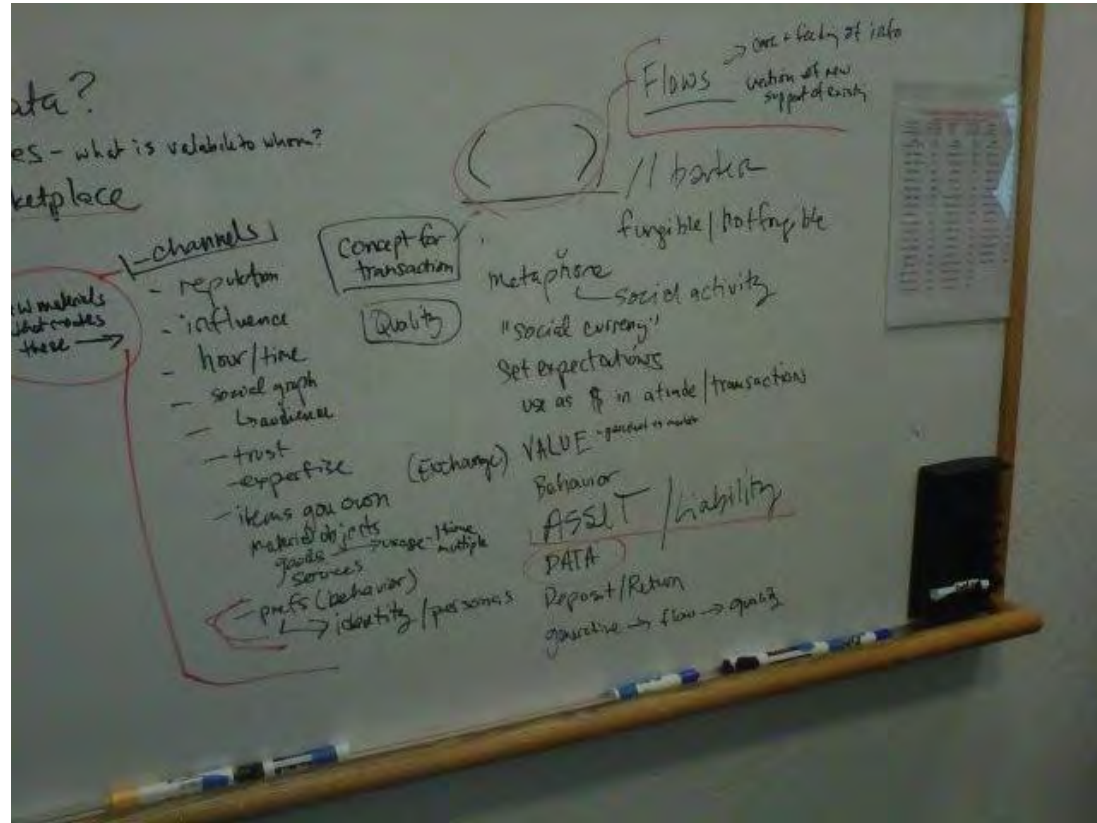
currency → a creator of currents; a formal system used to shape, enable or measure currents; creation and shaping of currencies & flows; care and feeding of info (nurturing), creation of new flows & supporting of existing flows

How to value the data?

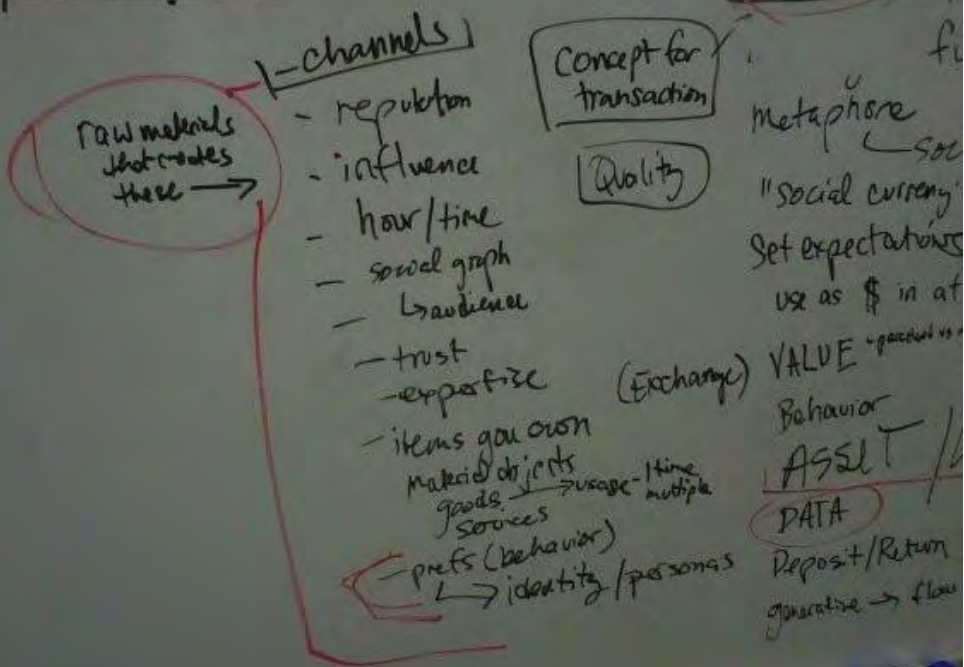
- weighed values - what is valuable to whom? (it's contextual)
- to sell / collect / marketplace

