Identity Assurance Framework: Realizing The Identity Opportunity With Consistency And Definition

Sept. 8, 2008
Liberty Alliance
Welcome!

- Introduction of speakers
- Introduction of attendees
  - Your organization’s interest in identity assurance
  - What do you want to learn today?
- Goals for the session
Introduction of the Identity Assurance Framework

Defining the framework and its goals

Peter Alterman
GSA
IAEG Charter

- Formed August 2007 to develop a **global standard** framework and necessary support programs for validating trusted **identity assurance** service providers in a way that scales, empowers business processes and benefits individual users of identity assurance services.

- Move beyond pure policy development and into **development of actionable and measurable programs** including certification education, awareness and broad market promotion.

- Provide public and private organizations with a **uniform means of relying on digital credentials** issued by a variety of providers in order to **advance trusted identity federation** and thereby **facilitate access to online services and information**.

- First version of the **IAF specification** was officially released and published June 22, 2008.

- **Certification program** will be available by end 2008.
Identity Assurance Framework

- **What is it?**
  - Framework supporting mutual acceptance, validation and lifecycle maintenance across identity federations
  - EAP Trust Framework and US e-Authentication Federation Credential Assessment Framework as baseline
  - Harmonized, best-of-breed industry identity assurance standard
    - Identity credential policy
    - Business procedure and rule set
    - Baseline commercial terms
  - Guideline to foster inter-federation on a global scale

- **It consists of 4 parts:**
  - Assurance Levels
  - Service Assessment Criteria
  - Accreditation and Certification Model
  - Business Rules
The IAF Ecosystem

- Accredited Assessors List
- IAF’s Initial Focus
- Federated Network
- Relying Parties (Applications)
- End user (subscriber)
- Network Operator
- Federated Identity
- Credential Service Provider
**IAF Assurance Levels**

- **Definition**: Level of trust associated with a credential measured by the strength and rigor of the identity-proofing process, the inherent strength of the credential and the policy and practice statements employed by the Credential Service Provider (CSP).

- **Four Primary Levels of Assurance**
  - Level 1 – little or no confidence in asserted identity’s validity
  - Level 2 – Some confidence
  - Level 3 – Significant level of confidence
  - Level 4 – Very high level of confidence

- **Use of Assurance Level**: is determined by level of authentication necessary to mitigate risk in the transaction, as determined by the Relying Party.

- **CSPs are certified by Federation Operators to a specific Level(s)**
### 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 and NIST Special Publication 800-63
IAF Service Assessment Criteria (SAC)

The SAC is how the framework materializes in practice

- **3 SAC areas:**
  - Common Organization - The general business and organizational conformity of services and their providers
  - Identity Proofing - The functional conformity of identity proofing services
  - Credential Management - The functional conformity of credential management services and their providers
IAF Certification / Accreditation Model

- **High-level Description**
  - Program for assessors to become accredited
  - Provide candidate CSPs with guidelines for certifying against IAF
  - Enables Federation operators to certify members against IAF
  - Liberty Alliance to provide governance over accreditation process
  - Phase one certification process for CPSs defined in Framework

- **Accreditation Program is current focus**
  - Opportunity to contribute and collaborate
  - Planned availability by end of 2008, if not sooner!
IAF Business Rules

- Focused on the use of credentials for authentication, initially targeting CSPs
- Liberty Alliance provides accreditation of assessors who will perform certification assessment
- Federation Operators will require Liberty-accredited assessments
- Provides guidelines for how all involved parties (relying parties, CSPs and Federation Operators) may work together
- Liberty Alliance will maintain the Identity Assurance Framework and provide a current list of accredited assessors
Questions?
Identity Assurance Accreditation

Frank Villavicencio
Citigroup Global Transaction Services
As presented, Liberty Alliance has developed and published an Identity Assurance Framework (IAF)

An IAF operational governance model for deployment needed to be created
  - Including standards for assessment of credential issuers and consumers
  - Accreditation of assessors

An accreditation and certification model must co-exist with existing controls programs
Accreditation Goals

- Standards conformity
  - Certification by any authority has equivalence to the four defined assurance levels
- Broad adoption
  - Not specific to any business model
  - Not geographically aligned
- Leverages existing control frameworks
Value Proposition

- **For Assessors**
  - Business opportunities in new digital identity realm
  - Deepen relationship with existing clients
- **For Credential Issuers**
  - Reduces/Eliminates need for unique and “one-off” assessments by credential consumers
  - Makes identity services more marketable
- **For Credential Consumers**
  - Creates a level playing field for an identity marketplace
  - Reduces/eliminates need to assess issuers
Liberty Accreditation Model

- **Pre-requisites for recognition**
  - Must hold accreditation from national accreditation body (UKAS, AICPA/CICA, EA, ANAB/Int’l Accreditation Forum)
  - Experience w/ ISO 27001 general controls review
  - Experience w/ Web Trust, or similar specific controls review
  - Familiarity w/ assessment provisions outlined in ISO 19011
  - Completion of Liberty-sponsored IAF expertise online exam

- **Required Documentation**
  - Application for Accreditation
  - Qualification Document

- **Annual re-accreditation**
Assessor Accreditation Process

- Submit application for accreditation designation to Liberty
- Submit Qualification Document for review and approval by Liberty
  - Qualifications/assessments vary by Assurance Level
- Register designated expert resources for Liberty-sponsored, online IAF compliance exam
- Successfully complete exam
- Sign Liberty Trademark License Agreement
- Annual re-accreditation
  - Onsite assessment not required
Accreditation Process Flow

Accredited Assessor

Submits application with pre-requisite information to IAEG

Complete Qualification Doc.

