Identity Assurance Framework: Advancing the Marketplace

Russ Cutler, Editor of the Identity Assurance Framework
Jim Gross, Senior Vice President, Wells Fargo
Jane Hennessy, Senior Vice President, Wells Fargo
Brett McDowell, Executive Director, Liberty Alliance
Roger Sullivan, President of the Liberty Alliance Management Board and Vice President of Oracle Identity Management

Welcome

- **Liberty Alliance**

www.projectliberty.org

- **Identity Assurance Special Interest Group**
(formal membership in Liberty Alliance is not required)

http://wiki.projectliberty.org/index.php/IASIG

- **Identity Assurance Framework for Review and Comment**

http://www.projectliberty.org/liberty/content/download/3736/24651/file/liberty-identity-assurance-framework-v1.0.pdf

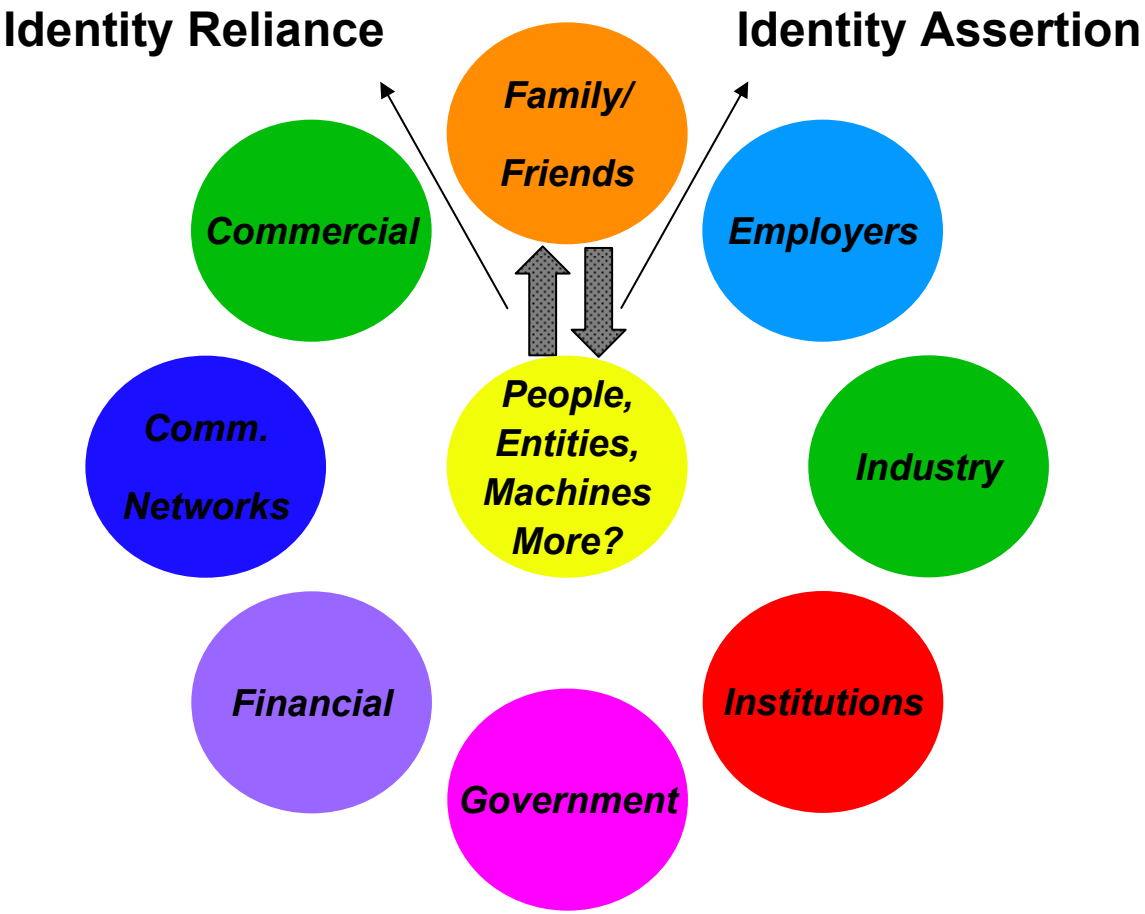
Agenda

- Current Marketplace Situation: Need for an Identity Assurance Framework
- Marketplace Ecology Review
- Why Liberty Alliance: Formation of Identity Assurance Expert Group
- Identity Assurance Framework Review
- Next Steps
- Obtain Your Feedback

