The Bridge to Assurance Communities, Governance and Technical Interoperability: A Global Context

Joni Brennan (Joni@kantarainitiative.org)
Hello!

• About Me
  • Kantara Initiative Executive Director
  • Identity Standards Development
  • Identity Assurance and Interoperability Certification
Problem Space

- Inefficient
- Does not scale
- Poor high risk solution
Agenda:

• Overview of Kantara Initiative
• Identity Assurance Framework
• Accreditation / Certification
• Next Steps
Kantara Initiative: Overview

- **Stödja Personlig Integritet | Supporting Privacy:**
  Developing solutions for secure, identity-based, privacy-respecting online interactions.

- **Bygga Förtroende | Building Trust:**
  Ensuring trusted network environments are available to support generative growth within the Internet.

- **Öppen Gemenskap | Open Community:**
  Bridging various technologies and harmonizing effective solutions related to online identity.
Technical Community Stakeholders

Focus on the **harmonization** of existing and evolving solutions.

Supporting **multiple solutions** that fit a variety of requirements and jurisdictions.
Kantara Initiative: Liaisons

- ISO: 29115, 29100, 29191, etc
- ITU-T: X.EAA, OITF
- OASIS: eGovernment, SAML SSTC, etc
- Governments: Performing confidential and non-confidential program reviews upon request for specific international governments and government agencies.
Kantara Initiative: Overview

KANTARA INITIATIVE WORK GROUPS

POLICY
- eGOV
- BCTF
- HIA
- P3
- IA WG
- InfoShare
- AM

JURISDICTION
- eGOV
- HIA WG
- JAPAN
- TELCO ID
- AM

USER-FOCUSED
- Consumer ID
- InfoShare
- UMA
- AM

WORK & DISCUSSION GROUP ACRONYMS:
- (AM) Attribute Management
- (BCTF) Business Cases for Trusted Federations
- (Consumer ID) Consumer Identity
- (eGOV) eGovernment
- (FI) Federation Interoperability
- (HIA) Heath Identity Assurance
- (IA) Identity Assurance
- (Info Sharing WG) Information Sharing
- (Japan) Japan
- (P3) Privacy and Public Policy
- (Telco ID) Telecommunication Identification
- (UMA) User Managed Access
Kantara Initiative: Overview

KANTARA INITIATIVE PROGRAMS

CERTIFICATION

INTEROPERABILITY
- Interop Review Board (IRB)
  - Certification
  - Demos

ASSURANCE
- Assurance Review Board (ARB)
  - Certification
  - Accreditation

NON-CERTIFICATION

HARMONIZATION
- User-Centric, Jurisdiction and Vertical Based

WORK & DISCUSSION GROUP ACRONYMS:

- (BCTF) Business Cases for Trusted Federation
- (eGOV) eGovernment
- (FI) Federation Interoperability
- (IOP) Interoperability
- (HIA) Health Identity Assurance
- (IA) Identity Assurance
- (Info Sharing) Information Sharing
- (OSSI) Open Source Strategic Initiative
- (P3) Privacy and Public Policy
- (Consumer ID) Consumer Identity
- (Japan) Japan
- (Telco ID) Telecommunication Identification
- (UMA) User Managed Access
Interest to Governments

Sverige: The 'E-delegationen is giving priority to a new inter-agency project in 2011. Its purpose is to facilitate information exchange between agencies, municipalities and county councils with the aim of simplifying everyday life for private individuals and businesses. http://en.edelegationen.se/report/making-progress

Canada: The Canadian Federal Government recently announced plans to create a single IT department ‘Shared Services’ that will save $100-200m a year through consolidation-driven efficiencies. http://cloudbestpractices.net/2011/08/08/canadian-community-cloud/

Higher Education Leads Way

- EduGain
  http://www.geant.net/service/edugain/FAQs/Pages/FAQs.aspx

- InCommon
  http://www.incommon.org/about.html

- Kalmar2
  http://www.kalmar2.org/kalmar2web/front_page.html

- SWAMID
  http://www.swamid.se/11/faq.html
Leveraging Scale-Free Networks

“Inter-Federation”
## Levels of Assurance: 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
Trust Framework Model

- Registration
- Assessment
- Certification Process
- Interested Parties
- Trust Status Listing Service
Identity Assurance Framework: Actors

**KANTARA INITIATIVE IAF**

**ASSESSORS**
- Get accredited by Kantara as an assessor against the IAF 1600 AQR
- Leverage demonstrable competencies to expedite certification

**CREDENTIAL SERVICE PROVIDERS**
- Get assessed by a Kantara Accredited Assessor for IAF certification against the IAF 1400 SACs
- Submit certification application to Kantara’s Assurance Review Board (ARB)
- Obtain and maintain compliance and certification

**FEDERATION OPERATORS**
- Define criteria for identity assurance for their federation
- Map policy against IAF SAC and IAF profiles
- Accept or recommend IAF certification to its constituents

