Kantara Identity Assurance Framework
Catalyzing an Identity Services Marketplace

Matthew Gardiner
President, Kantara Initiative
Director, CA Technologies
Agenda

- What is the Kantara Initiative
- Kantara Identity Assurance Framework
- Kantara Identity Assurance Certification Program
- Actions you should take
What is the Kantara Initiative?
What is the Kantara Initiative

Trustees
- BT
- CA Technologies
- Fidelity Investments
- Internet Society
- PayPal

Members
- AARP.org
- anakam
- AOL
- BIPAC
- NYC
- CSC
- Danish Biometrics Research Institute
- entr'ouvert
- Ericsson
- DataPortability Project
- T
- DMA
- Drummond Group
- HealthOhio
- E11EL
- U.S. General Services Administration
- Fugro
- FUSE
- GII
- GSA
- Helmut Broda
- HIMSS
- Identropy
- Internet
- Kantega
- Mednet
- Meristiq
- mydent
- National Notary Association
- Department of Internal Affairs
- Phase2 Healthcare
- Ping Identity
- IRIS
- SAFE-BioPharma
- Signicat
- Smart Card Alliance
- SPIKE
- SUNET
- Surescripts
- Swiss Sign
- TAS
- TENET
- The University of Washington
- UNINet
- Vivat!
- XDI.org
What is the Kantara Initiative

- Open community working on areas of common interest around identity
  - Interoperability, harmonization, certification, policy, legal & liability, privacy
  - Don’t need to be a member to participate
- ~20 working groups/discussion groups
- 2 programs
  - Assurance & Interoperability
- Small staff to help enable volunteers
Japan Work Group

Activities

- Generate best practice guidelines and suggestions for IdM standards to thrive in the Japanese market
- Translation of KI’s press releases and deliverables and other open IdM standards.
- Planning and execution of KI events in Japan
  - KI Japan WG has held 4 seminars including today

Co-chairs

- Toshihiro Suzuki, Oracle
- Yasuhisa Sakamoto, NTT
Japan Work Group (Cont’d)

- Liaison with OpenID Foundation Japan
  - OIDF-J and KI Japan WG have a good relationship since Liberty Alliance Japan SIG
Privacy & Public Policy WG

- Focused on improved privacy outcomes for users, data custodians, & others
- Define principles & best practices
- Liaise with other Kantara groups
  - Example - Identity Assurance
- Products
  - Privacy Guidance Document, Privacy Management Framework, Privacy Assurance Framework, F2F Summit Reports
Concordia Discussion Group

- **Activities**
  - Evolution of Project Concordia
  - Umbrella initiative to drive harmonization and interoperability of identity technology

- **Deliverable**
  - Draft version of “Deployment Guide for Proxying Assurance between OpenID and SAML” *1 is now open to all
  - Based on NTT & NRI’s activity which is honored as Kantara Initiative IDDY Award 2009

- **Chair**
  - Paul Madsen, NTT

Kantara Identity Assurance Framework
Catalyzing a New Marketplace

The Need
Web Identity Remains Highly Siloed
Too Much Security Burden on Users
We have the Technology
Not the Trust & Business Model

The Venn of Identity: Options and Issues in Federated Identity Management, Eve Maler & Drummond Reed, March/April 2008
Identity Ecosystem: All About Trust

End user — Credential Service Provider — Federation Operator (or) B2B CoT — Relying Parties

Relying Parties

Relying Parties

Relying Parties
Federated Identity requires Technical & Policy Interoperability

- Credential Service Provider (CSP)
  - Identity Proofing
  - Credential Lifecycle Management
  - Operational Criteria for Trust
- Relying Party (RP)
  - Assesses Risk of Application
  - Complies with Best Practices
  - Provisions the Service or Resource
- User gets great experience: safe, simple access from any device to services/resources
Certification aides technical interoperability

Interoperability Certification Program

Inventing new technologies and standards without sustained vendor certification testing is a recipe for slow and painful adoption of identity standards. Certification of interoperability of vendor implementations is critical to easing deployments in the real world.

Kantara Initiative has a goal of working collaboratively to solve harmonization and interoperability challenges among identity-enabled enterprise, Web 2.0 and Web-based applications and services. Our agile testing and certification program will help effectively accelerate adoption of new technologies and standards, helping deployers to deploy with confidence, success and minimal time and cost and vendors to incorporate standards effectively and interoperability into their offerings.

How is the Interoperability Program managed?
- The Interoperability Review Board, a Board of Trustees sub-committee provides Interoperability Program oversight.

Where does the supporting technical work happen?
- The Interoperability Work Group supports the Interoperability Program with technical input.

Where can I find the full details about the Interoperability Program?
- In the Interoperability Certification Center.

How can I apply to test my implementation?
Kantara IAF
Enables Policy Interoperability
# IAF Assurance Levels Illustrated

<table>
<thead>
<tr>
<th>Assurance Level</th>
<th>Example</th>
<th>Assessment Criteria – Organization</th>
<th>Assessment Criteria – Identity Proofing</th>
<th>Assessment Criteria – Credential Mgmt</th>
</tr>
</thead>
<tbody>
<tr>
<td>AL 1</td>
<td>Registration to a news website</td>
<td>Minimal Organizational criteria</td>
<td>Minimal criteria - Self assertion</td>
<td>PIN and Password</td>
</tr>
<tr>
<td>AL 2</td>
<td>Change of address of record by beneficiary</td>
<td>Moderate organizational criteria</td>
<td>Moderate criteria - Attestation of Govt. ID</td>
<td>Single factor; Prove control of token through authentication protocol</td>
</tr>
<tr>
<td>AL 3</td>
<td>Access to an online brokerage account</td>
<td>Stringent organizational criteria</td>
<td>Stringent criteria – stronger attestation and verification of records</td>
<td>Multi-factor auth; Cryptographic protocol; “soft”, “hard”, or “OTP” tokens</td>
</tr>
<tr>
<td>AL 4</td>
<td>Dispensation of a controlled drug or $1mm bank wire</td>
<td>Stringent organizational criteria</td>
<td>More stringent criteria – stronger attestation and verification</td>
<td>Multi-factor auth w/hard tokens only; crypto protocol w/keys bound to auth process</td>
</tr>
</tbody>
</table>

Note: Assurance level criteria as posited by the OMB M-04-04 & NIST SP 800-63
Public NIH Web Site

You are then taken to Google Using OpenID
If you click “Learn More”
Logged into NIH Web Site
Kantara Initiative’s Identity Assurance Certification Program

Catalyzing a Marketplace…
Identity Ecosystem
Making Trustworthiness Clear

End user → Credential Service Provider → Relying Parties

Assessors

Federation Operator (or) B2B CoT → Relying Parties

Relying Parties
Catalyzing a Marketplace of Identity Services
How to Scale This?

End user

Credential Service Provider

Trust Status List

Accredited Assessors List

Relying Party

Relying Party

Accredited Assessors List

End user

Credential Service Provider

Relying Party

Relying Party

Federation Operator

Relying Party
Recent collaboration with OIX

- OIX is a federation operator
- KI provides a forum to define federation policy & interoperability
- Collaboration
  - Use the Kantara IAF within the OIX program
  - Further development of Kantara IAF
  - Define & deploy a Certification Listing Service
  - Other areas
Actions you Should Take

- Spread the word & get active with the Kantara Initiative
- Auditors – Become an assessor
- CSP – Get assessed
- Federation operator/club – Adopt the framework
  - Governments are currently early adopters
- Technology provider – Get certified for interoperability
Questions