

Global Initiatives for Online Identity

NordSec 2009

14 October 2009

Oslo, Norway

Drummond Reed

Executive Director, Information Card Foundation
Co-Chair, OASIS XRI and XDI Tech. Committees

<http://xri.net/=drummond.reed>

We have reached a watershed
in the evolution and adoption
of open global identity
technologies

Governments have begun to recognize the benefits of adopting these technologies for citizen interaction online

This is: 1) moving the focus from technology to policy and usability, and 2) driving consolidation

This talk will:

1. Explain this new driving force for open global identity initiatives
 2. Assess the status of four open global identity protocols:
 - SAML, OpenID, Information Cards, XRI/XDI
 3. Introduce the Open Trust Framework
- Conclude by suggesting the next steps to completing an Internet identity layer

Part One:
The U.S. Government
Open Identity Solutions
Initiative

See <http://informationcard.net/white-papers/open-trust-frameworks>

Background

- Barack Obama strongly committed his administration to open government
- White House CIO Vivek Kundra instructed the U.S. CIO Council's Identity, Credential, and Access Management (ICAM) Committee to leverage open identity technologies
- In April ICAM and the U.S. General Services Admin (GSA) reached out to the OpenID and Information Card Foundations

Industry identity scheme profiles

- ICAM published an Identity Scheme Adoption Process (ISAP)
 - <http://www.idmanagement.gov/>
- Establishes the method by which ICAM will create profiles of industry-standard global identity schemes
 - SAML eGov Profile (grandfathered)
 - OpenID 2.0 Profile published August 2009
 - Information Card IMI 1.0 Profile Sept 2009

Industry trust frameworks

- ICAM published a Trust Framework Provider (TFP) Adoption Process (TFPAP)
- Establishes a method by which private industry bodies can be approved by ICAM to serve as TFPs to US gov't agencies
- Based on the four levels of assurance (LOAs) defined by NIST 800-63
- Open to any private industry organization to submit an application

OMB M04-04 and NIST 800-63

Risks	Assurance Level Impact Profiles			
	1	2	3	4
Potential Impact Categories for Authentication Errors				
Inconvenience, distress or damage to standing or reputation	Low	Mod	Mod	High
Financial loss or agency liability	Low	Mod	Mod	High
Harm to agency programs or public interests	N/A	Low	Mod	High
Unauthorized release of sensitive information	N/A	Low	Mod	High
Personal Safety	N/A	N/A	Low	Mod High
Civil or criminal violations	N/A	Low	Mod	High

Industry response

- The OpenID Foundation (OIDF) and Information Card Foundation (ICF) agreed to jointly submit a TFP
 - On Sept 9 announced the first 10 industry identity providers participating in U.S. gov't pilots at National Institute of Health (NIH)
- TFP applications also pending from
 - InCommon Federation (SAML/Shibboleth)
 - Kantara Initiative (Liberty Identity Assurance Framework)

Current status

- OI DF and ICF TFP application currently being revised to reflect their collaboration on the Open Trust Framework
 - See Part 3 of this presentation
- InCommon and Kantara applications under review
- NIH preparing to go live with OpenID and Information Card pilots
- Many other agencies in talks with NIH

Part Two: Global Identity Protocols



Market Education



**Internet
Identity
Layer**

Usability (User Experience Ceremonies)