**IDENTITY ASSURANCE FRAMEWORK 2.0 MAP**

**NON-NORMATIVE:**
- (IAF 1000) Overview
- (IAF 1100) Glossary
- (IAF 1200) Assurance Levels

**NORMATIVE:**
- (IAF 1300) Assurance Assessment Scheme
- (IAF 1400) Service Assessment Criteria
- (IAF 1600) Assessor Qualifications & Requirements

http://kantarainitiative.org/confluence/x/e4R7Ag
Kantara Trust Framework

Board of Trustees

Assurance Review Board (ARB)

Identity Assurance Work Group (IAWG)

Identity Assurance Framework (IAF)

Assurance Assessment Scheme (AAS)

Assessor Qualifications & Requirements (AQR)

Service Assessment Criteria (SAC)

Trust Status Published to:

Reviews & Verifies External Assessment

Manages the Set of IAF Documents

Complete Set of IAF Documents

Core IAF Document Set
Kantara Trust Framework

Board of Trustees

Assurance Review Board (ARB)

Identity Assurance Work Group (IAWG)

Identity Assurance Framework (IAF)

Assurance Assessment Scheme (AAS)

Assessor Qualifications & Requirements (AQR)

Service Assessment Criteria (SAC)

Trust Status Published to:

Reviews & Verifies External Assessment

Manages the Set of IAF Documents

Complete Set of IAF Documents

Core IAF Document Set
Multiple Trust Frameworks

- Technical
  - SAML
  - OpenID
  - OAuth

- Verticals
  - Social Networks
  - Healthcare
  - Banking

- Jurisdictions
  - National Governments
  - Local Governments

+ Others
Trust Framework Profiles

- Core Framework
  - Common, Well-Vetted Foundation
- Technical Profile
  - Complete Assessment Criteria
  - Specific Technical Deployment Rules
- Privacy Profile
  - Specific Policy / Regulation Rules
- Final Framework
Collaboration is Key

**Kantara Initiative**

- Accredits Assessors and Certifies IdPs against Identity Assurance Framework Policy
- US Federal ICAM LoA 1, 2, 3
- Identity Assurance WG (IAWG) manages IAF and enables IAF Profile development; develops Federal Operator Guidelines
- Federation Interoperability WG (FIWG) develops technical tools enabling federations to communicate certification meta-data
- Privacy and Public Policy WG (P3WG) supports development of Levels of Protection

**Open Identity Exchange**

- "Open Market Model"
- Technology-agnostic, internet utility for identity federation meta-data
- Technology Platform for:
  - global certification listings
  - trans-federation operational meta-data
  - automated attribute exchanges
- Developing legal structures for Levels of Assurance
- Development of the OIX Trust Wiki "model" term sheets/contracts for Trust Framework actors and services
- Adopting FIWG technical tools for automated certification listings

**Kantara Initiative Work Groups**

**Open Identity Exchange Work Groups**
Building on the Core

- **Privacy Assurance:** Building upon the Kantara US Federal Privacy Profile the Privacy and Public Policy (P3) WG will build Privacy Assessment Criteria (PAC) for audit controls applied in a Privacy Assessment.

- **Attribute Management Assurance:** Recently formed AM group is in process of discovery and gap analysis for next steps to Attribute Management

- **Relying Party Guidelines:** Identity Assurance WG focusing in on areas of Relying Party concern and engagement.
Benefits to Adoption

**Cost Savings**
- As Federated networks adopt IAF cost savings will be greater for organizations certified against IAF.
- Federation Operators reduce their cost in defining and maintaining Identity Assurance policies and practices, thus reducing cost for constituents as well.

**Business Agility**
- An organization is able to join other IAF networks faster and more efficiently.
- The ability to inter-federate is an added value to each IAF certified service and their respective subscribers.

**A Higher Standard**
- Best of breed cross-industry standard that reflects the best known practices from a substantial cross-section of industry and government. It benefits from a large and deep pool of contributors not available in any single federated network.
- Over time IAF will cross-pollenate other networks providing a consistently higher standard for Identity Assurance.
Status and Lessons Learned

• **Status:**
  - Operational SAML Framework
  - Operational Organization
  - Approved for US Government Use through LOA 3
  - Referenced by eGov communities including Canada, New Zealand, Sweden
  - First Assessments Underway
  - International Partners

• **Lessons Learned So Far:**
  - Need Additional Members, Participants, and Customers
  - Need Additional Technical Frameworks
  - Need Additional Levels of Assurance
  - Need Additional Privacy Profiles
Shaping the Future of Digital Identity

- **Kantara Initiative Website:**
  - http://kantarainitiative.org

- **Community Mail List:**
  - http://kantarainitiative.org/listinfo/community

- **Assurance Certification Center:**
  - http://kantarainitiative.org/confluence/x/EYCYAQ

- **Membership Documents:**
  - http://kantarainitiative.org/wordpress/membership/
Questions?

• Kantara Executive Director: Joni Brennan (joni@kantarainitiative.org)