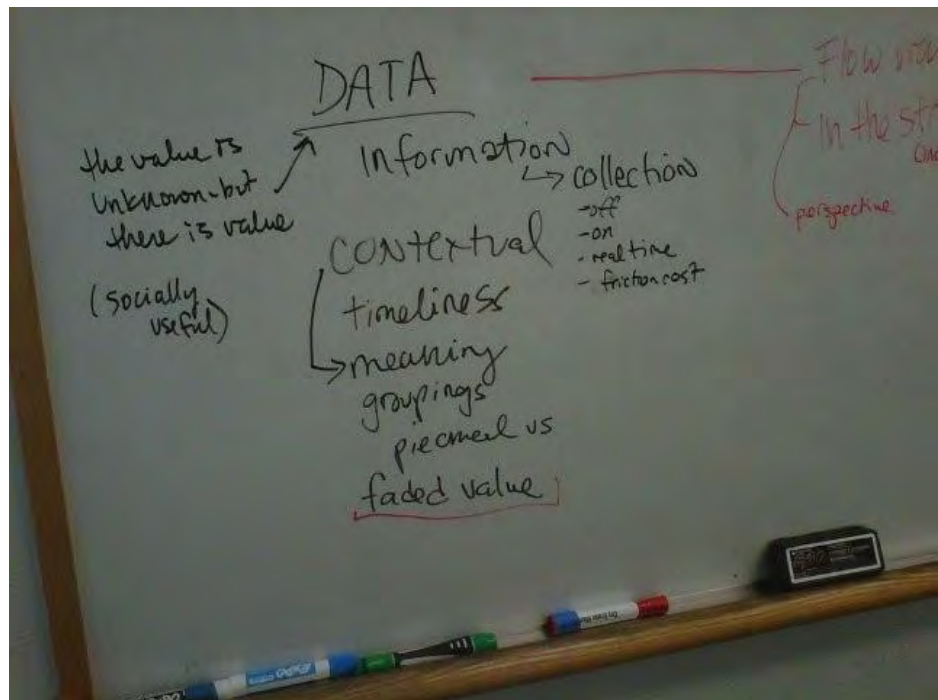
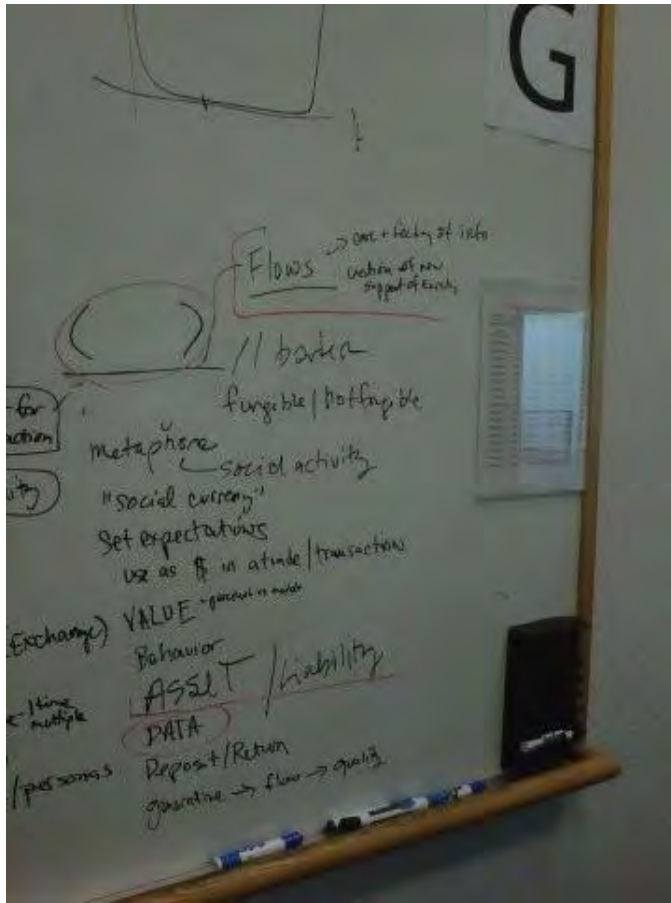
What are some concepts for transactions? what are the raw materials that create them?

- reputation
- influence
- time/hour
- social graph → audience
- expertise
- trust
- preferences (behaviors)



# collect / marketplace





## ***How Yahoo! Became RP: A Large Scale Implementation Study (W5I)***

URL: [http://iiw.idcommons.net/How Yahoo! Became RP: A Large Scale Implementation Study](http://iiw.idcommons.net/How_Yahoo!_Became_RP:_A_Large_Scale_Implementation_Study)

Convener:

Note-Taker(s):



## ***Open Architecture for Step Up Authentication (W5N)***

URL: [http://iiw.idcommons.net/Open\\_Architecture\\_for\\_Step\\_Up\\_Authentication](http://iiw.idcommons.net/Open_Architecture_for_Step_Up_Authentication)

Convener:

Note-Taker(s):

Day 3 - Thursday, May 5<sup>th</sup>

Session 1

***For Public Consumption. Choose Wisely: Identity as Selective Pressure on Biology (TH1A)***

URL:

[http://iiw.idcommons.net/For Public Consumption. Choose Wisely: Identity as selective pressure on biology](http://iiw.idcommons.net/For_Public_Consumption._Choose_Wisely:_Identity_as_selective_pressure_on_biology)

Convener:

Note-Taker(s):

## ***Respect Trust Framework Q+A (part 3) Become a trust Anchor (TH1C)***

URL: [http://iiw.idcommons.net/Respect\\_Trust\\_Framework\\_Q+A\\_\(part\\_3\)\\_Become\\_a\\_trust\\_anchor](http://iiw.idcommons.net/Respect_Trust_Framework_Q+A_(part_3)_Become_a_trust_anchor)

Convener:

Note-Taker(s):

## ***Data Portability for Trust Frameworks (TH1E)***

URL: [http://iiw.idcommons.net/Data\\_Portability\\_for\\_Trust\\_Frameworks](http://iiw.idcommons.net/Data_Portability_for_Trust_Frameworks)

Convener:

Note-Taker(s):

## ***OpenID Specificatin Work (TH1G)***

URL: [http://iiw.idcommons.net/OpenID\\_Specification\\_Work](http://iiw.idcommons.net/OpenID_Specification_Work)

Convener: Mike Jones

Notes-taker(s): Mike Jones

Tags for the session - technology discussed/ideas considered:

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

Nat Sakimura  
Axel Nennker  
Michael Buck  
Tony Nadalin  
Mike Jones  
George Fletcher  
John Bradley  
Breno de Medeiros

Listed issues still open:

- UserInfo schema
- Where/how to represent session state
- Compatibility/migration support
- Specifying identifier type (omnidirectional, directed, ephemeral, etc.)

