Identity Assurance Interoperability Needs Panel

RSA April 20, 2009

Liberty Alliance & Information Card Foundation – Harnessing the Power of Digital Identity – 2009 and the Promising Road Ahead

Lena Kannappan,
Founder & CEO, FuGen Solutions, Inc.
Who am I?

- Lena Kannappan, Founder & CEO
  FuGen Solutions, Inc.
- Active Contributor, Identity Assurance Expert Group
- Editor, Contributor to SAML 2.0, ID-WSF, WS-* and IIW
- Former Chair of Identity Services Group, Liberty Alliance
- Former Chair of Web Services Convergence sub-committee
- Former Chair of Mobile Web Services, Open Mobile Alliance

What does FuGen Solutions do?

- Founded in 2006, based in Sunnyvale, CA
- IDENTITY FEDERATION EXCHANGE SERVICES provider offering SaaS-based services that include:
  - Federation On-boarding
  - Certification for Compliance
  - Federation Monitoring & Reporting
  - Federated Identity Auditing
  - Hosted Federation for SMBs
- Customers include Government, Financial and Application Service Providers
Digital Identity Management Landscape

Governments
- Government-to-Citizen
  - Taxes, loans
- Government-to-Business
  - Wage reporting, trade processes
- Government-to-Government
  - Disaster assistance and disaster response
- Internal Effectiveness and Efficiency
  - Travel, training

“SaaS” Applications
- CRM Service Provider
- HR Service Provider
- MRP Service Provider

Ecosystem of Enterprises

IdP
User Store

IdP
User Store

Consumers
- IdP
- SP
- Google
- Yahoo!
- Customs
- Passport

Information Cards
- the new way to control your personal data and identity on the web

Copyright 2006-2009 FuGen Solutions, Inc. - Confidential
Identity Assurance Needs

- Interoperable across domains
- Subject to Identity Proofing standards
- Trust levels defined
  * Minimal to High (Low to Strong Auth)
- Service assessment criteria
- Protocol agnostic
- Privacy
- Consumed by New/Emerging Federations
- Enable Inter-Federations
- Customer Convenience
- Commercially Viable
- A Source of Revenue for Certification Agents

By Context/Language of Assurance

Commercial

Identity Reliance

Family/Friends

Identity Asserted

Employers

Industry

Digital Trust Generated

Financial

Government

Institutions

People, Entities, Machines More?
Identity Assurance Definition

- Identity assurance, in an online context, is the ability for a party to determine, with some level of certainty, that an identity claim made by some entity – whether a human or a machine, with which it interacts to effect a transaction, can be trusted or actually pertain to the entity.

- In the case the entity is a person, identity assurance is the level at which the identity being claimed can be trusted to pertain to the individual making the claim, and not someone else. Identity claims can be made by presenting personally identifiable information such as name, address, birth date, etc. by presenting an acceptable form of an electronic credential.

- The level of certainty one can have about the claim is what is referred to as the "Assurance Level". Assurance Levels (ALs) are the levels of trust associated with a claim as measured by the associated technology, identity proofing processes, and policy and practice statements.
Example: Identity Assurance Levels Illustrated

Assurance level criteria as posited by the OMB M-04-04 and NIST Special Publication 800-63:

- **Level 1** – little or no confidence (e.g. registration to a news website)
  - Satisfied by a wide range of technologies, including PINs
  - Does not require use of cryptographic methods
- **Level 2** – some confidence (e.g. change of address)
  - Single-factor remote network authentication
  - Claimant must prove control of token through secure authentication protocol
- **Level 3** – high level of confidence (e.g. online access to a brokerage account)
  - Multi-factor remote network authentication
  - Tokens can be “soft”, “hard” or “one-time password”
- **Level 4** – very high level of confidence (e.g. dispensation of controlled drugs)
  - Multi-factor remote authentication through “hard” tokens
  - Cryptographic authentication
Introducing Our Panel

