

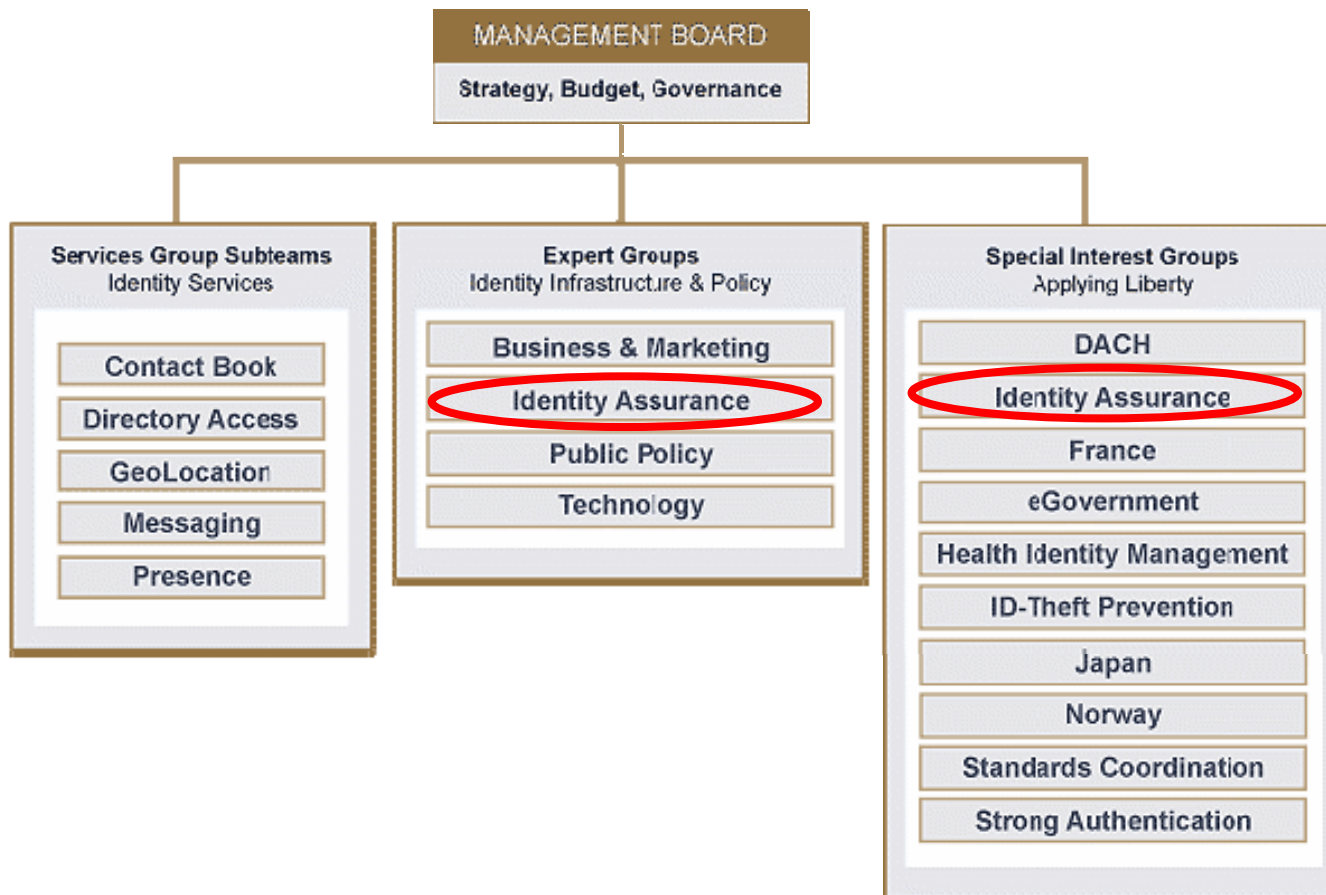
# Introduction of the Identity Assurance Framework

**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

# Focus on Identity Assurance



## IAEG Focus

- ✓ Help shape identity assurance policy for both public and private sectors
- ✓ Expand markets by promoting wider use of identity credentials
- ✓ Stay abreast of government policy worldwide that will have an impact on identity assurance
- ✓ Discuss the latest technology, standards, and solutions in the e-authentication and identity assurance industry with your peers
- ✓ Get to know public and private sector leaders in e-authentication and identity assurance
- ✓ Help streamline and accelerate implementation of identity federations
- ✓ Contribute and help shape the Identity Assurance Framework as it evolves
- ✓ Avoid “re-inventing the wheel” or needlessly duplicating effort by identifying best practices across multiple industry sectors in this globally diverse working group

# 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 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

Assurance Level	Example	Assessment Criteria – Organization	Assessment Criteria – Identity Proofing	Assessment Criteria – Credential Mgmt
AL 1	Registration to a news website	Minimal Organizational criteria	Minimal criteria - Self assertion	PIN and Password
AL 2	Change of address of record by beneficiary	Moderate organizational criteria	Moderate criteria - Attestation of Govt. ID	Single factor; Prove control of token through authentication protocol
AL 3	Access to an online brokerage account	Stringent organizational criteria	Stringent criteria – stronger attestation and verification of records	Multi-factor auth; Cryptographic protocol; “soft”, “hard”, or “OTP” tokens
AL 4	Dispensation of a controlled drug or \$1mm bank wire	Stringent organizational criteria	More stringent criteria – stronger attestation and verification	Multi-factor auth w/hard tokens only; crypto protocol w/keys bound to auth process

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 CSPs defined in Framework
  
- **More details later on today...**

# 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

- Finalize Phase One of Certification Program for CSPs, introduced in Framework
- 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

# Reference Documents

- **EAP Trust Framework:**  
[http://eap.projectliberty.org/docs/Trust\\_Framework\\_010605\\_final.pdf](http://eap.projectliberty.org/docs/Trust_Framework_010605_final.pdf)
- **OMB e-Authentication Guidance (OMB M-04-04):**  
<http://www.whitehouse.gov/omb/memoranda/fy04/m04-04.pdf>
- **NIST Special Publication 800-63 Version 1.0.1: NIST Special Publication 800-63 Version 1.0.1:** [http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1\\_0\\_2.pdf](http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1_0_2.pdf)
- **Authentication Service Component Interface Specifications:**  
<http://www.cio.gov/eauthentication/documents/TechApproach.pdf>
- **GSA Credential Assessment Framework, Password CAP, Certificate CAP and Entropy Spreadsheet:**  
<http://www.cio.gov/eauthentication/documents/PasswordCAP.pdf>
- **Tscheme**  
<http://www.tscheme.org/profiles/index.html>
- **TSCP**  
<http://tscp.org/about.htm>



# Questions?