Reviewed request structure from yesterday

Decision: One id\_token (rather than separate id and session tokens) - try to keep small

Decision: Put PAPE information in id\_token

Decision: Try to keep PAPE information short - possibly using IANA registry (which is already being created) for short names

Decision: Spec only defines how UserInfo endpoint provides information about user the access token is for

## ***Internet Bill of Rights for “Vegas” Model (TH11)***

URL: [http://iiw.idcommons.net/Internet Bill of Rights for “Vegas” Model](http://iiw.idcommons.net/Internet_Bill_of_Rights_for_“Vegas”_Model)

Convener:

Note-Taker(s):

## Session 2

### *ietf OAuth: Status & Next Steps (TH2A)*

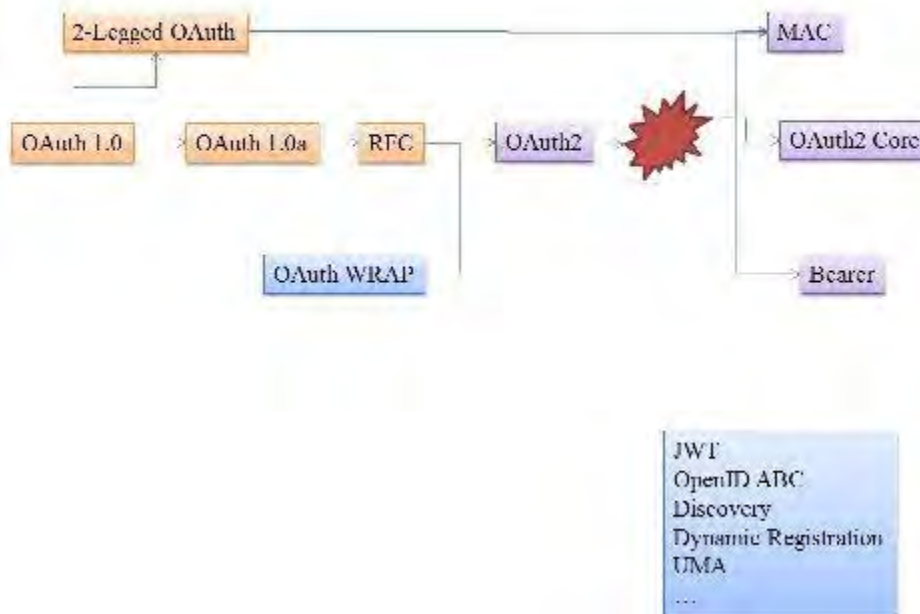
URL: [http://iiw.idcommons.net/ietf\\_oauth: Status %26 Next Steps](http://iiw.idcommons.net/ietf_oauth: Status %26 Next Steps)

Convener: Justin , Hannes, Tom, Mike

Notes-taker(s): Slide from Justin

Tags for the session - technology discussed/ideas considered:

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



## ***MYDEX CIC (TH2D)***

URL: [http://iiw.idcommons.net/MYDEX\\_CIC](http://iiw.idcommons.net/MYDEX_CIC)

Convener:

Note-Taker(s):



## ***NSTIC Attributes (TH2E)***

URL: [http://iiw.idcommons.net/NSTIC\\_Attributes](http://iiw.idcommons.net/NSTIC_Attributes)

Convener:

Note-Taker(s):

## ***Purpose Binding (TH2F)***

URL: [http://iiw.idcommons.net/Purpose\\_Binding](http://iiw.idcommons.net/Purpose_Binding)

Convener:

Note-Taker(s):

## ***Personal Data Ecosystems (TH2G)***

URL: [http://iiw.idcommons.net/Personal Data Ecosytems](http://iiw.idcommons.net/Personal_Data_Ecosytems)

Convener:

Note-Taker(s):

## Session 3

### ***What Part Is Identity and What Part is Personal Data? (TH3A)***

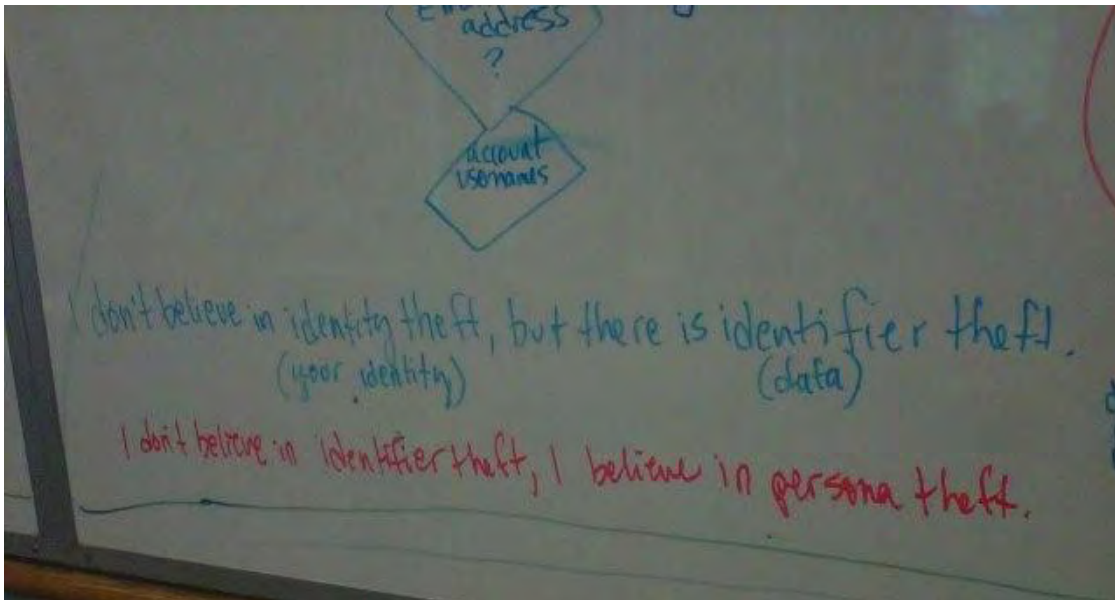
URL: [http://iiw.idcommons.net/What\\_part\\_is\\_Identity%3F\\_What\\_part\\_is\\_Personal\\_Data%3F](http://iiw.idcommons.net/What_part_is_Identity%3F_What_part_is_Personal_Data%3F)

Convener: Heather Vescent and Mary Hodder

Notes-taker(s): Heather Vescent (white board photo's)

Tags for the session - technology discussed/ideas considered:

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





## **Open ID Specification Work (TH3&4B)**

URL: [http://iiw.idcommons.net/Open\\_ID\\_Specification\\_Work](http://iiw.idcommons.net/Open_ID_Specification_Work)

Convener: Mike Jones

Notes-taker(s): Mike Jones

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

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

Thursday 11:30

George Fletcher  
Breno de Medeiros  
Pamela Dingle  
Vikas Jain  
Tony Nadalin  
Michael Buck  
John Bradley  
Nat Sakimura  
Mike Jones