- Ron Carpinella, Equifax
- Colin Wallis, New Zealand Government
- Nat Sakimura, Nomura Research Institute (NRI)
- Bob Morgan, InCommon
Identity Assurance Panel
RSA Conference April 2009

Ron Carpinella, VP Identity Management

2009
I’m the other guy here…

» Vice President of Identity Management
   • Developing User Centric Identity Management Solutions

» Board Member
   • Information Card Foundation (ICF)
   • Center for Applied Identity Management Research (CAIMR)

» Founder
   • Atlanta Interactive Marketing Association
   • South Florida Interactive Marketing Association

» Formerly
   • Google, Veoh, Flycast (CMGi), Relevant Knowledge

» Education
   • Duke University (MBA), Purdue University (BA)
In the beginning,...

“On the Internet, nobody knows you’re a dog.”
...Today,...
…The Future

“On Facebook, 273 people know I’m a dog. The rest can only see my limited profile.”

“Do you remember my OpenID URI? It was either dog.pets.com, =dog, snowclone/dog, …”
Equifax’s Identity 2.0 Goals

- Identity is more than fraud prevention and mitigation
- Identity is about empowerment and engagement
- Your Identity isn’t monolithic
- Identity should be exchangeable
- Identity should be empowering
- Identity should be verifiable and secure
Equifax’s Efforts

- Identity Validation and Verification: eID
- Federated Identity Tools: Information Cards
- Identity Provider (IdP) capabilities
- Identity Relationship Tools
Identity Assurance Interoperability Needs Panel

RSA Conference 2009

Colin Wallis
Identity Standards Manager
SSC, New Zealand government

colin.wallis@ssc.govt.nz
New Zealand delegate on ISO JTC1 SC27 Working Group 5, (Identity Management)

Chair the eGov Special Interest Group at Liberty Alliance (soon to join Kantara, a consortium specializing in Identity Management)

OASIS roles: eGov Steering Committee and Security Services (SAML) and Customer Information (CIQ) Technical Committees

ITU_T and UN/CEFACT rep for my organisation
Government knows a lot about you.

- Criminal/police history
- Educational record
- Fines
- Business interests
- Property interests
- Library history
- Health record
- GP
- Test results
- Blood group
- Medicines
- Health number
- Accidents
- IRS number
- Remuneration
- Where you work
- Student loan balance
- Allowances/benefits
- Citizenship
- Passport number
- Permanent resident
- Overseas travel
- Goods imported/exported
- Life events, e.g. marriage
- Previous names
- Right to drive
- Drivers license number
- Which car you own
- Car registration
- Certificate of fitness
- Donor status
- Address
- Phone number, email
- Name
- Date of birth/age
- Place of birth
- Gender
- Marital status
- Parents
- Children/siblings
- Where you work
- Student loan balance
- Allowances/benefits
- Citizenship
- Passport number
- Permanent resident
- Overseas travel
- Goods imported/exported
- Life events, e.g. marriage
- Previous names
- Right to drive
- Drivers license number
- Which car you own
- Car registration
- Certificate of fitness
- Donor status
- Address
- Phone number, email
- Name
- Date of birth/age
- Place of birth
- Gender
- Marital status
- Parents
- Children/siblings

\[\text{STATE SERVICES COMMISSION}\]
\[\text{igovt}\]
The Industrial Age...
For the last 200 years people have had to shuffle paper documents between government agencies – **slow, expensive** for citizens and government.

The Information Age... still largely Identity 1.0 but creeping slowly towards Identity 2.0!
Replace with a metasystem of online, realtime assertions, from authoritative sources direct to where it’s needed, under the full control of the citizen – **fast, cheap** for citizens and the government.

