Trust Frameworks: Tools to build Identity Ecosystems

*It takes a village*

support@kantarainitiative.org
Agenda:

• Overview of Kantara Initiative
• Federation and Trust Frameworks
• Identity Assurance Framework
• Accreditation / Certification
• Next Steps
Kantara Initiative: Overview

Values

• **Trust:**
  
  *Operating Accreditation, Approval and Certification programs* to ensure trusted network environments are available to support generative growth within the Internet.

• **Privacy:**
  
  *Developing solutions* for secure, identity-based, privacy-respecting online interactions.

• **Community:**
  
  *Bridging technologies and policies* to harmonize effective solutions related to online identity.
Kantara Initiative: Overview
Federation, Compliance, and Interoperability

Focus on the harmonization of existing and evolving solutions.

Operating compliance programs for multiple solutions that fit a variety of requirements and jurisdictions.
Kantara Initiative: Overview
Governance Model

Board of Trustees

Assurance Review Board
Interoperability Review Board
Operates Compliance Programs

Leadership Council
Consists of: Work and Discussion Group Leadership
Develops Requirements and Practices
Kantara Initiative: Overview
Liaisons and Governments

- ISO: 29115, 29100, 29191, 27001, 27002, etc
- ITU-T: X.1254 (was X.EAA), OITF
- OASIS: eGovernment, SAML SSTC, etc
- OECD Internet Technical Advisory Committee (ITAC)

Governments:

- Providing neutral forum for Government Programs and Agencies to share information and identify common goals
- Performing confidential and non-confidential program reviews upon request for specific international governments and government agencies
Kantara Initiative: Overview
Work and Discussion Groups

KANTARA INITIATIVE WORK AND DISCUSSION GROUPS

POLICY

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

JURISDICTION

- eGOV
- HIA
- JAPAN
- TELCO ID
- AM

USER-FOCUSED

- Consumer ID
- InfoShare
- UMA

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
Groups and Programs

KANTARA INITIATIVE PROGRAMS

COMPLIANCE and CERTIFICATION

INTEROPERABILITY
Interop Review Board (IRB)
• Certification, Verification
• Tools, Demos

ASSURANCE
Assurance Review Board (ARB)
• Certification
• Accreditation

HARMONIZATION
User-Centric, Jurisdiction and Vertical Based

NON-CERTIFICATION

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

2012 Kantara Initiative - Trust Frameworks: A Global Context 9
What is good?

- Strengthening communities
- Opening of new markets
- Enhanced privacy for end users
- More and better services to the users
- Re-use of user names and passwords

Federation and Trust Frameworks

What is bad?

- Lingua franca for inter-federation? SAML2?
- How to announce new services?
- Legal stuff...

What is ugly?

- Identity-management requirements
- Semantics
- SAML2 interoperation profiles (saml2int.org) no longer 'just' Shibboleth

Federation and Trust Frameworks
What does Federation look like?

Hub-and-spoke, central login

Services

Institutions

Federation and Trust Frameworks
What does Federation look like?

“Inter-Federation”
Target Audience

- Enable **End-users (Enterprise, Governments, Communities)** to **trust** credentials issued by **Identity Providers / Credential Service Providers**

Value Proposition

- Increased security
- Compliance with laws, regulations, and standards
- Improved interoperability
- Enhanced customer service
- Elimination of redundancy
- Increase in protection of Personally Identifiable Information (PII)
### Federation and Trust Frameworks
#### 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

- Assessment
- Registration
- Trust Status Listing Service
- Interested Parties
- Certification Process
- Trust Status Listing Service, Registry, White List

Kantara Initiative - Trust Frameworks: A Global Context
Identity Assurance Framework: Documents

**Note:** A Trust Framework may apply specific profiles for specific Technology and Privacy Constraints used to achieve Levels of Assurance.

- **IAF 1000 - Overview**
  Overview of the IAF documents and structure

- **IAF 1100 - Glossary**
  Glossary of terms used in the IAF documents

- **IAF 1200 – Levels of Assurance**
  Overview in detail of the Levels of Assurance

- **IAF 1300 – Assurance Assessment Scheme**
  Process of how the Assurance Program operates

- **IAF 1400 – Service Assessment Scheme**
  Criteria that a Service will need to provide compliance to for Service Approval at the different Levels of Assurance

- **IAF 1600 – Assessor Qualifications and Requirements**
  Qualifications that an Assessor must prove to become Accredited to perform IAF assessments
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

2012 Kantara Initiative - Trust Frameworks: A Global Context
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:

List Services, Registries, Whitelists

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
Kantara Trust Framework: Progress

Kantara Accredited to LoA 1-4

Deloitte.

Electrosoft
IT Security Solutions and Compliance

eValid8 Corporation

Kantara Approved to LoA 3 non-crypto

Verizon Universal Identity Service (VUIS)*
* ICAM Trust Framework Approval

Registered Applicants

• Accreditation:
  - europoint
  - Zygma

• Service Approval:
  - Experian™
• **Identity Assurance:**
  Building in service module approach enabling Identity Proofing, Credential Management and Organizational component assessments

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

• **Attribute Management (AM) Assurance:**
  Performed landscape review of varying AM standards and development activities in Identity focused communities
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
  • Assessments in progress
  • 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/
Thanks!

Questions?

• Kantara Executive Director: Joni Brennan joni @ kantarainitiative.org
• General Inquiries: support @ kantarainitiative.org