What's the Problem

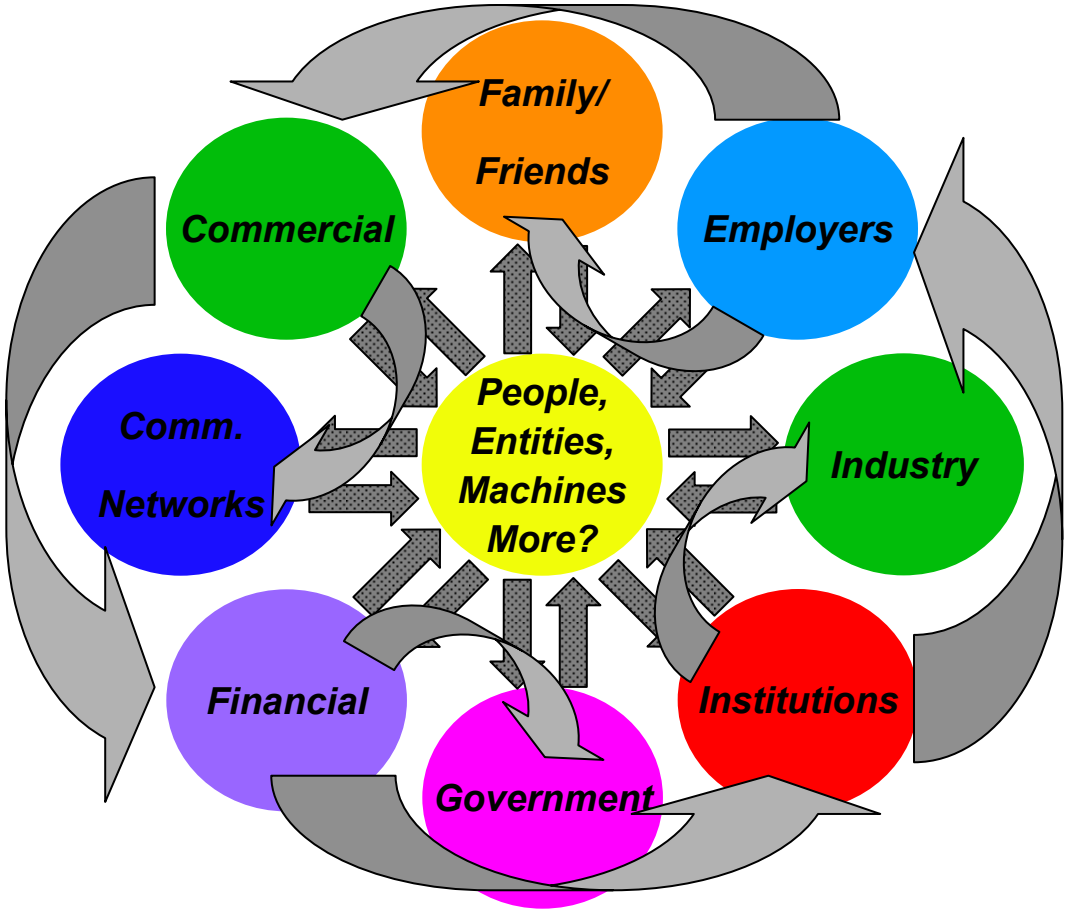
- World of identity is too complex for its own good…..
  - Individuals and commercial entities need simplicity in achieving what they want to do securely, privately, and confidently
  - In order to grow outside the enterprise—federate the federations—identity marketplace needs a scalable, trustworthy commercially viable solution