- Birth Certificate - Internal Affairs Dept
- IRS Number
- Citizenship/Residence visa – Internal Affairs Dept
- Eligible Course - University
The igovt logon service - iLS

- Pseudonymous centralised logon service
- Identity proofing at agency from OMB M-04-04 based on service risk
- LoA determined by service risk from NIST Special Publication 800-63
- Considering Liberty Identity Assurance Framework ‘SACs’ in addition
- Supporting all the above into ISO standardization
- Contributing to the development of a global eGov Profile and vendor test plan
Identity Assurance Panel
RSA Conference April 2009

Nat Sakimura
Senior Researcher
Nomura Research Institute, Ltd.
Nat Sakimura

- Senior Researcher at Nomura Research Institute, Tokyo, Japan
- Working on “Identity” since year 2000
  - Including some government assignments on identity related issues,

- Vice Chair, XDI Public Trust Organization
- Co-Chair, OASIS Open, Open Reputation Management Systems (ORMS) TC
- Founder, OpenID Japan
- Community Board Member, OpenID Foundation

- =nat, n-sakimura@nri.co.jp, http://www.sakimura.org/
- Founder, gosoudan.com
- Founder, Marimba.org
- Plays Flute
- Loves beer, wine, sake
- Grew up in Kenya
- Etc.

My Partial Identity
Use Cases

Citizen Interacting with Government

- Asking for General but Customized Information etc.
- Asking to receive a grant, etc.
- Registering oneself, land ownership, etc.

Customers interacting with Shops

- Buying a book – contrast between OTC and the Net
  - Do you tell your name, birthday, address, credit card number, etc. when you buy a book at a bookstore?
  - I do not.

KEYWORDS

- Privacy
  - Minimum Disclosure
- Types of Identity
  - Veronym
  - Pseudonym
  - Anonymous
- Level of Assurance
- Reputation
Shop Use Case

(1) I am =alice
Want to buy prod #4356
Use Wisa for Payment
Use VPS to ship to me

(2) =alice wants to spend $120 on invoice #1435.
Authorize?

(3) Did you want to spend $120 on invoice #1435 as =alice?

(4) YES

(5) YES

(6) Deliver this parcel to =alice

(7) OK. =alice is actually =nat
So I deliver to him!

WISA

VPS

=alice

=nat
Identity Assurance: A Higher-Ed View

RL “Bob” Morgan
University of Washington
Internet2 / InCommon
Background

RL “Bob” Morgan
identity architect, University of Washington
co-leader, Internet2 Middleware Initiative
co-chair, InCommon Technical Advisory Committee
SAML, LDAP, Kerberos, Shibboleth guy

InCommon Federation
US Higher-Ed identity federation, since 2004
100 universities, 40 partners, doubling yearly
SAML-based, considering other protocols
Identity Assurance

HE IdM supports wide range of users
  faculty, staff, students, alums, affiliates, guests, medical staff, researchers, ...
  usually all in one IdM system, so need “levels”
    password policies etc based on affiliation
HE practices roughly consistent, not standardized

Interest in formal Assurance driven by US Gov
  federated access to apps at NIH, NSF at “Level 2”
  hence compliance with ... NIST 800-63? E-Auth?
InCommon Assurance Program

developed IA framework parallel to US E-Auth

Bronze, Silver == E-Auth 1, 2
compatible, but more precise, realistic, auditable ... for HE community

use the term “profiles” rather than “levels”
may be other non-ordered profiles

covers (a little) assurance of user attributes
(e.g. “is-a-student”) in addition to “identity”

uses for profiles outside of federation appearing still new, no campus has certified yet ...
The Big Issue: Cost

Cost of compliance is significant
maybe 4 FTE-months minimum, likely more?
where will auditors come from? internal?
what percentage of US HE can afford it?

Relying parties are the ones who benefit
assurance done by IdPs is work they don't have to do, so will they contribute?
will high assurance bar cause RPs/IdPs to continue with current high-cost, low-assurance account management?
Questions for the Panelists

- What is the commercial model that you would see fit?

- What are the challenges around the Identity proofing processes adopted today and what would you see as the future approach?

- Definition of levels of assurance—does this translate across protocols and what are the future needs of interoperability across multiple disparate domains or inter-federation scenarios?

- Do the current privacy laws and regulatory mandates address what’s required?