LIBERTY ALLIANCE PROJECT

Liberty Alliance

Colin Wallis, State Services Commission, New Zealand Government

(On behalf of Brett McDowell, Executive Director, Liberty Alliance Project)

September 30, 2007

Lucerne, Switzerland

Who is Liberty Alliance?

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 NTT Novell. ORACLE Sun microsystems

Members include…

ActivIdentity Adobe CATCert Agència Catalana de Certificació AmSoft Systems BankofAmerica. betasystems BIPAC

bmcsoftware BT ca Transforming IT Management Drummond group falkin systems life secured FuGen Solutions gemalto

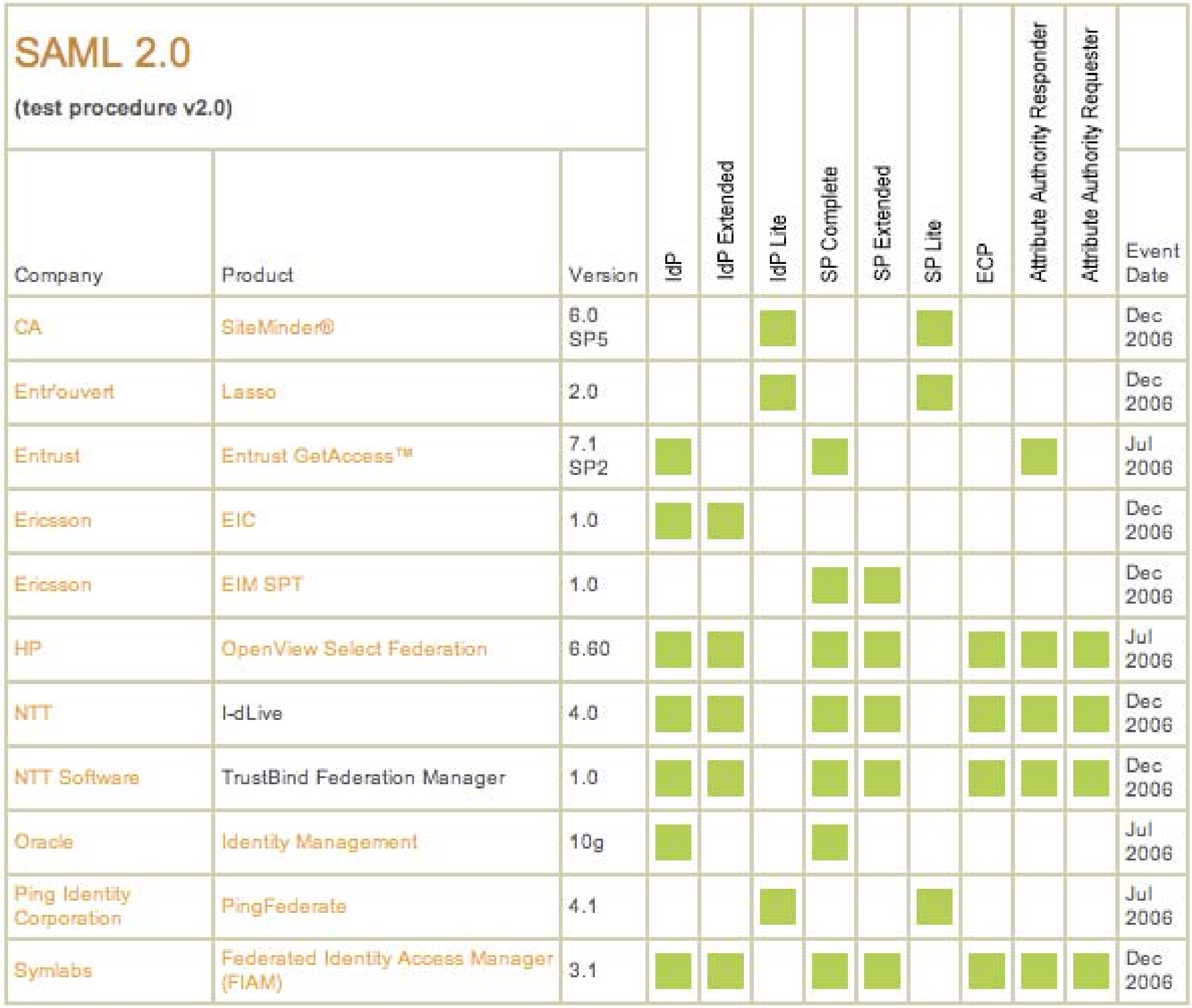
GEOFEDERATION GM GSA IBM kantega LUMINANCE CONSULTING MEDcommons

NANOIDENT TECHNOLOGIES AG NEC NEUSTAR STATE SERVICES COMMISSION Te Komihana O Ngā Tari Kāwanatanga NOKIA PingIdentity RSA SECURITY symLABS Identity Management Infrastructure SanDisk

Telefónica Móviles Telefónica T··Com· telenor THALES UNINETT WELLS FARGO

Who is implementing our standards?