The General Ecology



… a complex problem to solve

The General Ecology

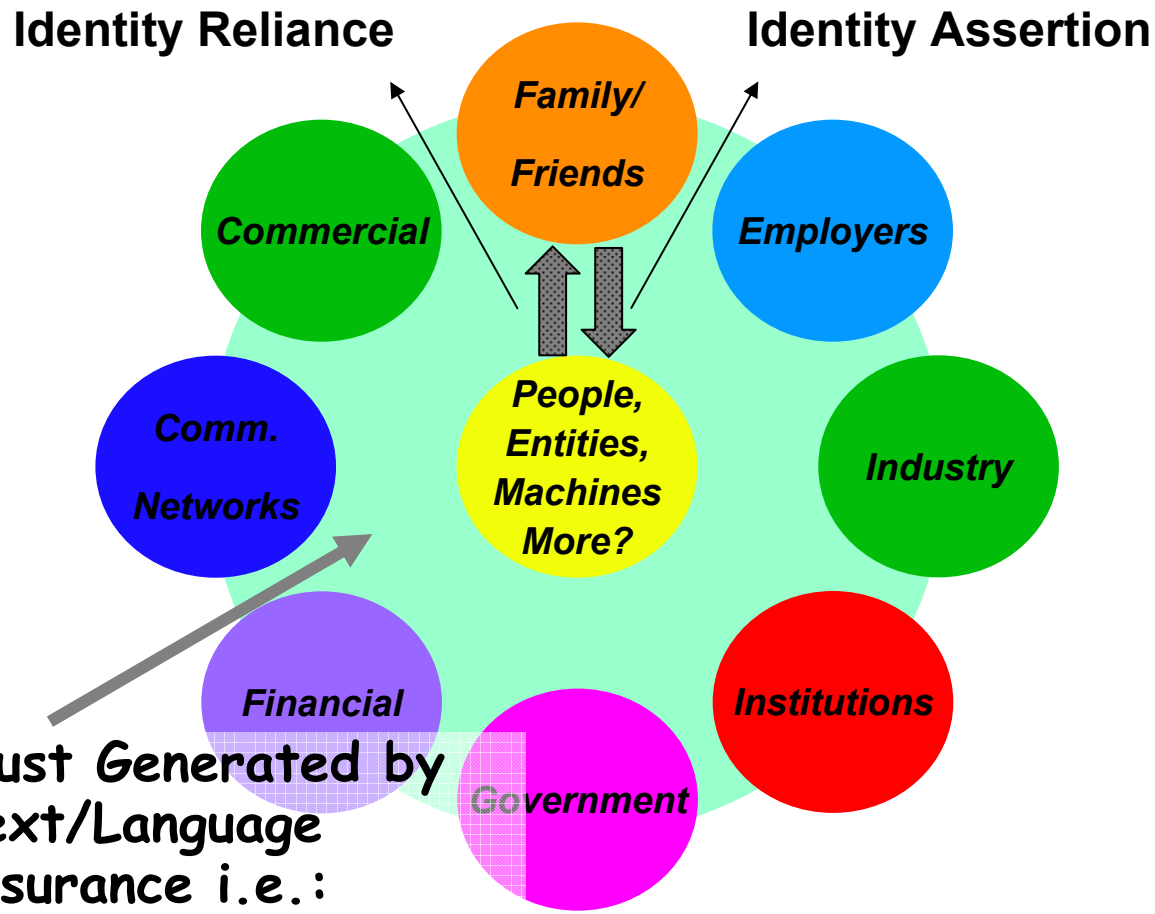


And getting more complex all the time …

To succeed and progress, the industry needs…

- Ubiquitous, **interoperable**, privacy-respecting, identity layer:
  - Liberty represents all constituencies toward this objective
    - (vendors, enterprise, government, consumers, universities, SME's, etc.)
  - Must be an open, collaborative system vs. single vendor strategy
  - Identity is important & complex. We must come together OR:
    - industry will become more fractured
    - governments will intervene
- Privacy-compliant practices to exchange identity information
- Standards-based model to …
  - Interoperate in heterogeneous environments
  - Avoid proprietary vendor lock-in
  - Provide flexible foundation for future growth
  - Scale to the WWW
- Consumer & enterprise confidence that security, privacy and data integrity will be maintained

The Enriched Ecology



Digital Trust Generated by Context/Language of Assurance i.e.: "Identity Assurance Framework"

LIBERTY ALLIANCE PROJECT

A Word From The Bard

Who steals my purse steals trash...