These people joined us during the lunch hour, as work continued:

Dale Olds  
John Panzer  
Edmund Jay

We started with the topic of the schema for the UserInfo endpoint. Chuck Mortimore supplied this input data for the decision:

- This is PoCo - also wire compatible with OpenSocial - <http://portablecontacts.net/draft-schema.html>
- This is the early SCIM work. We based ours on PoCo - I'd like to make sure this is overlapped and wire compatible - <http://www.simplecloud.info/>
- RPX normalizes all their providers to PoCo - [https://rpxnow.com/docs#profile\\_data](https://rpxnow.com/docs#profile_data)
- Here's detail on how the data that the networks will actually return - <https://rpxnow.com/docs/providers>

Decision: Don't invent something new

Decision: Adopt a subset of the Portable Contacts schema

Fields in basic set:

Display Name

Nickname  
Full Name  
Photo  
e-Mail Address  
URLs (typed, with types including “profile”, “blog”, etc.)  
Data of Birth / Age  
Equivalent of everything in SREG  
Verified e-mail (verified other?)

Breno: could define a mechanism to ask about validation of claims  
(especially e-mail)

Mike: Use claim(s) to express that e-mail and maybe other claims  
are verified

Decision: Don’t change POCO e-mail format - add verification  
claim(s) that can be ignored if not understood

Decision: Add “verified” into the POCO structure - parallel to  
“primary”

Meta - time last modified  
Phone number

Breno: May want to define second set of supplemental attributes that are not in basic  
set

Address  
Organization

Rejected:

providerName - comes at the wrong point in the flow  
preferred username

George: Context and purpose form-fill for site registration

Observation: POCO contains both fields about me and fields about what I know about  
others.

Decision: We are only including fields that are about me.

Nat: Need to extend to be able to represent information in multiple scripts

Nat has proposal for how to extend fields for multiple scripts

#language\_script\_country  
#ISO639\_ISO15924\_ISO3166

Example: [http://axschema.org/namePerson#ja\\_Kana\\_JP](http://axschema.org/namePerson#ja_Kana_JP)

Breno: There is an ISO format for this - Nat and Breno will investigate

Decision: Ignore information you don’t understand

Need to discuss “id”, PPID, ephemeral ID

SCIM “id” stable and omnidirectional

Breno: “id” omnidirectional, stable, IdP-relative. Should not be returned if directional identifier in id\_token.

Breno: ID returned from userInfo endpoint should match the one in the id\_token. If directional, call it “ppid”.

Decision: Single “id” field, and also an ID Type field that can be ignored if not understood.

Defined ID Type values “omnidirectional”, “directional”. Other understood values MAY be used.

Breno: For compatibility: define “openid\_identifier” field

Decision: SCIM externalId, userName don’t make sense in this context



## ***Bill O' Rights O Rama (TH3D)***

URL: [http://iw.idcommons.net/Bill\\_O'Rights\\_O\\_Rama](http://iw.idcommons.net/Bill_O'Rights_O_Rama)

Convener: Kaliya

Notes-taker(s): Kevin Meiler

Tags for the session - technology discussed/ideas considered:

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

Personal Data Bill of Rights

Legal Law

Standards

Implementation

Is there broad interest in privacy?

- diaspora - has large number of signups

"In America, Bill of rights was given to people from the elite"

What rights to your "own" data do you have?

Difference in Finland, Italy.

Use of US data sources.

Italy: public agencies - 15 days to correct & explain mistakes

McCain Bill: intended to bring to level of European norms

Use of law and commerce to enforce / understand ownership.

What's OK, what's not?

Kaliya:

- OK if single site monitors behavior

- not OK if do cross-site correlation without permission

(website terms of use permits this)

(not permitted in Italy w/o specific permission)

(EU: cannot do this w/o specific purpose; Google gives better service sw

it's OK)

PDE: working to evaluate \$ in ecosystem

Segmentation discussion "segment of 1", additional propensity measure

Discussion on economic value for those making privacy/exchange tools for tool maker, for end users, for others

- \$280M in startup funding in this area
- 12 startups in this space

## ***Strategies for Ubiquity (TH3E)***

URL: [http://iiw.idcommons.net/Strategies\\_for\\_Ubiquity](http://iiw.idcommons.net/Strategies_for_Ubiquity)

Convener:

Note-Taker(s):

## ***NSTIC Risks Legal Liability (TH3F)***

URL: [http://iiw.idcommons.net/NSTIC Risks Legal Liability](http://iiw.idcommons.net/NSTIC_Risks_Legal_Liability)

Convener:

Note-Taker(s):

***News personalized by inference or expression... managing the users persona (TH3G)***

URL:

[http://iiw.idcommons.net/News\\_personalized\\_by\\_inference\\_or\\_expression...managing\\_the\\_user's\\_persona](http://iiw.idcommons.net/News_personalized_by_inference_or_expression...managing_the_user's_persona)

Convener:

Note-Taker(s):

## ***The Locker Project (TH3H)***

URL: [http://iiw.idcommons.net/The Locker Project](http://iiw.idcommons.net/The_Locker_Project)

Convener:

Note-Taker(s):

## Session 4

### ***What part is Identity? What part is Personal Data? (TH4A)***

URL: [http://iiw.idcommons.net/What\\_part\\_is\\_Identity%3F\\_What\\_part\\_is\\_Personal\\_Data%3F](http://iiw.idcommons.net/What_part_is_Identity%3F_What_part_is_Personal_Data%3F)

Convener: Heather Vescent and Mary Hodder

Note-Taker(s): Heather Vescent (white board photo's)