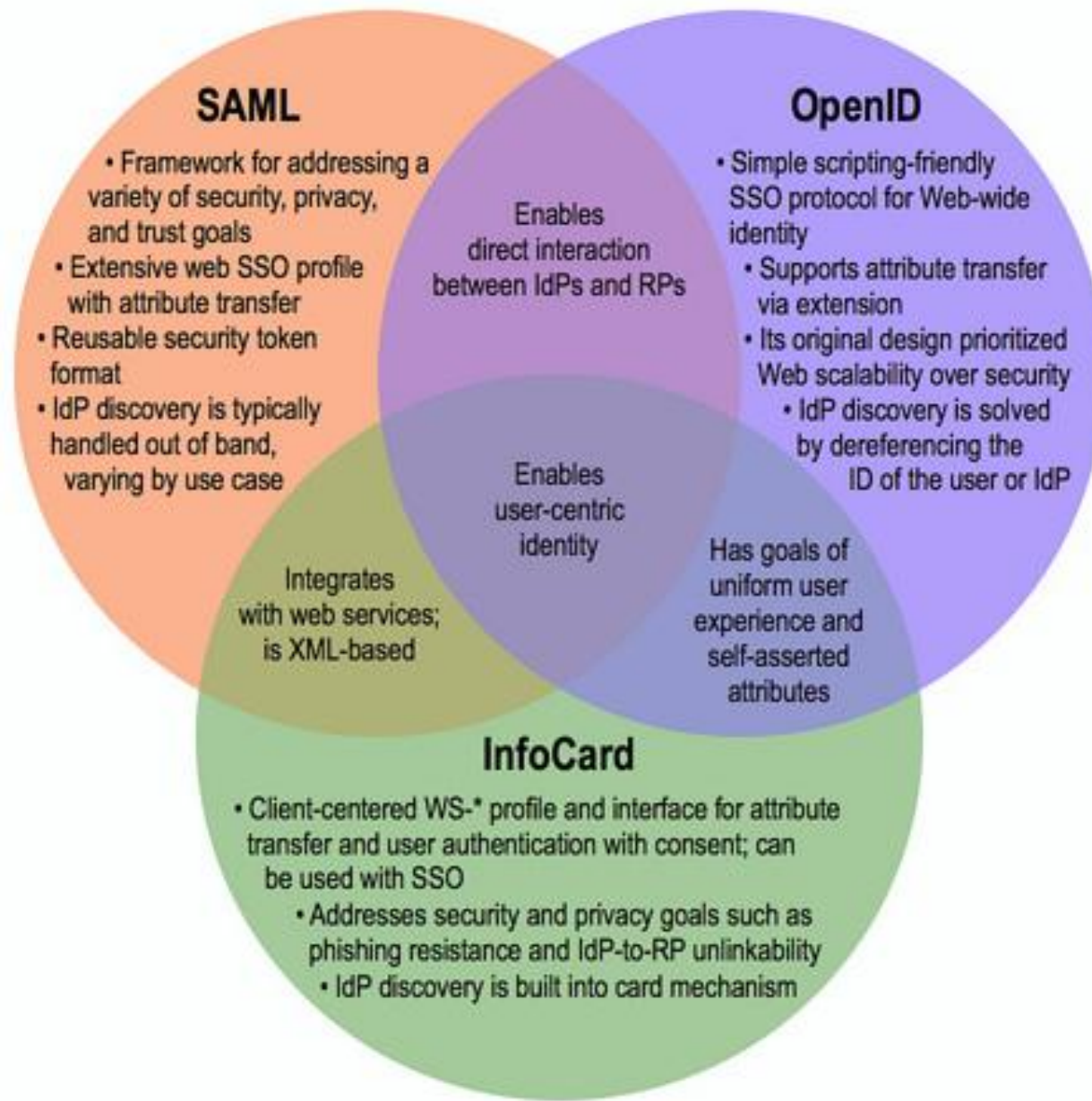
Policy Interoperability (Trust Frameworks)

Technology Interoperability (Identity Schemes)

Hardware Devices (Security Capabilities)

Overview

- 3 global identity protocols already have U.S. government identity scheme profiles
 - SAML 1.1 & 2.0 (LOAs 1 and 2)
 - OpenID 2.0 (LOA 1)
 - IMI (InfoCard) 1.0 (LOA 1, 2, and non-PKI 3)
- One is emerging but already being integrated with the above
 - XRI and XDI



Legend

IdP Identity provider
 RP Relying party
 SSO Single sign-on

The Venn of Identity

September 2009

Eve Maler – VennOfIdentity.org

Acknowledgments: Gary Ellison, Johannes Ernst, Paul Madsen, Jeff Hodges, Ashish Jain, many others

SAML

- OASIS specification
 - Stable at V2.0
 - Many profiles published including STORK
- Most widely used Internet identity token format
- Richest authentication context vocabulary
- Weakest element is IdP discovery – the WAYF (Where Are You From) problem
- Presumes out-of-band circles of trust

OpenID

- Specifications stewarded by OI DF
 - Stable at V2.0 for Authentication and SREG; Attribute Exchange (AX) 1.0 much weaker
 - Strong forces to push to 2.1 or 3.0, but great diversity of opinion about next steps
- Strengths are simplicity and IdP discovery: does NOT presume out-of-band trust
- Weakness is security and (surprisingly) user experience – the “NASCAR” problem

The OpenID “NASCAR” problem

Log in with OpenID

You're currently an **anonymous** user. Just browsing around? That's totally cool with us.

If you'd like to register, or if you've already registered, enter your OpenID:

(you will be returned to your previous location after you log in)

Alternately, click your account provider:



Don't forget to **enable OpenID support** with your preferred provider first!