ELIOS Informatique
ALCATEL
hp invent
ERICSSON
epok
Novell.
NEC
Entrust
gemalto security to be free
entr'ouvert
symLABS
ORACLE
Ping Identity
RSA
Sun microsystems
NTT
Reactivity
ETRI
NOKIA Connecting People



SAML 2.0 (test procedure v2.0)												
Company	Product	Version	IdP	IdP Extended	IdP Lite	SP Complete	SP Extended	SP Lite	ECP	Attribute Authority Responder	Attribute Authority Requester	Event Date
CA	SiteMinder®	6.0 SP5			🟩			🟩				Dec 2006
Entr'ouvert	Lasso	2.0			🟩			🟩				Dec 2006
Entrust	Entrust GetAccess™	7.1 SP2	🟩			🟩				🟩		Jul 2006
Ericsson	EIC	1.0	🟩	🟩								Dec 2006
Ericsson	EIM SPT	1.0				🟩	🟩					Dec 2006
HP	OpenView Select Federation	6.60	🟩	🟩		🟩	🟩		🟩	🟩	🟩	Jul 2006
NTT	I-dLive	4.0	🟩	🟩		🟩	🟩		🟩	🟩	🟩	Dec 2006
NTT Software	TrustBind Federation Manager	1.0	🟩	🟩		🟩	🟩		🟩	🟩	🟩	Dec 2006
Oracle	Identity Management	10g	🟩			🟩						Jul 2006
Ping Identity Corporation	PingFederate	4.1			🟩			🟩				Jul 2006
Symlabs	Federated Identity Access Manager (FIAM)	3.1	🟩	🟩		🟩	🟩		🟩	🟩	🟩	Dec 2006

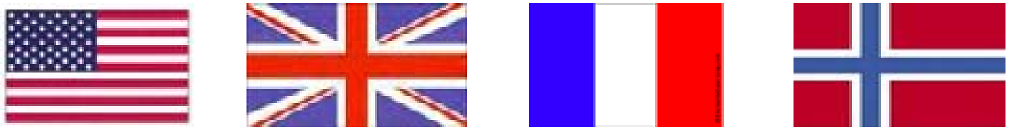
Who is deploying?: One Billion and Growing

see - http://projectliberty.org/index.php/liberty/adoption

AMERICAN EXPRESS · Telefónica · orange · GM · Fidelity INVESTMENTS · BOEING

More than one billion Liberty-enabled identities and devices in the marketplace today…

The de-facto standard for Identity Federation



Organizations moving from early deployment strategies to mapping ROI

hp

"…authentication integrated into a centralized identity management system is about one fourth the cost."

"…Liberty Federation has reduced the cost of manual transactions in the Finland Tax Office to approximately 10-50 cents, representing a cost savings of upwards of 95%"

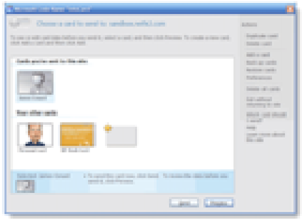
T··Com·

"…T-Online found that 'each click a user was required to make reduced usage by 10%.' Federation has reduced the required number of "clicks."