But he that filches from me my good name

Robs me of that which not enriches him*

And makes me poor indeed

--William Shakespeare

* Elizabethan England had not yet succumbed to wiles of the Internet

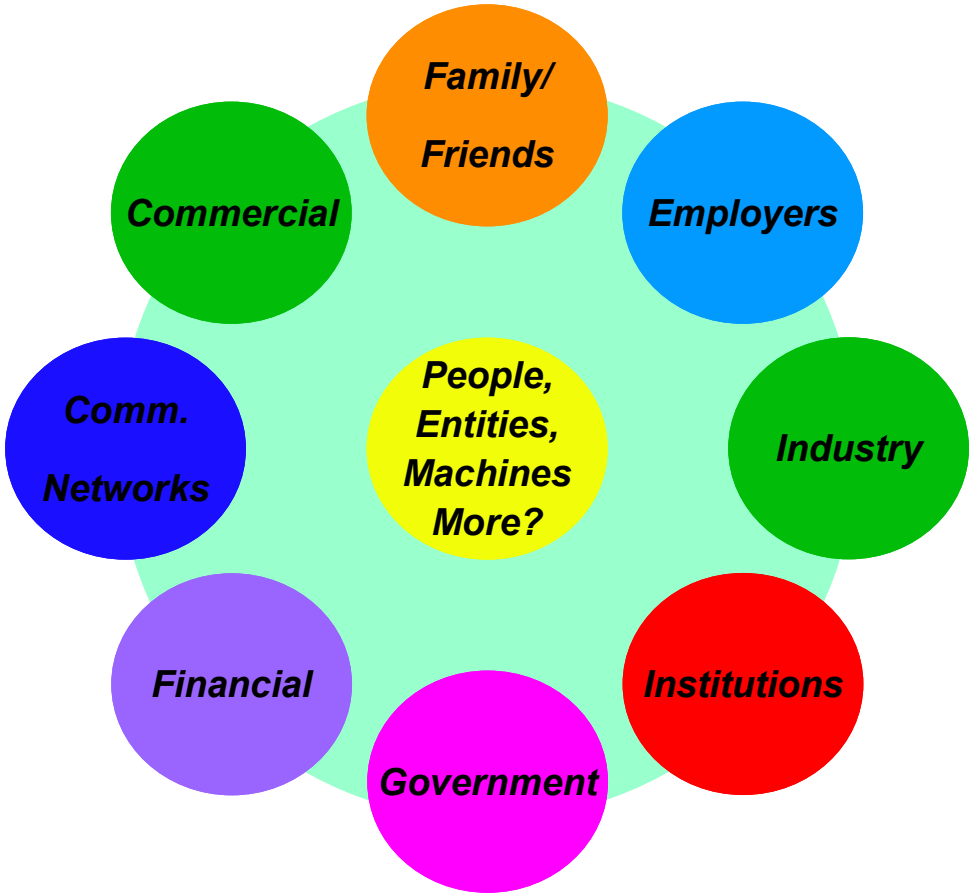
The Enriched Ecology

The *Framework* Must Be:

- Universally Understood
- Subject to standard definitions
- Commercially viable
- Scalable
  - Minimal to High
  - Non-repudiation
- Politically savvy

