Real World Identity Assurance: Wells Fargo Demonstration of Identity Assurance Principles In Action

August 6, 2008
Jim Gross
Senior Vice President, Wells Fargo
WellsSecure® Trusted Identity Service
The General Ecology

Getting more complex all the time …
Why Do They Have To Be So Difficult ... Can't They Just Learn To Get Along?

My 2.0 Agents

Buying Stuff

Getting In The Door

Always With Me
It Takes Two To Tango

Interoperable Hardware, Code and Network Specs.

Interoperable Business Policy, Rules and Contractual Framework

Common Identity Assurance “Drive Train” Across The Identity Ecology

Gangly Adolescent

Young Adult

Our Focus Today
Identity Assurance Is The Key Business Driver

- **Standard, broadly accepted Levels of Assurance** allow relying parties (or their agents) to readily determine, on the fly, their confidence in an identity credential
  
  - Desired results are:
    - **Less complex/more rapid deployment** of digital identity services
    - Operational streamlining of identity service provider certification/accreditation processes for entire industry

- **Liberty Alliance IAF (Identity Assurance Framework)**
  
  - Objective is to create a framework of baseline policies, business rules and commercial terms against which identity assurance services can be assessed and certified

  - Check out the public draft (for comment) at: http://www.projectliberty.org/resource_center/specifications/liberty_alliance_identity_assurance_framework_iaf_1_1_specification
Liberty Focus

- Technology Standards and Guidelines
- Business and Privacy Guidelines
- An Ecosystem of Interoperable Products & Services
- Identity Assurance Framework & Assessors

Assurance
Liberty’s Global Membership

150 diverse member companies and organizations representing leaders in IT, mobility, government, service provision, system integration and finance working collaboratively to address the technology, business and policy aspects of digital identity management

Management Board

Sponsors
IAF Assurance Level Policy Overview

- Level of trust is associated with the strength and rigor of the identity-proofing policy and practices statements joined to an identity credential.

- **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 Relying Party risk and the level of authentication rigor necessary to mitigate a given risk(s).

- CSP’s (Credential Service Providers) are certified by Federation Operators to offer services at the given assurance level(s).
## Assurance Level Criteria Overview

<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>
How IAF Certification Will Unfold

- Initially focused on the use of credentials for authentication, targeting CSP’s (Credential Service Providers)
- Liberty Alliance (LAP) provides accreditation of assessors who will perform certification assessment
- Federation Operators will require LAP-accredited assessments
- Provides guidelines for how all involved parties (relying parties, CSP’s and Federation Operators) may work together
- LAP will maintain the Identity Assurance Framework and provide a current list of accredited assessors

With the IAF in final draft, development of the assessment and assessor accreditation programs is the Liberty Identity Assurance Expect Group’s top 2008 priority
Identity Assurance Principles
In Action:
Use Cases
Use Case: Annuity Funds Transfer

- Initiation/transfer of $XXMM from demand deposit account to third party annuity product provider
  - Basic customer financial institution requirement: customer authentication onto network and application in order to submit request. *Existing tools satisfy requirement.*
  
  - Further requirement: customer authorization to submit request. *Existing tools partially satisfy requirement.*
  
  - But, do both the financial institution and the third party have high assurance that the identity credential submitted can *non-repudiably* represent the customer and other dependent parties? *IAF framework and supporting network deliver this capability.*
Identity Assurance Use Case: Physical Access

- Physical access to storage facility containing negotiable documents
  - Facility maintains directory of identities authorized to enter
  - Person x is authorized to enter, but does not have a facility access card to allow authorized entry
  - Person x does holds a payment card that also holds a high assurance identity credential
  - Person x can be authorized to enter without further effort via assurance level match
Identity Assurance Use Case: First Responders

Identity Infrastructure
Personal Identifiable Information (PII) Retained

- Federal HSPD-12
- State/Local
- Private Sector FRAC

Attribute Infrastructure
No PII Retained

- Web-based Public CRLs
- FEMA Attribute Repository
- Trusted Attributes
- Consolidated Information = PIV Auth Cert + Electronic Attribute

Validation Infrastructure
Validated Information Retained

Key:
- AHJ - Authority Having Jurisdiction
- CRLs - Certificate Revocation Lists
- FRAC - First Responder Authentication Credential
- PIV Auth Cert – FIPS 201 Personal ID Verification Authorization Certificate

"Standardized FIPS 201 Credential & Attribute Validation Process"

For Official Use Only (FOUO)
Graphic and content courtesy of Tom Lockwood, DHS
Real World Identity Assurance Use Case/Deployment

- US Federal: GSA eOffer procurement site acceptance of federated WellsSecure® certificates
Contact Information

Jim Gross
Senior Vice President
Wells Fargo
One Front Street
MAC A0195-204
20th Floor
San Francisco, CA
V: (415) 222-5007
F: (415) 788-3039
jgross@wellsfargo.com