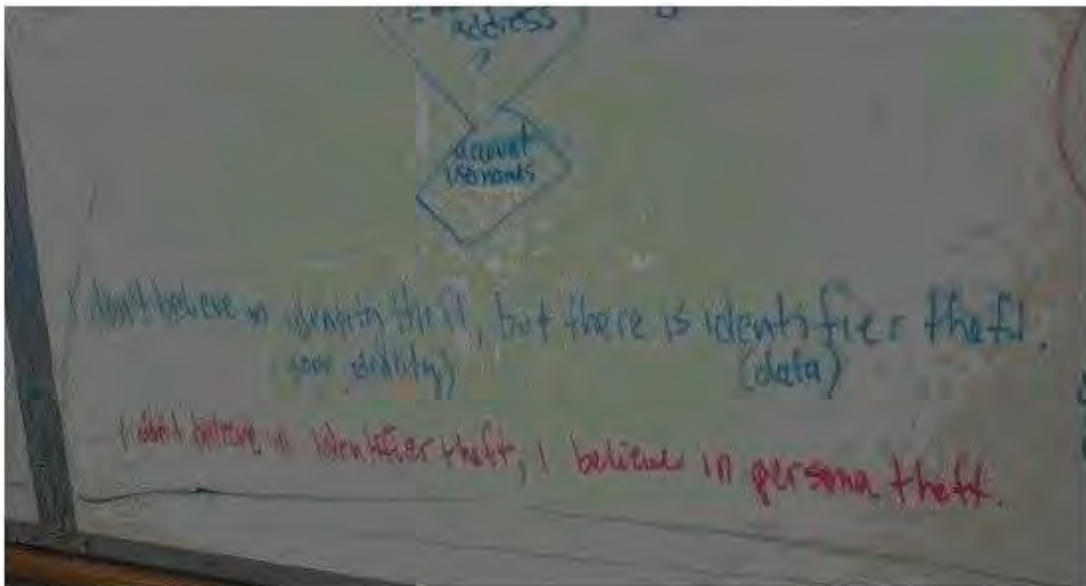
### **What Part Is Identity and What Part is Personal Data? (TH3A)**

Convener: Heather Vescent and Mary Hodder

Notes-taker(s): Heather Vescent (white board photo's)

Tags for the session - technology discussed/ideas considered:

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



## ***Open ID Specification Work (TH3&4B)***

URL: [http://iiw.idcommons.net/Open\\_ID\\_Specification\\_Work](http://iiw.idcommons.net/Open_ID_Specification_Work)

Convener: Mike Jones

Notes-taker(s): Mike Jones

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

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

Thursday 11:30

George Fletcher  
Breno de Medeiros  
Pamela Dingle  
Vikas Jain  
Tony Nadalin  
Michael Buck  
John Bradley  
Nat Sakimura  
Mike Jones

These people joined us during the lunch hour, as work continued:

Dale Olds  
John Panzer  
Edmund Jay

We started with the topic of the schema for the UserInfo endpoint. Chuck Mortimore supplied this input data for the decision:

- This is PoCo - also wire compatible with OpenSocial - <http://portablecontacts.net/draft-schema.html>
- This is the early SCIM work. We based ours on PoCo - I'd like to make sure this is overlapped and wire compatible - <http://www.simplecloud.info/>
- RPX normalizes all their providers to PoCo - [https://rpxnow.com/docs#profile\\_data](https://rpxnow.com/docs#profile_data)
- Here's detail on how the data that the networks will actually return - <https://rpxnow.com/docs/providers>

Decision: Don't invent something new

Decision: Adopt a subset of the Portable Contacts schema

Fields in basic set:

Display Name



Nickname  
Full Name  
Photo  
e-Mail Address  
URLs (typed, with types including “profile”, “blog”, etc.)  
Data of Birth / Age  
Equivalent of everything in SREG  
Verified e-mail (verified other?)

Breno: could define a mechanism to ask about validation of claims  
(especially e-mail)

Mike: Use claim(s) to express that e-mail and maybe other claims  
are verified

Decision: Don’t change POCO e-mail format - add verification  
claim(s) that can be ignored if not understood

Decision: Add “verified” into the POCO structure - parallel to  
“primary”

Meta - time last modified  
Phone number

Breno: May want to define second set of supplemental attributes that are not in basic  
set

Address  
Organization

Rejected:

providerName - comes at the wrong point in the flow  
preferred username

George: Context and purpose form-fill for site registration

Observation: POCO contains both fields about me and fields about what I know about  
others.

Decision: We are only including fields that are about me.

Nat: Need to extend to be able to represent information in multiple scripts

Nat has proposal for how to extend fields for multiple scripts

#language\_script\_country  
#ISO639\_ISO15924\_ISO3166

Example: [http://axschema.org/namePerson#ja\\_Kana\\_JP](http://axschema.org/namePerson#ja_Kana_JP)

Breno: There is an ISO format for this - Nat and Breno will investigate

Decision: Ignore information you don’t understand

Need to discuss “id”, PPID, ephemeral ID

SCIM “id” stable and omnidirectional

Breno: “id” omnidirectional, stable, IdP-relative. Should not be returned if directional identifier in id\_token.

Breno: ID returned from userInfo endpoint should match the one in the id\_token. If directional, call it “ppid”.

Decision: Single “id” field, and also an ID Type field that can be ignored if not understood.

Defined ID Type values “omnidirectional”, “directional”. Other understood values MAY be used.

Breno: For compatibility: define “openid\_identifier” field

Decision: SCIM externalId, userName don’t make sense in this context

***How is it that the legal structures don't have the right terms/approach for identity + data + What do we do about it? (TH4C)***

URL: [http://iiw.idcommons.net/Legal\\_Structures](http://iiw.idcommons.net/Legal_Structures)

Convener: Dave Sanford

Notes-taker(s): Dave Sanford

Tags for the session - technology discussed/ideas considered:

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

Session did not occur.

From short exchange:

“Who has what right to access and use data?”