Concordia Brings Together Disparate Initiatives

inames

OpenID



OPENLIBERTY
SECURE IDENTITY WEB SERVICES

LIBERTY ALLIANCE PROJECT

W3C®

OASIS

INTERNET IDENTITY WORKSHOP 2006

Identity Open Space

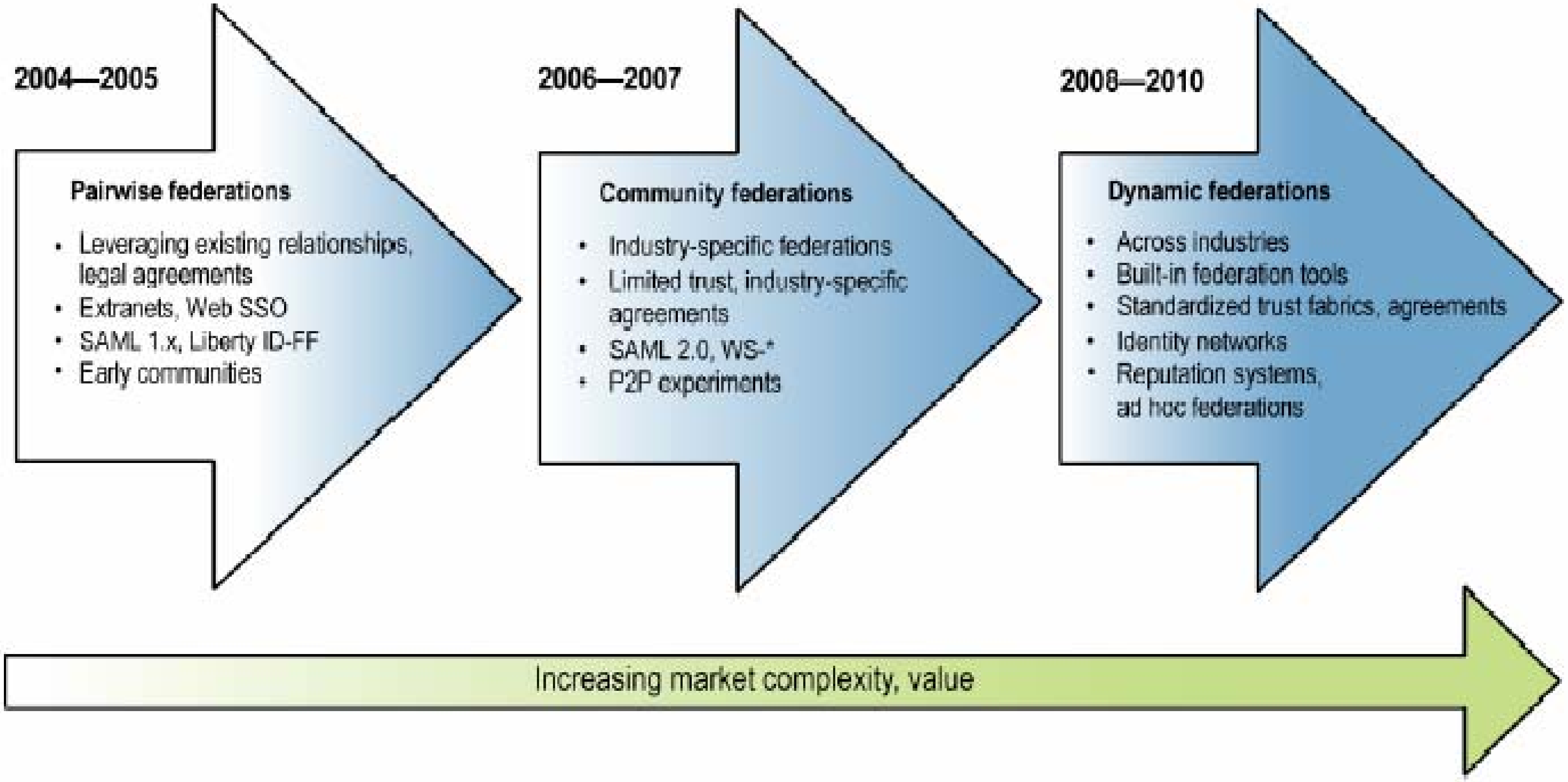
In collaboration with Liberty Alliance LIBERTY ALLIANCE PROJECT

LIBERTY ALLIANCE INTEROPERABLE

What 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.

Moving the Industry Forward



2004—2005

Pairwise federations

- Leveraging existing relationships, legal agreements
- Extranets, Web SSO
- SAML 1.x, Liberty ID-FF
- Early communities

2006—2007

Community federations

- Industry-specific federations
- Limited trust, industry-specific agreements
- SAML 2.0, WS-*
- P2P experiments

