Introduction of the Identity Assurance Framework

Defining the framework and its goals
IAEG Charter

- Formed in August of 07 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.

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

IAF’s Initial Focus

Accredited Assessors List

Credential Service Provider

Assessor

Network Operator

Federated Network

Relying Parties (Applications)

Identity Credentials

End user (subscriber)

Authentication Technology Vendors

Federated Identity

IAF’s Initial Focus

Credential Service Provider

Assessor

Network Operator

Federated Network

Relying Parties (Applications)

Identity Credentials

End user (subscriber)

Authentication Technology Vendors

Federated Identity

IAF’s Initial Focus

Credential Service Provider

Assessor

Network Operator

Federated Network

Relying Parties (Applications)

Identity Credentials

End user (subscriber)

Authentication Technology Vendors

Federated Identity

IAF’s Initial Focus

Credential Service Provider

Assessor

Network Operator

Federated Network

Relying Parties (Applications)

Identity Credentials

End user (subscriber)

Authentication Technology Vendors

Federated Identity

IAF’s Initial Focus

Credential Service Provider

Assessor

Network Operator

Federated Network

Relying Parties (Applications)

Identity Credentials

End user (subscriber)

Authentication Technology Vendors

Federated Identity

IAF’s Initial Focus

Credential Service Provider

Assessor

Network Operator

Federated Network

Relying Parties (Applications)

Identity Credentials

End user (subscriber)

Authentication Technology Vendors

Federated Identity

IAF’s Initial Focus

Credential Service Provider

Assessor

Network Operator

Federated Network

Relying Parties (Applications)

Identity Credentials

End user (subscriber)

Authentication Technology Vendors

Federated Identity

IAF’s Initial Focus

Credential Service Provider

Assessor

Network Operator

Federated Network

Relying Parties (Applications)

Identity Credentials

End user (subscriber)

Authentication Technology Vendors

Federated Identity

IAF’s Initial Focus

Credential Service Provider

Assessor

Network Operator

Federated Network

Relying Parties (Applications)

Identity Credentials

End user (subscriber)

Authentication Technology Vendors

Federated Identity

IAF’s Initial Focus

Credential Service Provider

Assessor

Network Operator

Federated Network

Relying Parties (Applications)

Identity Credentials

End user (subscriber)

Authentication Technology Vendors

Federated Identity

IAF’s Initial Focus

Credential Service Provider

Assessor

Network Operator

Federated Network

Relying Parties (Applications)
**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 – High 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 IAEG’s current focus**
  - Opportunity to contribute and collaborate
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
Roadmap

- Launch Accreditation Program to accompany the Certification Program
- 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
  - SAC Maintenance
    - Process by which IAEG maintains the currency of criteria
Questions?