IAEG

Appeal

Direct Assessor to sample required documents

Federation Operator

Submit required documents to Liberty

IAEG reviews materials

Yes

No

Complete Application?

Approve Assessor App.

Pass

Fail

Apply Accredited Assessor designation

Acknowledge IAEG-accredited Assessors

Credential Service Provider

Request certification assessments from only IAEG-accredited Assessors
<table>
<thead>
<tr>
<th><strong>Ongoing Participant Checklist</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Assessor</strong></td>
</tr>
<tr>
<td>• Application submission</td>
</tr>
<tr>
<td>• Provide pre-requisite information</td>
</tr>
<tr>
<td>• Designate resources for examination</td>
</tr>
<tr>
<td><strong>Liberty</strong></td>
</tr>
<tr>
<td>• Support Application process</td>
</tr>
<tr>
<td>• Draft sample accreditation material</td>
</tr>
<tr>
<td>• Provide updated Assessor list</td>
</tr>
<tr>
<td><strong>CSP</strong></td>
</tr>
<tr>
<td>• Identify IAEG-accredited Assessors</td>
</tr>
<tr>
<td>• Request IAEG certification</td>
</tr>
<tr>
<td>• Provide assessment from IAEG-accredited body to Federation Operator(s)</td>
</tr>
<tr>
<td><strong>FO</strong></td>
</tr>
<tr>
<td>• Acknowledge IAEG-accredited Assessors</td>
</tr>
<tr>
<td>• Request only CSP assessments by IAEG-accredited Assessors for IAEG certification</td>
</tr>
<tr>
<td>• Provide ongoing list of IAEG-certified CSPs to Liberty</td>
</tr>
<tr>
<td><strong>RP</strong></td>
</tr>
<tr>
<td>• Establish acceptance policies with respect to IAEG-certified CSPs</td>
</tr>
<tr>
<td>• Officially acknowledge Federations to which they subscribe</td>
</tr>
<tr>
<td>• Sign Trademark License Agreement</td>
</tr>
<tr>
<td>• Annual re-accreditation</td>
</tr>
<tr>
<td>• Maintain list of participating CSPs and Federations</td>
</tr>
<tr>
<td>• Maintain currency of IAF and Accreditation program</td>
</tr>
<tr>
<td>• Publish and maintain Operating document</td>
</tr>
</tbody>
</table>
Implementation Roadmap

1. Industry Analysis
   - Analysis of existing accreditation programs
   - Research standards bodies’ existing programs

2. Process Design
   - Identify business model
   - Create process flow diagram
   - Identify roles and responsibilities
   - Write process checklist
   - Develop IAEG development checklist

3. Development
   - Write Assessor Application
   - Draft sample documents
   - Develop online exam
   - Draft Operating document
   - Draft TMLA
   - Create sub-committee

4. Validation
   - Publish process for review with feedback gathering
   - Stakeholder approval
   - Liberty Board approval
   - Plan for official launch
   - Identify initial candidate

5. Launch
   - Post application and sample docs on site
   - Press release
   - Analyst “road” show
   - Engage feedback process
   - Maintain currency of IAF and Accreditation program
   - First assessor accredited

Outside Consulting
Input from IA EG and SIG
Liberty Infrastructure
Questions?
Planning for the Future

Peter Alterman, GSA
and
Frank Villavicencio,
Citigroup Global Transaction Services
Roadmap

- Launch Accreditation Program to accompany the Certification Program
  - Available by end of 2008
- Scope and define Phases 2 and 3 for Relying Parties and Federation Operators
- Refine Service Assessment Criteria (SAC) introduced in IAF document
  - SAC Development
    - Process for reviewing and approving new criteria to keep up with technological advances
    - SAC Requirements Matrix
- Mapping project
  - IAF and US Government e-Authentication Credential Assessment Framework & NIST Special Publication 800-63 to streamline government adoption
  - Complete by Oct. 2008
Roadmap (cont.)

- Work with the ITU-T
- Expansion to RP focus?
- Others?
  - Group discussion on where your priorities are→
For More Information

- Visit our site: http://projectliberty.org/liberty/strategic_initiatives/identity_assurance
- Get involved with the public Identity Assurance Special Interest Group: http://wiki.projectliberty.org/index.php/IASIG
- Contact Frank Villavicencio (frank.villavicencio@citi.com) or Peter Alterman (peter.alterman@gsa.gov)
- Attend kick off keynote session for DIDW featuring Identity Assurance panel
Thank You