## ***Personal Data Ecosystem (TH4D)***

URL: <http://iiw.idcommons.net/Personal Data - Stores, Lockers, Vaults>

Convener: Kaliya Hamlin

Notes-taker(s): Wendell Baker

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

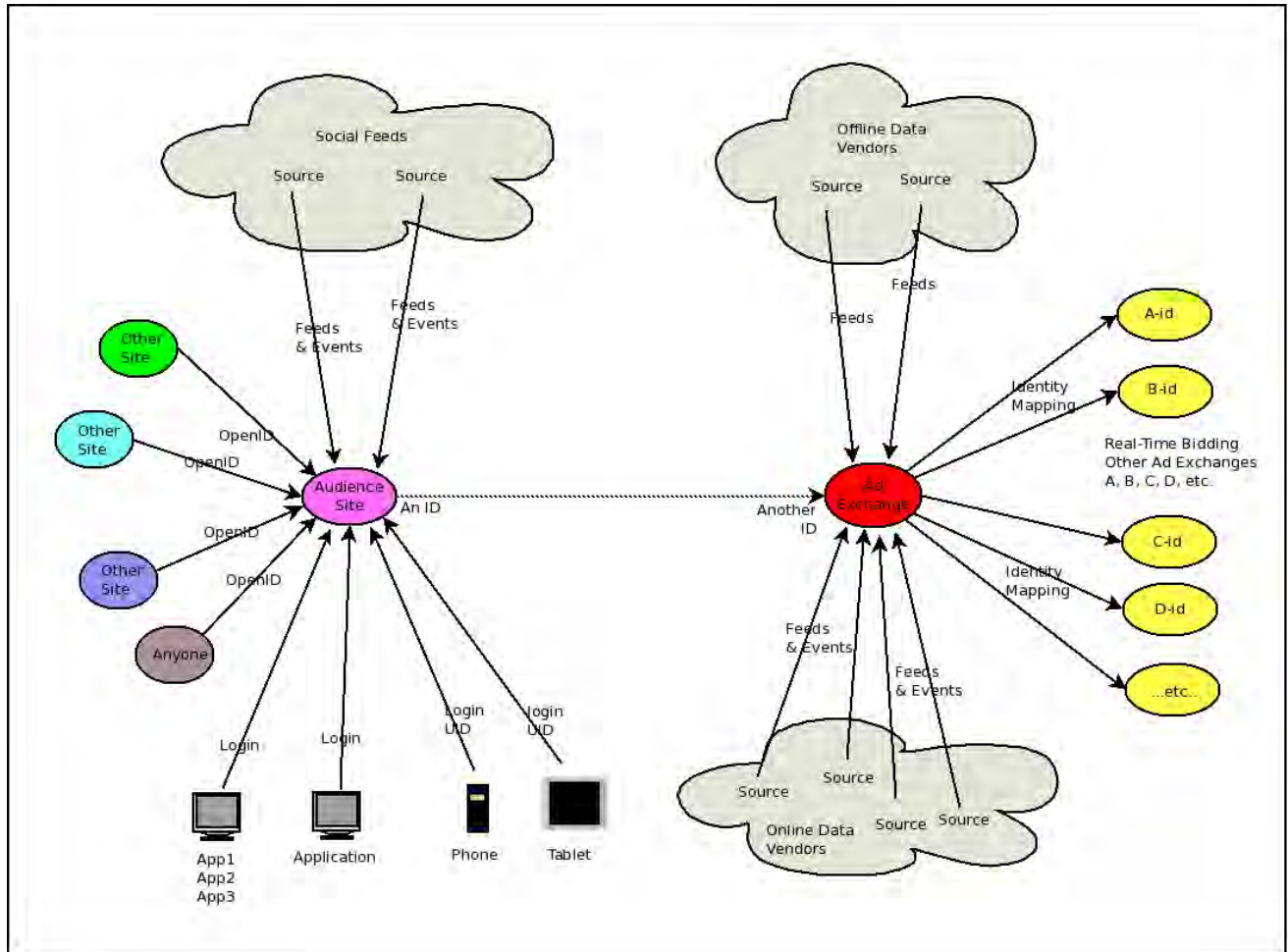
**H. Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:**

The identity ecosystem from the perspective of an entertainment provider consists of an audience side and an advertising side. The audience side of the house creates experiences which are fun to play and cause the users to return to the site. The advertising side is often a key aspect of the monetization strategy for the site. The current structure of the industry maintains both of these systems in parallel though that is changing. This diagram is part of that story.

Audience sites typically manage user identities using a "screen name" or "email provider" approach. This works well to identify the person sitting behind the program or device that is contacting the service. This works well when "the browser" is the only interface to the site. However, with the rise of the "app" economy (installed-on-client programs that are not obviously a JavaScript-enabled HTML browser) there is interest in identifying both the application and the user behind the application. Audience sites are increasingly finding ways to chain identities together using open protocols such as OpenID or by other means. Additionally the audience sites use information about user behavior on other sites to help personalize the experience. This can be done with offline data feeds that are provided to the audience site to help customize the experience.

The advertising side typically manages user identities in a "force-placed" approach where the browser or applications are assigned a unique identifier. This is done to manage the user experience along such dimensions such as frequency capping, recency or intensity and to associate personalization with the advertising experience. In these systems, the advertising identifier stamp is typically tied one-to-one to the device or program. However, a user may have multiple computers or browsers; also a computer or browser may be shared among multiple users. Both of these effects confound intensity and personalization systems which are actually directed towards individuals, not devices. Both online and offline sources of data are used to enhance the ad selection process. For a given opportunity, ads are often selected using an "exchange" which clears a trade much like an open-cry stock or commodities market. In order to increase liquidity in these marketplaces, systems of real-time bidding have arisen to allow the opportunity to be traded across multiple marketplaces. In order to ensure that the original levels of privacy and anonymity are preserved across the marketplaces, the user identity stamp is typically transformed (cryptographically hashed) when the opportunity is offered on a different marketplace. This preserves the privacy of the user and ensures that the publisher's data rights are preserved.

The dashed arrow in the middle is a new development in the entertainment industry. In that model the audience side identity, which nominates a user, is chained to the advertising side identity system. This allows the advertising system to personalize and to limit the advertising towards an person rather than having to guess (or not) about that based on device or browser use.



## ***Square Tag (TH4E)***

URL: [http://iiw.idcommons.net/Square\\_Tag](http://iiw.idcommons.net/Square_Tag)

Convener: Sam Curren

Notes-taker(s): Sam Curren

Tags for the session - technology discussed/ideas considered:

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

SquareTag - Thursday Session 4 Sam Curren

Issues/Opportunities moving forward:

Industry redirection/namespace organization - create an organization that handled providers going out of business, porting of tags to other providers, and global namespace

full JSONSchema support - lists of objects

Multi-owner scenarios - Data and access rights.

Public tag data - allowing the public to see/update portions of data

Monetization opportunities beyond tag purchase

Manufacturer involvement - data from the beginning

Signed/Certified information/records - ability to verify attributes/records present in a tag.

Media attachment - adding pictures and other encoded data.