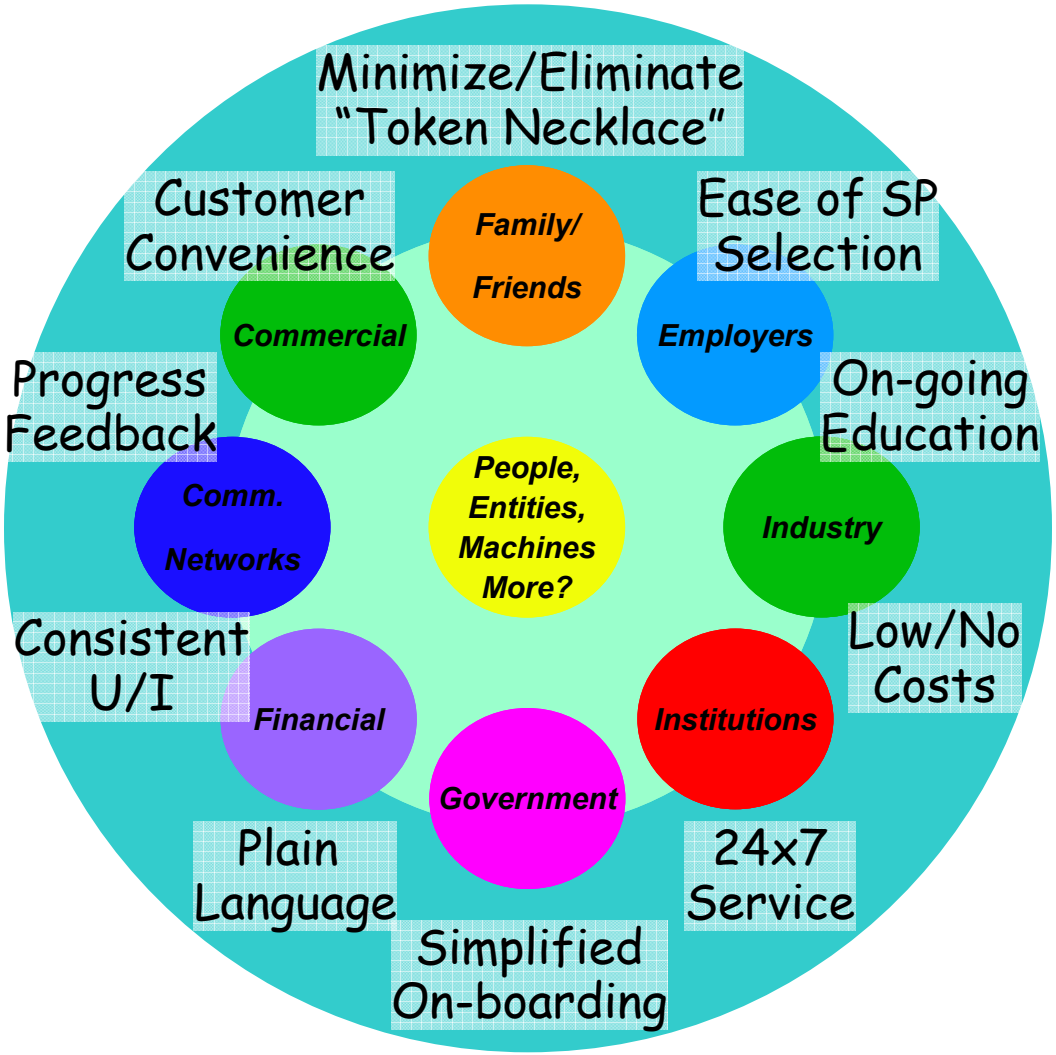
The *Framework* Will be:

- Consumed by new emerging federations
- A source of revenue for certification agents
- A source of customer convenience