2008—2010

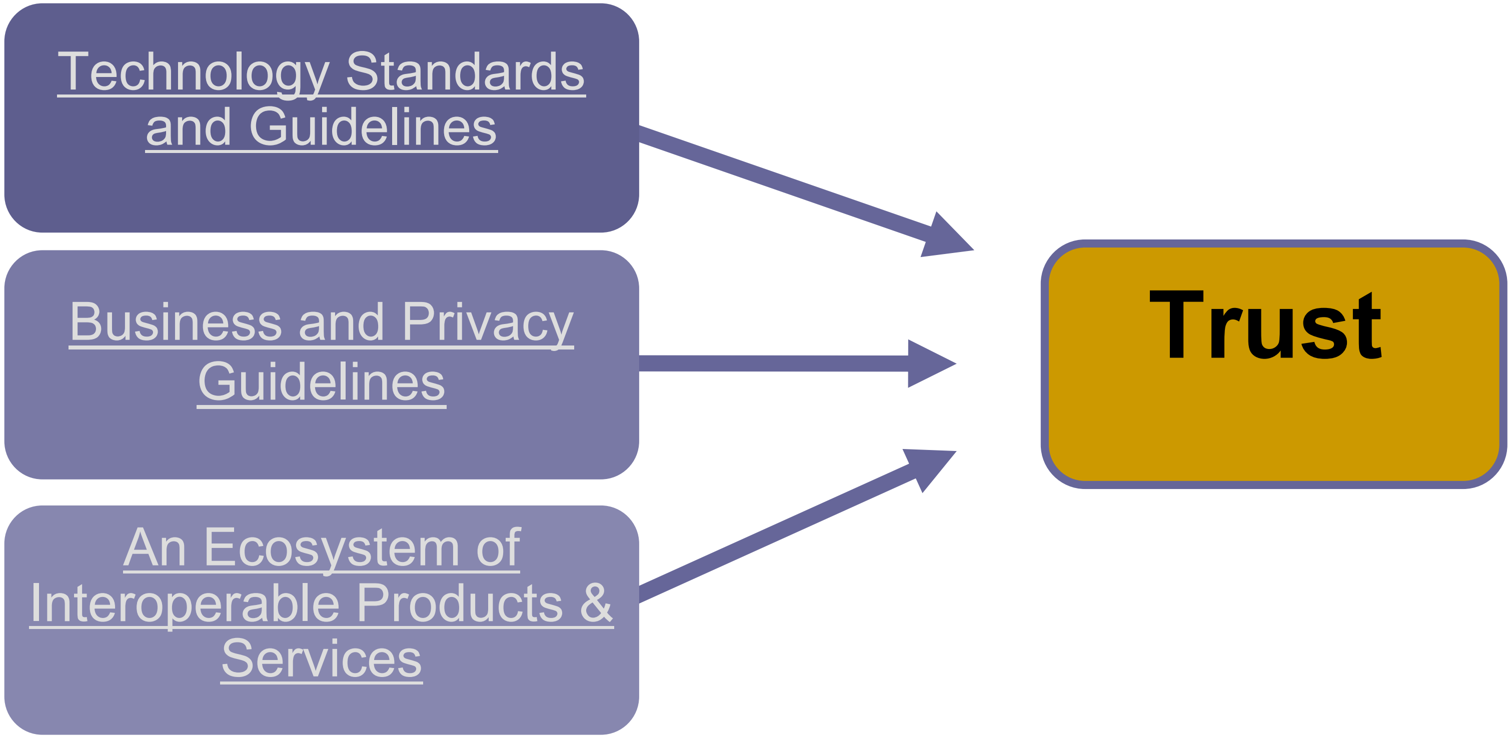
Dynamic federations

- Across industries
- Built-in federation tools
- Standardized trust fabrics, agreements
- Identity networks
- Reputation systems, ad hoc federations

Increasing market complexity, value

Figure 1: *Projecting Federated-Identity Adoption*

What Liberty is Doing about it

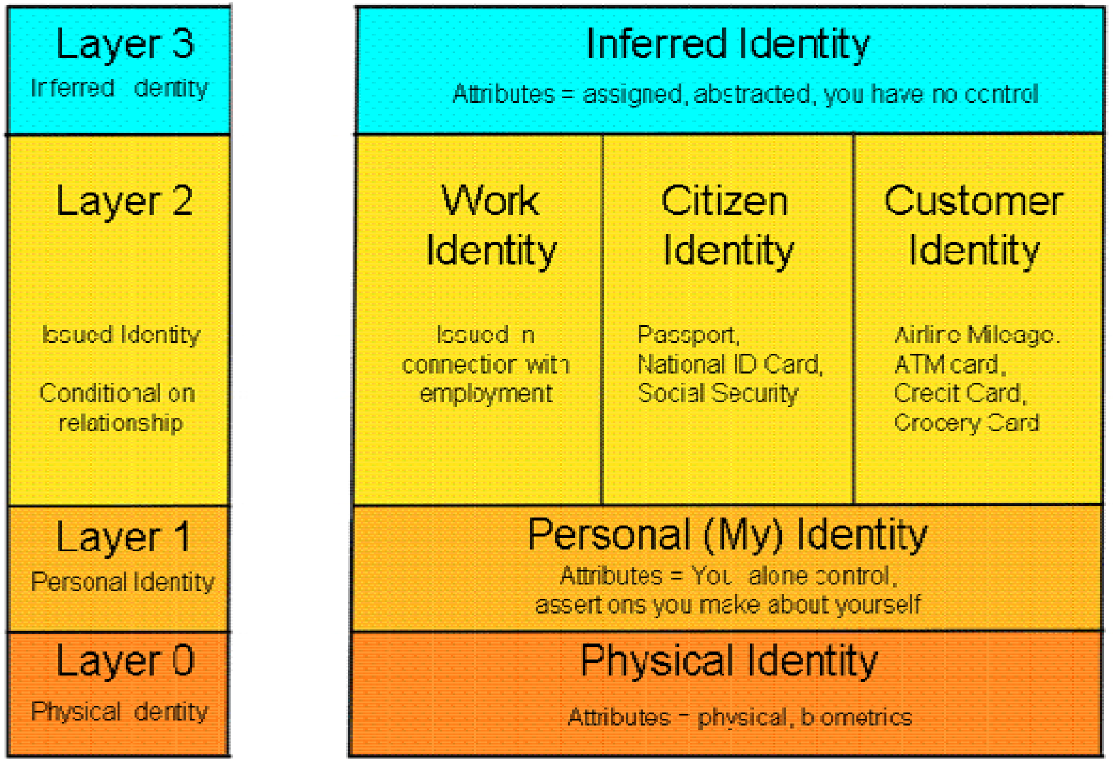

Technology Standards and Guidelines
Business and Privacy Guidelines
An Ecosystem of Interoperable Products & Services
Trust

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

What's the Problem?