Information Cards & IMI

- OASIS specification published by Identity Metasystem Interoperability (IMI) TC
- V1.0 approved as OASIS standard July 1
- Strengths
 - Strong security (a “GUI for PKI”)
 - Strong privacy
 - Does not presume out-of-band trust
 - Supports user-approved third-party claims
 - Simple, intuitive, consistent user experience for all types of claims and LOAs

Information Card weaknesses

- Requires a client-side component: the card selector
 - Must come installed (MS Vista) or be downloaded (Higgins/Azigo)
- Requires more new user education
 - Same challenge as OpenID
 - Exacerbates problem for RPs that want to support both OpenID and Information Cards

XRI (i-names and i-numbers)

- New standard for structured global identifiers
- OASIS Extensible Resource Identifier TC (2004)
- XRI 2.0 completed May 2008
 - OASIS Standard vote narrowly missed passage due to opposition from W3C TAG
- Subsequent discussions removed misconceptions and produced a redefinition of the relationship of XRIs and URIs
 - XRI 3.0 specifications should be completed by end of 2009

XDI

- New structured data sharing protocol
- OASIS XRI Data Interchange TC (2005)
- XDI 1.0 specifications still being drafted based on mature XDI RDF model
- One extensive open source implementation – XDI4J (XDI for Java) Project
 - A component of the Higgins Project
 - <http://wiki.eclipse.org/XDI4j>

The drive for consolidation

- These are all forms of representing, transferring, and verifying identity credentials
- Each has its respective design center and its particular strengths and weaknesses
- The goal now is to consolidate them under:
 - a) a layer of widely deployed trust frameworks
 - b) a unified user experience
- Only this will finally achieve mass adoption



Market Education



**Internet
Identity
Layer**

Usability (User Experience Ceremonies)

Policy Interoperability (Trust Frameworks)

Technology Interoperability (Identity Schemes)

Hardware Devices (Security Capabilities)

Part Three: The Open Trust Framework

Background

- The OIDF and ICF began collaborating to meet the U.S. gov't TFP requirements
 - 90+% of our Trust Framework Provider infrastructure would be identical
 - The only difference is the identity scheme profiles and how they can meet different security and privacy requirements
- Because OpenID and InfoCard are both open identity protocols, we also shared the need to create an *open trust framework*

Key design principles

- 1) Open to any trust community
- 2) Open to any identity provider and assessor/auditor that meets the requirements of that trust community
- 3) Open to any process for certification that meets the requirements of the trust community
- 4) Open to adaptation and evolution

Open to any trust community

- The US ICAM Trust Framework would be just the first instance of many
- Each trust framework can specify the requirements at each LOA for:
 - Identity proofing
 - Security
 - Privacy
 - Liability
 - Dispute resolution

Open to all IdPs and assessors

- The Open Trust Framework specifies
 - Global requirements for IdPs and assessors/auditors
 - Limited to universal req's for acceptable legal form, representatives, contact data, etc.
- Each trust framework instance can specify
 - Certification requirements for IdPs at each LOA
 - Qualification requirements for IdP assessors/auditors at each LOA

Open to all certification processes

- There is no “one size fits all” for IdP certification requirements
- For example, the InCommon model supports IdP self-certification followed by assessor/auditor verification
- The Open Trust Framework permits each trust community to specify its requirements (or reference others already established)

Open to adaptation and evolution

- The policy layer is the layer that most closely reflects the requirements of people and society
- We KNOW it is going to change
- Design the trust framework specification, certification, and adoption process so it can evolve and adapt to those changes
 - Example: Use URI-based references to trust frameworks and LOAs that can be versioned

A special note about privacy

- Read Bob Blakley's recent blog post:
 - <http://identityblog.burtongroup.com/bgidps/2009/10/gartner-gets-privacy-dead-wrong.html>
 - “Privacy is a social good which we *give* to one another, not a social order in which we *control* one another”
- The Open Trust Framework may do more to turn privacy into a social norm on the Internet than any technology ever could

Status

- The OIDF and ICF are actively collaborating on development of the Open Trust Framework right now
- A new white paper is being prepared for review by both boards at Internet Identity Workshop (Nov 3-5, Mountain View, CA)
- We openly invite all governments and industry experts to participate

Conclusion:
Completing the
Internet Identity Layer

Four major steps

1. Drive the necessary consolidation/interoperation of Internet identity protocols
2. Complete and implement the Open Trust Framework
3. Develop a standardized user experience for Internet identity transactions
4. Educate the market worldwide



Market Education



4

3

2

1

Usability (User Experience Ceremonies)

Policy Interoperability (Trust Frameworks)

Technology Interoperability (Identity Schemes)

Hardware Devices (Security Capabilities)

**Internet
Identity
Layer**



Thank you

Drummond Reed

<http://xri.net/=drummond.reed>

<http://informationcard.net/blog>

<http://equalsdrummond.name>

director@informationcard.net

drummond.reed@cordance.net

[Twitter and Skype: drummondreed](#)