## ***Red Teaming Trust Frameworks (TH4F)***

URL: [http://iiw.idcommons.net/Red Teaming Trust Frameworks](http://iiw.idcommons.net/Red_Teaming_Trust_Frameworks)

Convener:

Note-Taker(s):

## ***Give me tips on creating personal (TH4G)***

URL: [http://iiv.idcommons.net/Give me tips on creating persona](http://iiv.idcommons.net/Give_me_tips_on_creating_persona)

Convener:

Note-Taker(s):



## ***Field Guide to Real World Trust Frameworks (TH4H)***

URL: [http://iiw.idcommons.net/Field\\_Guide\\_to\\_Real\\_World\\_Trust\\_Frameworks](http://iiw.idcommons.net/Field_Guide_to_Real_World_Trust_Frameworks)

Convener:

Note-Taker(s):

## ***Start-ups table (TH4M)***

URL: [http://iiw.idcommons.net/Start-ups table](http://iiw.idcommons.net/Start-ups_table)

Convener:

Note-Taker(s):

## Session 5

### *OPEN ID Specification Work (cont) (TH5B)*

URL: [http://iiw.idcommons.net/Open ID Specification Work \(Cont.\)](http://iiw.idcommons.net/Open_ID_Specification_Work_(Cont.))

Convener: Mike Jones

Notes-taker(s): Mike Jones

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

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

George Fletcher  
Nat Sakimura  
John Bradley  
Pamela Dingle  
Tony Nadalin  
Dale Olds  
Vikas Jain  
Breno de Medeiros  
Edmund Jay  
Mike Jones  
Michael Buck

How do we request directional or omnidirectional identifiers?

In OpenID 2.0, could only request directional identifiers. ICAM profile has PAPE parameter to ask for directional identifiers.

Decision: Allow “idType” claim value in request. Default type is omnidirectional. IdPs should be allowed to only support one idType.

MUST be illegal to return omnidirectional if directional or ephemeral requested.

Discussion: “ephemeral”, “transactional” may be a request types we define in the future, based upon use cases.

Unsigned JWT: `base64url({"sig":"none"}).base64url({claims...})`.

Breno: Define `maxAuthAge=seconds` query parameter as common case

Breno: If a defined parameter occurs twice, it should be an error

Nat: Wants requested language preference of RP to be expressible to IdP. Canada wants the same thing.

====

Final remaining open issue: OpenID 2.0 compatibility/migration issues

One element of support: "openid\_identifier" UserInfo field

OpenID 2.0 allows identifier delegation - we already decided not to support this in ABC

George: Need a way for IdP to say that old identifier and new identifier are the same

Breno: Treat identifier migration as a form of account recovery - John: it's an account linking problem

Breno: need to define an OpenID discovery endpoint to allow OPs to discover the clientID of RP realm for the issuer to enable migration

Breno: For compatibility, have openid\_realm parameter in request, which must match beginning substring of redirect URI

Then can generate OpenID 2.0 OP local identifier and put it in the UserInfo endpoint

RP must verify that OP is authoritative for OP local identifier returned

Need OpenID 2.0 service that identifies OpenID ABC endpoint

**WE APPEAR TO HAVE CLOSED ALL THE OPEN ISSUES!!!**

Spec editing tasks:

Revise spec to reference (not include!) OAuth 2.0

Breno: Spec as a whole needs to be reworked to be much more readable, complete

John: John, Nat, Mike together in Munich next week - take an initial pass at it together

Compatibility not in core spec - Breno volunteered for this

UserInfo endpoint schema in its own spec - Pamela volunteered for this

Claims request and claims response - Mike will write up, Edmund will then turn into spec language

## ***Is There Value In An Open Reputation Framework, If So Where Should it be Standardized? (TH5C)***

URL: [http://iiw.idcommons.net/Is\\_there\\_value\\_in\\_an\\_open\\_reputation\\_framework%3F](http://iiw.idcommons.net/Is_there_value_in_an_open_reputation_framework%3F)

Convener: Dave Sanford

Notes-taker(s): Dave Sanford

### **Tags for the session**

technology discussed/ideas considered: reputation, meta-reputation, rogue reputation sites,

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

Started session with explanation that Nat (?) had talked to me in the last few hours and indicated that the OASIS effort for Open Reputation Management was not dead necessarily, just dormant, and that work could re-start on that once people were available and once some of the related IIW work on identity and user managed information was clearer - so that we have a better basis for an ethical framework for information about people that shouldn't be able to be managed by them.

Discussion started with artifacts of reputation (badge) that would be provided by a site that assigns value to reputation generated from other sites. Lots of discussion of Stack Overflow. Turns out there could be lots of such meta-reputations sites and should be for a good ecosystem. In part, because reputation generating sites should have reputation themselves, particularly because of the inevitability of rogue reputation sites.

There was discussion of contracts and other cases where entities were relying on reputation information sites in ways that relate to real world value - and the concern that it is particularly important to make sure that reputation receivers are not somehow compensating the reputation givers.

Reputation was described as a predictor of the future if it has any utility.

Meta-critic was described as a good example of a meta-reputation and/or aggregator of reputation for video games, movies and other things. One person indicated that they had contemplated writing contracts that depended on a good score from Meta-critic. Discussion of how meta-critic works. Talked about various niche communities and the pros and cons of having algorithmic as well as human ratings.

Discussion of the role of transparency, anonymity and the ability to create new identities and how that could dilute the utility of reputation for certain purposes. The least cost might be opportunity cost of one's time.

The idea was brought up that perhaps Connect.Me is trying to build the framework for a reputation system. There was discussion of what happens when a big network joins a small network - if practices of the small network apply to the large network, it could change it - but in general the big network practices will swamp the smaller one.

The idea was posed that the best reputation networks would include people who have reasons to compete or disagree to create creative tension and competition.

## ***Digital Death (TH5D)***

URL: [http://iiw.idcommons.net/Digital\\_Death](http://iiw.idcommons.net/Digital_Death)

Convener:

Note-Taker(s):

## ***Real world VRM example + code for VRM App (TH5E)***

URL: [http://iiw.idcommons.net/Real\\_world\\_VRM\\_example\\_code\\_for\\_VRM\\_App](http://iiw.idcommons.net/Real_world_VRM_example_code_for_VRM_App)

Convener:

Note-Taker(s):



## Make OAuth Easy for REST Developers (TH5F)

URL: [http://iiw.idcommons.net/Make\\_OAUTH2\\_Easy\\_for\\_Rest\\_Developers](http://iiw.idcommons.net/Make_OAUTH2_Easy_for_Rest_Developers)

Convener: Kristoffer Gronowski

Notes-taker(s): Kristoffer Gronowski

Tags for the session - technology discussed/ideas considered:

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

Some 25 people turned up in room F 2-3 p.m. Thursday for the session. Several of the authors in IETF of OAuth 2 and also some of the UMA chairs.