- Barriers persist for widespread deployment:
  - Standards confusion exists
  - Identity agent interoperability (SAML, OpenID, Cardspace, Higgins etc)
  - Inter-organizational “trust” is hard to scale
  - Enterprises are struggling to comply with “consent” regulation
  - The market is confused
  - Enterprise PoC's are non-trivial to stand up
- What is Liberty doing to overcome these?...

Identity Management can not be an afterthought



Layer 3
Inferred Identity

Layer 2
Issued Identity
Conditional on relationship

Layer 1
Personal Identity

Layer 0
Physical Identity

Inferred Identity
Attributes = assigned, abstracted, you have no control

Work Identity
Issued in connection with employment

Citizen Identity
Passport, National ID Card, Social Security

Customer Identity
Airline Mileage, ATM card, Credit Card, Grocery Card

Personal (My) Identity
Attributes = You alone control, assertions you make about yourself

Physical Identity
Attributes = physical, biometrics

It will take time to build the right capabilities

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

Identity Assurance Trust Framework

- Utilizes EAP Trust Framework and US e-Authentication Federation Credential Assessment Framework as a baseline
- Harmonized, best-of-breed industry identity assurance standard
- Framework supporting mutual acceptance, validation and lifecycle maintenance across identity federations
- Framework consists of:
  - Business Rules
  - Assurance Levels
  - Service Assessment Criteria
  - Accreditation and Certification Model

Trust Framework Business Rules

- Focused on the use of credentials for authentication, with the initial phase targeting Identity Providers (IDPs)
- IAEG provides accreditation of assessors who will perform certification assessment
- Federation Operators will make ultimate IAEG-certification decision based on findings of accredited assessors
- Relying Parties agree to abide by IAEG framework and have agreements in place with CSPs, accordingly
- IAEG will maintain relevance of the Trust Framework criteria and provide an updated list of accredited and certified providers

Trust Framework 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 service provider
  - 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)

Trust Framework Assurance Levels

- 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; $1mm wire)
    - Multi-factor remote authentication through “hard” tokens
    - Transactions are cryptographically authenticated using keys bound to the authentication process

Service Assessment Criteria (SAC)

- *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

Credential Assessment Profiles

- Description / Criteria
  - Maturity of Operations
  - Business Continuity Planning
  - Information Security policies and practices
  - Network and system security
  - Interoperability with authentication systems (i.e. e-Auth)
  - Credential strength
  - Subscriber agreements
  - Rigor of Registration and Record Retention policies
- 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 CAPs

Identity Assurance Certification Model

- Program for auditors to execute certification/accreditation process
- Provide Identity Assurance service providers with guidelines for certifying to Liberty Alliance IAEG
- Federations certifying their members for the benefit of inter-federation and streamlining the certification process for the industry
- Liberty Alliance IAEG to provide governance over certification process
- Phase 1 = Identity Providers
- Phase 2 & 3 = Relying Parties and Federation Operators