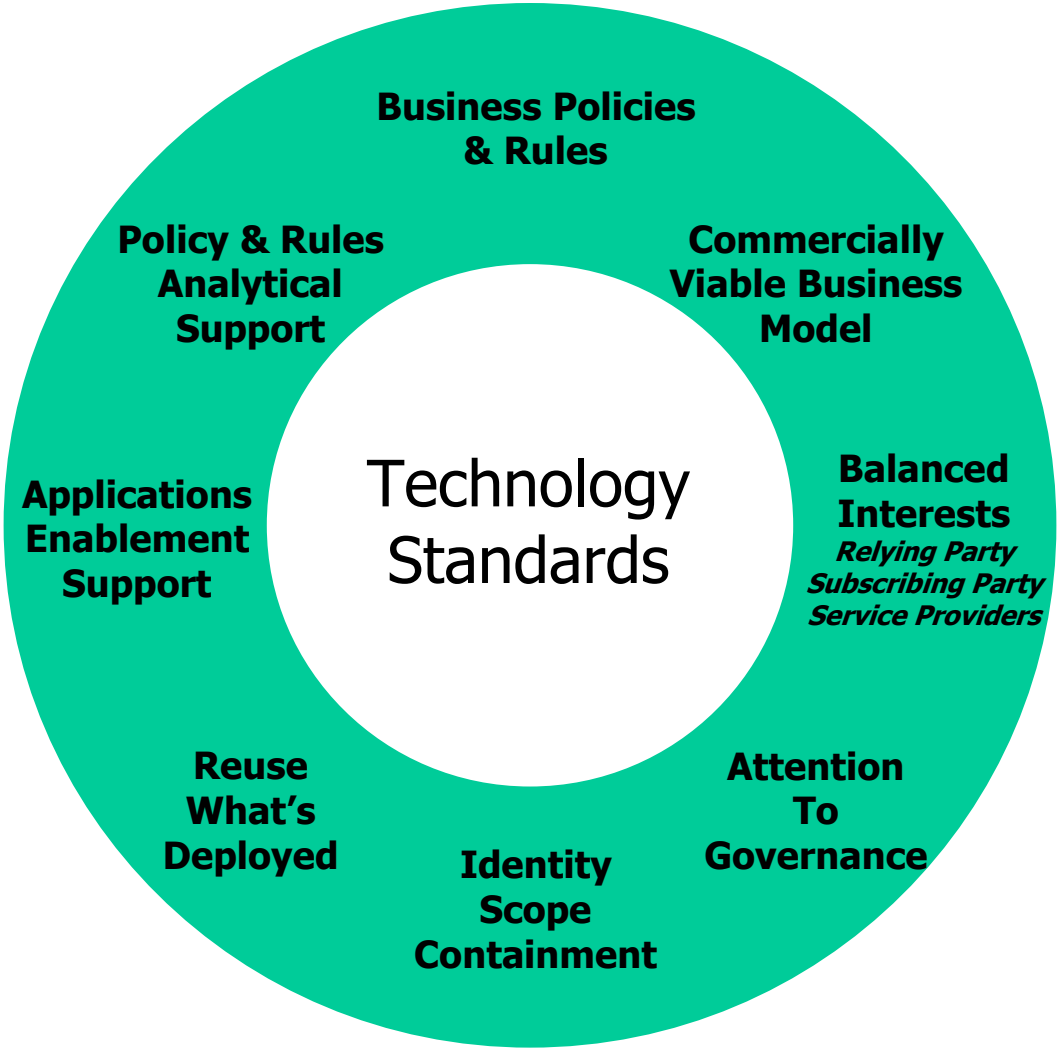


LIBERTY ALLIANCE PROJECT

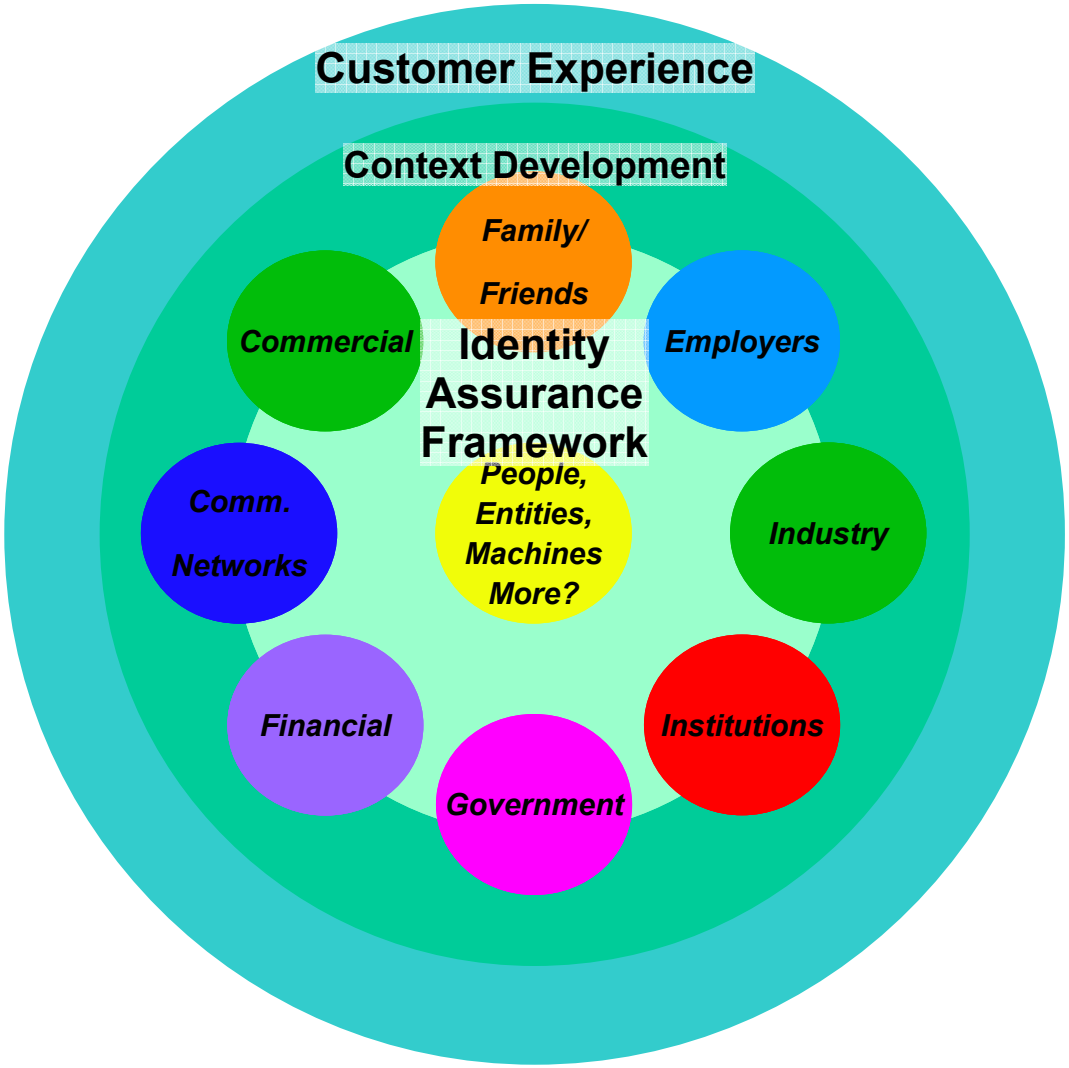
Consistent & Clear Customer Experience



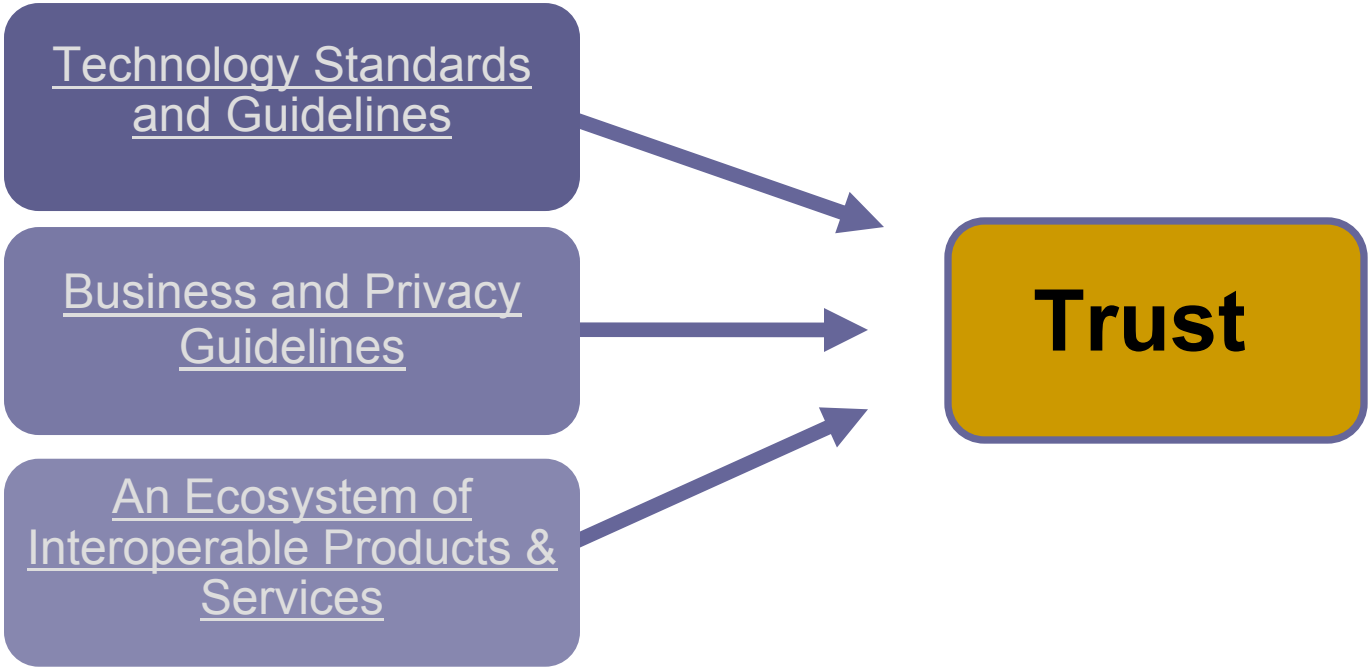
Identity Assurance Context Development



Success Model Includes All



What Liberty is Doing About it…



Liberty helps organizations build a foundation for trust -- critical for the overall success of identity-based services and efficiencies