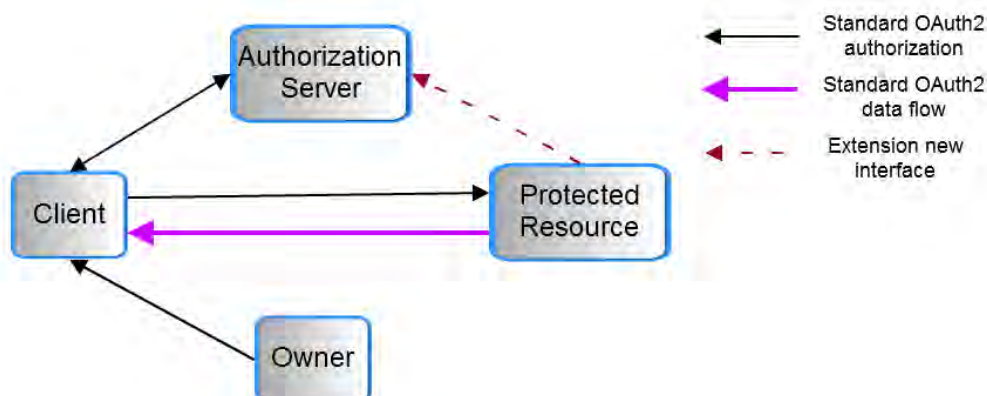
Just some background to the discussion:

Kristoffer with his team from Ericsson research has been building a distributed social network and during that work implemented parts of it in OAuth2.

The research work was conducted in collaboration with the <http://restlet.org> community providing the base rest platform. All standard pieces were contributed to the Restlet open source community.

Other components are blogged and put on display for interoperability at <https://labs.ericsson.com/apis/oauth2-framework/> hoping to spread the word about the technology.

I am including the notes and a reconstruction of the white board sketch.



Please feel free to post them and if appropriate a thank you note to all participants of the workshop listening and contributing to a fantastic discussion.

## ***Certified Identity (TH5H)***

URL: [http://iiw.idcommons.net/Certified\\_Identity](http://iiw.idcommons.net/Certified_Identity)

Convener: Sid Sidner

Notes-taker(s): Amanda Anganes

Tags for the session - technology discussed/ideas considered:

Reputation, certification, verification, claims, attributes

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

Origin documents

Building up credit/reputation - takes time, build up credit history with multiple OK transactions => creates trust

Story from Sid about getting TS security clearance - \$20,000 from company, lots of investigators working, expensive process but in the end having clearance makes Sid more valuable - tons of job offers immediately after

FB has said they want to be a "real ID" service

Self-attested info more reliable?

Check info - email addr must not bounce, mailing addr must be real (check w post office)

"Real ID" drivers license suggestion - turned down, too much work for DMV

Idea: suppose services could vett attributes - make claims, giving you a badge to show certified attr. on your FB page

Is this valuable?

Chaining ID forms / verification

Over time, value of badge could accrue - I have been certified with X for 5 years, etc

In Finland, Nils (last name?) created ID badge for FB linking your page to national ID - worked, but FB changed app model and it couldn't be used anymore.

On FB certification doesn't matter so much - social links provide verification of your ID

On LinkedIn, more useful - verify employers, etc

Mechanics are complicated - security, authorization of asserting parties

One different idea is that of an Oracle - doesn't directly release your info, but can answer questions like "is this person over 18?" Not what is being suggested here.

Some use cases:

Verify user is over 18 before visiting certain websites, or over 21 to purchase alcohol online

Verify user is a real person for online dating sites

Verify employer history on LinkedIn/resume

Proves there is value in such a service.

Idea here is to validate claims - not necessarily focusing on proving you are you; that is another problem

Universal ID - Netherlands national ID w/card reader, generates passwords/keys

Predict that in 2-5 years US will adopt same model, but until then not useful

Whatever is used needs to be ubiquitous

This is still a hard problem

Names are not unique identifiers

Money is not in proving that you = you, but in proving certain attributes assuming you = you has been proven sufficiently.

Organizational ID can be “proven” with domain email or social network

Idea - extend that to organizations, not just people

This FB app really does come from org X, I can trust it

2 schools of thought - iPhone vs Android apps marketplace

Where does the value of this live? Person pays or organization/application pays? To whom is it more valuable?

Who is the customer? In some cases may be more valuable for RP or asserting party.

Alcohol example - if store is liable for selling to underage person, store wants to pay for certification check.

For credit/bank cards, more profitable to put through possibly invalid transactions - only brings more \$\$ to company.

In real world we do both depending on context - company pays for security clearance; you pay for your drivers license.

Some companies are doing this already to a small extent - Amazon “real name” badge, Paypal “verified seller” badge.

## About IIW Events

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

It has been one of the most effective venues for promoting and developing Web-site independent identity systems like OpenID, OAuth, and Information Cards. Past IIW events have proven to be an effective tool for building community in the Internet identity space as well as to get actual work accomplished.

The event has a unique format - the agenda is created live the day of the event. This allows for the discussion of key issues, projects and a lot of interactive opportunities with key industry leaders that are in step with this fast paced arena.

**For additional information about IIW, you can go here:**

<http://www.internetidentityworkshop.com/about/>

**To read the Values of IIW as articulated by attendees of the 11<sup>th</sup> event held in November of 2010, you can go here:**

<http://www.internetidentityworkshop.com/iw-values/>

**To read descriptions of 'what IIW is' as articulated by attendees of the 11<sup>th</sup> event held in November of 2010, you can go here:**

<http://www.internetidentityworkshop.com/what-is-iw/>

**IW #13 will be October 18 - 20, 2011 in Mountain View, California at the Computer History Museum. Registration will open in late July 2011. You can check for it here: <http://www.internetidentityworkshop.com/>**

IIW Events would not be possible without the community that gathers or the sponsors that make the gathering feasible. Sponsors of IIW #12 were:

**Ping Identity  
Microsoft  
Google  
Facebook  
Intel  
OASIS ID Trust  
Gigya  
Cisco  
Respect Network  
Yahoo!**

**IIW 2012 in Mountain View California: May 1, 2 and 3, 2012  
October 23, 24 and 25, 2012**