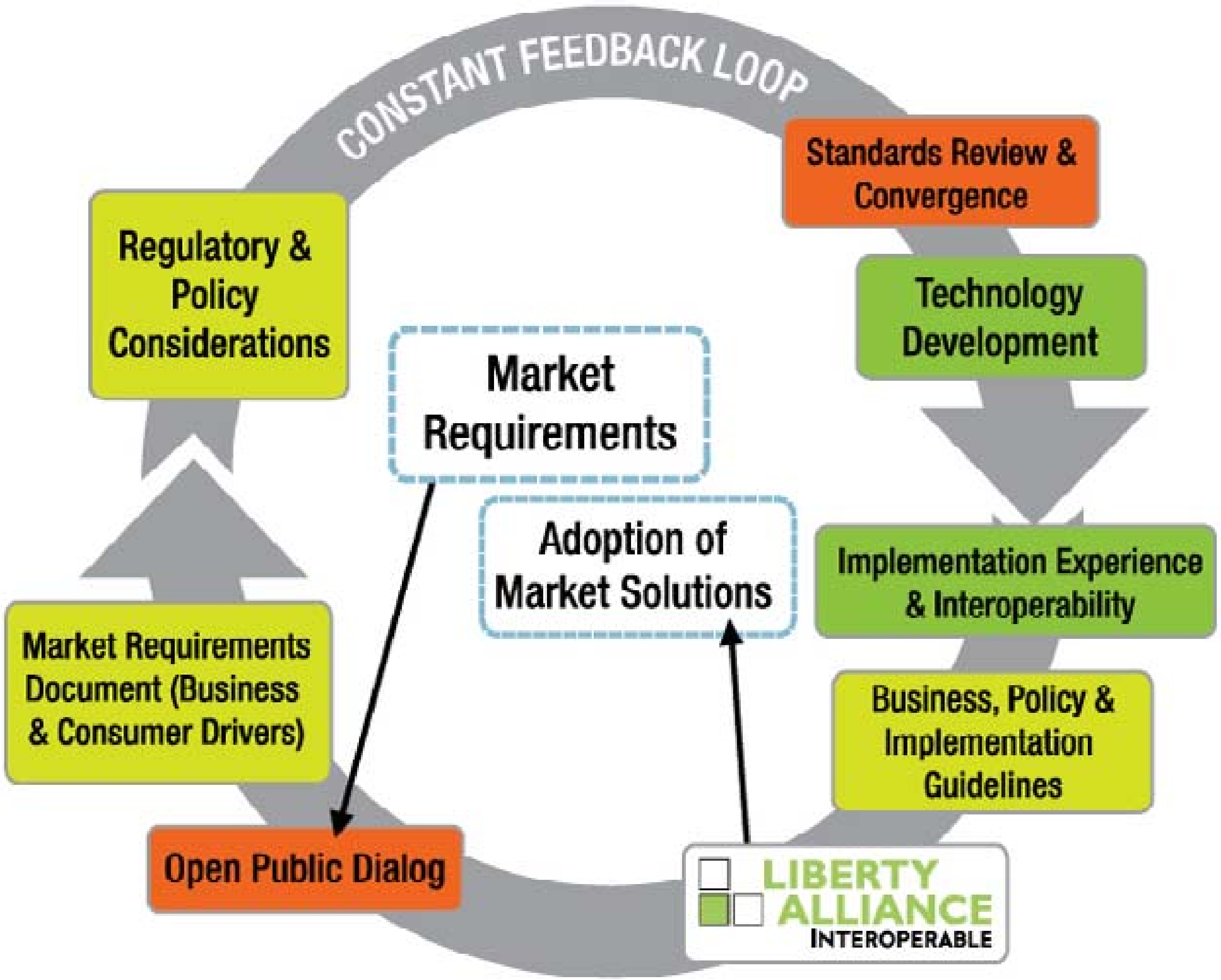
Reference Documents

- EAP Trust Framework
- OMB e-Authentication Guidance (OMB M-04-04)
- NIST Special Publication 800-63 Version 1.0.1
- Authentication Service Component Interface Specifications
- GSA Credential Assessment Framework, Password CAP, Certificate CAP and Entropy Spreadsheet