Building a Foundation of Trust

LIBERTY ALLIANCE PROJECT

Why Liberty Alliance: Who We Are

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

AOL, Ericsson, Fidelity Investments, France Telecom, HP invent, Intel, Novell, NTT, Oracle, Sun microsystems

Sponsors

Adobe, CATCert Agència Catalana de Certificació, Bank of America, betasystems, BIPAC, bmc software, BT, CA Transforming IT Management, Drummond Group, gemalto, GEOFEDERATION, GM, GSA, IBM, kantega, LUMINANCE CONSULTING, Mortgage Bankers Association, MEDcommons, NEC, NeuStar, State Services Commission Te Komihana O Ngā Tari Kāwanatanga, NHK 放送技術研究所 Science & Technical Research Laboratories, Nokia, PostSecondary Electronic Standards Council, Ping Identity, SanDisk, symLABS Identity Management Infrastructure, Telefónica Móviles, Telefónica, T-Com, Thales, VeriSign, UNINETT, Wells Fargo

Identity Assurance Expert Group (IAEG)

- Newly formed Identity Assurance Expert Group (IAEG) designed to foster adoption of identity assurance services
- Initial contributions from EAP and U.S. E-Authentication Federation
- Objective is to create a framework of baseline policies, business rules and commercial terms against which identity assurance services can be assessed and certified
- Goal is to facilitate trusted identity federation to promote uniformity and interoperability amongst identity service providers
- Desired result is operational streamlining of identity service provider certification/accreditation processes for entire industry

Identity Assurance Framework (IAF)

- Harmonized, best-of-breed industry identity assurance standard that is technology agnostic
- Framework supporting mutual acceptance, validation and lifecycle maintenance across identity federation
- Document publicly available
- Framework consists of:

✓ Assurance Levels

✓ Service Assessment Criteria

✓ Accreditation and Certification Rules

IAF Assurance Levels

- Policy Overview
  - 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 in Detail

- **Assurance level criteria as posited by the OMB M-04-04 and NIST Special Publication 800-63:**
  - Level 1 – (e.g. registration to a news website)
    - Satisfied by a wide range of technologies, including PINs
    - Does not require use of cryptographic methods
  - Level 2 – (e.g. change of address by beneficiary)
    - Single-factor remote network authentication
    - Claimant must prove control of token through secure authentication protocol
  - Level 3 – (e.g. online access to a brokerage account)
    - Multi-factor remote network authentication
    - Authentication by keys through cryptographic protocol
    - Tokens can be “soft”, “hard” or “one-time password”
  - Level 4 – (e.g. dispensation of controlled drugs)
    - Multi-factor remote authentication through “hard” tokens
    - Transactions are cryptographically authenticated using keys bound to the authentication process

IAF Service Assessment Criteria (SAC)

Mapping to levels

- Common Organization SAC - The general business and organizational conformity of services and their providers
  - Enterprise maturity; Information Security Mgmt; Operational Infrastructure, etc.
- Identity Proofing SAC - The functional conformity of identity proofing services
  - Identity verification; Verification records
- Credential Management SAC - The functional conformity of credential management services and their providers
  - Operating environment; Issuance; Revocation; Status Mgmt; Validation/Authentication

Accreditation and Certification Rules

- **Focused on the use of credentials for authentication, initially targeting CSPs**
- **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, CSPs and Federation Operators) may work together**
- **LAP 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 Credential Assessment Profiles (CAP) introduced in IAF document
  - CAP Development
    - Process for reviewing and approving new CAPs to keep up with technological advances
  - CAP Maintenance
    - Process by which IAEG maintains the currency of CAP

Reference Documents

- **EAP Trust Framework**:
  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:**
  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

Getting Involved

- **Liberty Alliance**

www.projectliberty.org

- **Identity Assurance Special Interest Group**
(formal membership in Liberty Alliance is not required)

http://wiki.projectliberty.org/index.php/IASIG

- **Identity Assurance Framework for Review and Comment**

http://www.projectliberty.org/liberty/content/download/3736/24651/file/liberty-identity-assurance-framework-v1.0.pdf

LIBERTY ALLIANCE PROJECT

Thank You