Questions

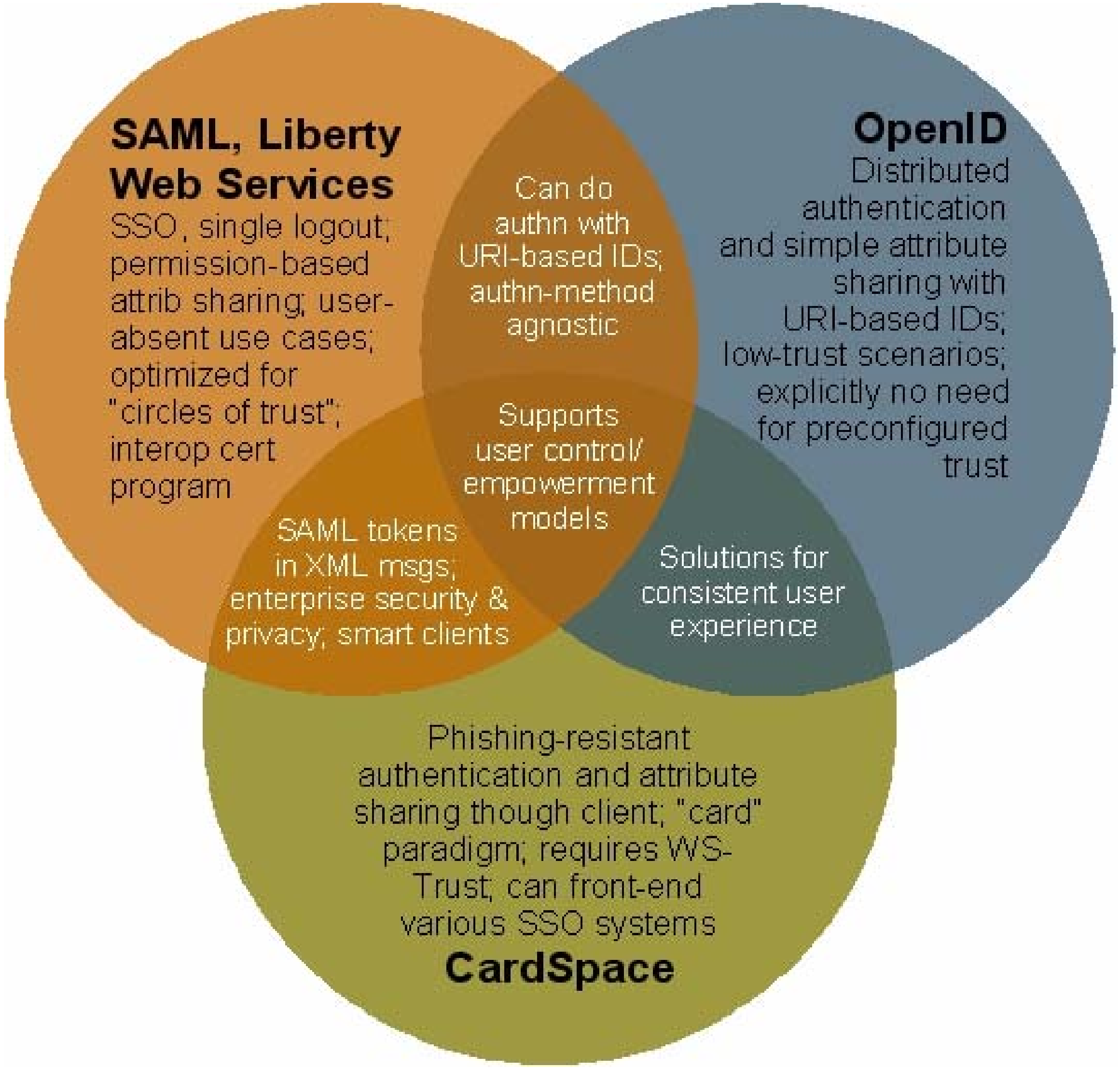
Contact: Brett McDowell, Executive Director, brett@projectliberty.org (+1.413.662.2744)

How Do We Get Things Done?



CONSTANT FEEDBACK LOOP
Standards Review & Convergence
Technology Development
Implementation Experience & Interoperability
Business, Policy & Implementation Guidelines
LIBERTY ALLIANCE INTEROPERABLE
Open Public Dialog
Market Requirements Document (Business & Consumer Drivers)
Regulatory & Policy Considerations
Market Requirements
Adoption of Market Solutions

Potential Unification Touch Points



SAML, Liberty Web Services
SSO, single logout; permission-based attrib sharing; user-absent use cases; optimized for "circles of trust"; interop cert program

OpenID
Distributed authentication and simple attribute sharing with URI-based IDs; low-trust scenarios; explicitly no need for preconfigured trust

Can do authn with URI-based IDs; authn-method agnostic

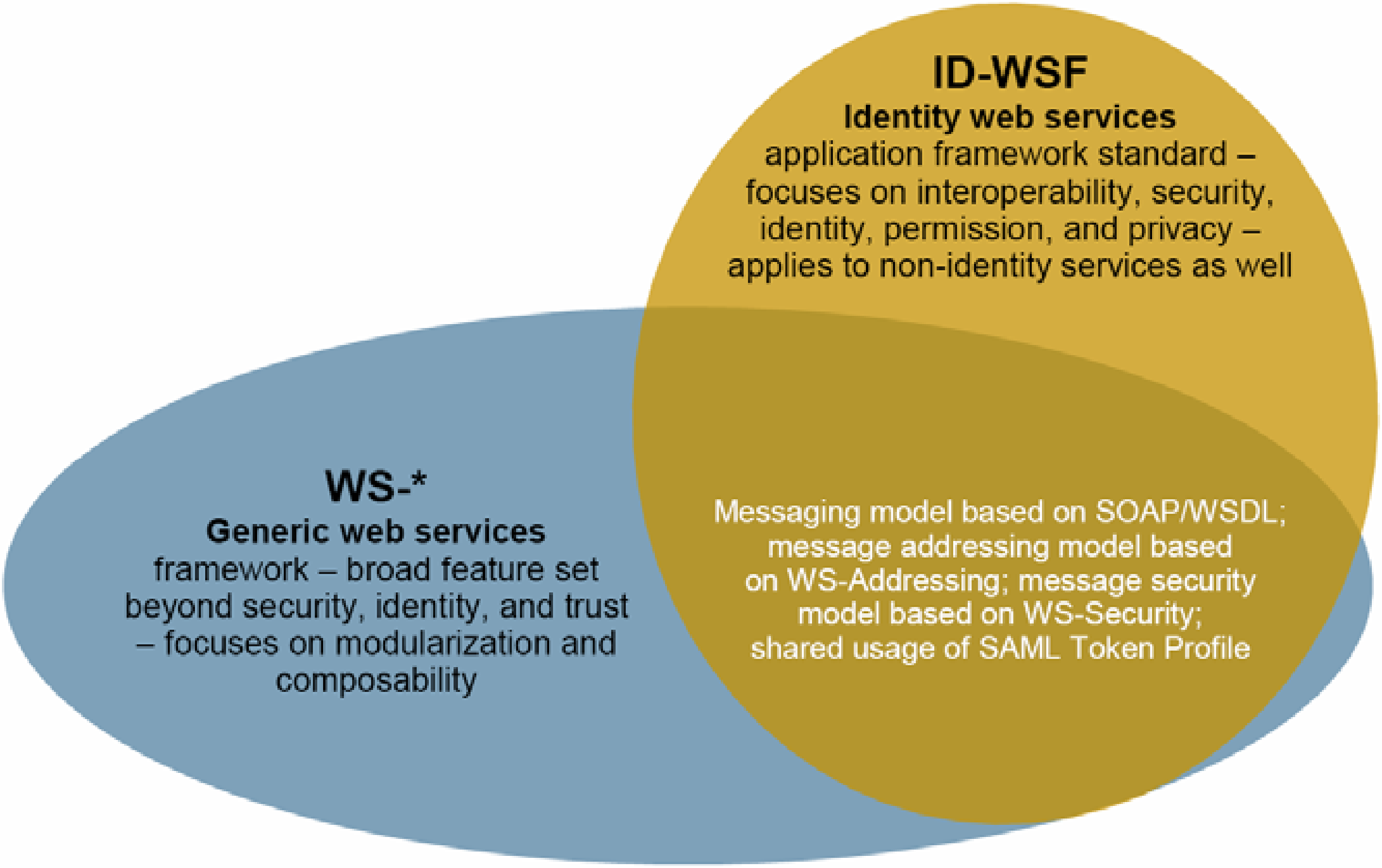
Supports user control/ empowerment models

SAML tokens in XML msgs; enterprise security & privacy; smart clients

Solutions for consistent user experience

Phishing-resistant authentication and attribute sharing though client; "card" paradigm; requires WS-Trust; can front-end various SSO systems
CardSpace

Liberty's Identity Web Services



ID-WSF

Identity web services application framework standard – focuses on interoperability, security, identity, permission, and privacy – applies to non-identity services as well

WS-*

Generic web services framework – broad feature set beyond security, identity, and trust – focuses on modularization and composability

Messaging model based on SOAP/WSDL; message addressing model based on WS-Addressing; message security model based on WS-Security; shared usage of SAML Token Profile

How to address the new challenges

- Introducing The Concordia Project
  - A new program designed to drive interoperability throughout the Internet Identity Layer
  - Global, cross-initiative collaboration
  - A public call for interop use cases for heterogeneous environments
  - Expansion of Liberty's interoperability testing to meet new and varied requirements
  - Open source support for relying parties

LIBERTY ALLIANCE PROJECT

Liberty ID-WSF 2.0
Marketing Requirements Document
Version: 1.0

LIBERTY ALLIANCE INTEROPERABLE

OPENLIBERTY
SECURE IDENTITY WEB SERVICES

Concordia Components

- Open Wiki: http://www.projectconcordia.org
- Events
  - IOS, IIW, Catalyst, DIDW, etc.
- Use case definitions
  - More than 20 submissions, including detailed use cases from AOL, Boeing, GM, Government of British Columbia, and the US GSA
- Future Interop Event(s)
- Specification work to be done in appropriate standards bodies
- Future Certification Program Support from Liberty Alliance

IGF to help industry meet regulation

- Increasing legal and regulatory concern about access to identity-related data about users
  - Privacy concerns: HIPAA, SB 1386, theft of user data
  - Compliance: SOX, GLB, EU legislation
  - Who has access to my social security number or account number, and, under what conditions?
- Effective business applications require flexible access to data about users
  - Value of data held by enterprise lies in its use!
  - Application developers should focus on business requirements not on protocols or identity stores
- CHALLENGE: Need an enterprise-wide framework for managing access to identity-related data provided by multiple sources

Identity Governance Framework

- CARML – Defines application identity requirements
  - what identity information an application needs and how the application will use it.
- AAPML – Defines identity use policies (XACML)
  - Constraints on user and application access to personal data
  - obligations and conditions under which data is to be released
- Attribute Service – Links applications to identity data
- Developer APIs/Tools – Developers can express identity requirements at a business level at development time
  - Key to IGF adoption/use