SATW
Schweizerische Akademie der Technischen Wissenschaften
Académie suisse des sciences techniques
Accademia svizzera delle scienze tecniche
Swiss Academy of Engineering Sciences

e-Health
e-Education
e-Society
Engineering the Knowledge Society

eHealth Workshop
Konolfingen (CH)
Dec 4--5, 2007

Sun microsystems

LIBERTY ALLIANCE PROJECT

Managing Trust in e-Health with Federated Identity Management

Dr. rer. nat. Hellmuth Broda

Distinguished Director and CTO, Global Government Strategy, Sun Microsystems Inc.
Spokesperson, Liberty Alliance; Member of the Business Marketing Expert Group
Individual Member, SATW; Vice President, Scientific Advisory Board SATW

Healthcare Implications

Healthcare is all about communities …

- Patients
- Providers
- Insurances
- Pharmacy

…that need to share information

- Securely, with
- Strong Authentication, and
- Simplified Identity Management

Issues in Healthcare

Healthcare: a complex landscape of interaction, information sharing and regulation

- Many systems and locations where authentication required
- Each system requires a different password or login
- Most systems don't interoperate/ talk to each other!
- Overall requirement to safeguard PHI

Complexity reduces security

- Individuals and organizations must manage many identities
- Multiple points of vulnerability
- Adverse impact on interaction and privacy

Healthcare: A Complex Community

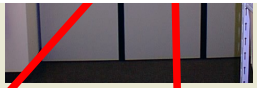




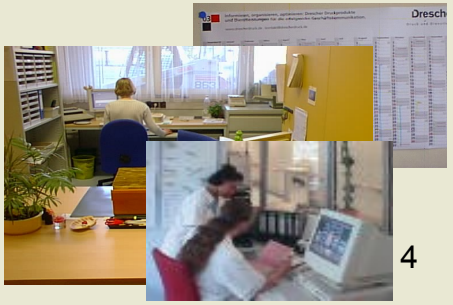










Telemedicine
Imaging
Pharmacy
Health Insurance
Family Doctor
Laboratory Services
Patient Health Information
Medical Specialist
Research & Education
Hospital Services
Billing
Hospital

Enter Liberty

Liberty Alliance provides the means to build the Common Framework for e-Health

- Technology
- Policy
- Knowledge
- Certifications

Over 150 diverse member companies and organizations from around the world:

- Government organizations
- End-user companies
- System integrators
- Software and hardware vendors

Huge adoption:

- Close to a billion identities already under Liberty standards

Who Is the Liberty Alliance?

- Consortium developing open standards
  - ♣For federated identity management
  - ♣In coordination with other standards groups
- Develops open specifications that anyone can implement
  - ♣Liberty does not deliver specific products or services
- Conformance testing & certification to ensure interoperability
  - ♣30+ Liberty-enabled products and services currently available
- Addresses business & policy issues of identity
  - ♣Guidelines, best practices documents, checklists
  - ♣Support for global privacy regulations built into specs

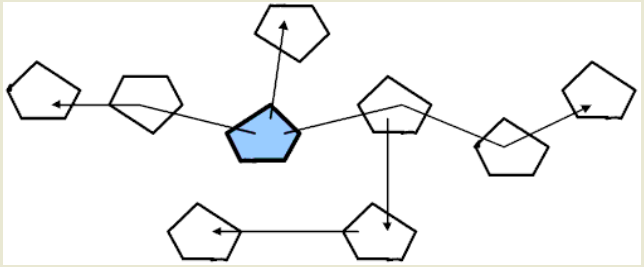
Who is the Liberty Alliance?

About 150 diverse member companies and organizations representing leaders in IT, mobility, government, service provision, system integration and finance from across the globe

Management Board and Sponsor members include:

How We Can Build Trust

- The biggest concern of the principal/patient/customer is **privacy**
- Privacy does not mean that “nobody knows nothing about me”
- It is about managing the faith of the principal/patient/customer by adhering to the agreed scope and holding the information in trust
- Customers are afraid of “Purpose Creep”
- What could an architecture for privacy and trust management look like?



Architecture for Trust Management

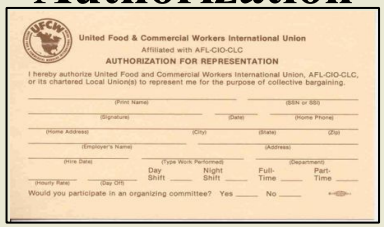
Definitions

Identity Management

Policy

A combination of business and technology practices which define *how* a relationship is conducted and services are performed

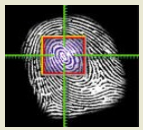
Authorization



A set of rules governing decisions about *what* the user can do: access to information, services or resources

Security Management

Authentication



Assertion of validity of a set of credentials. Credentials express a person´s identity. "A Yes/No answer"

Identity

Basic set of information that creates a "unique" entity (a name with a corresponding set of attributes)

Architecture for Trust Management

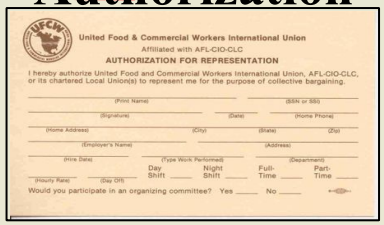
Digitally Speaking . . .

Identity Management

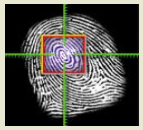
Security Management

Policy

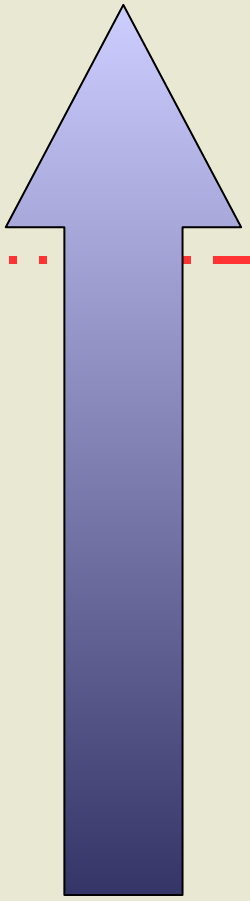
Authorization


United Food & Commercial Workers International Union
Affiliated with AFL-CIO-CLC
AUTHORIZATION FOR REPRESENTATION
I hereby authorize United Food and Commercial Workers International Union, AFL-CIO-CLC, or its chartered Local Union(s) to represent me for the purpose of collective bargaining.
Would you participate in an organizing committee? Yes ____ No ____

Authentication



Identity



4. Business practices to manage risk, enforce security/privacy, provide auditability.
User, customer preferences, history, personalized services,

3. Determination of access rights to systems, applications and information: Match credentials against profiles, ACLs, policy

2. Log on with a UID/PW, token, certificate, biometrics etc. A process that demands the prove that the person presenting them is indeed the person to which credentials were originally issued. accept or reject

1. User, customer, device "facts", e.g., name, address, ID, DNA, keys; credentials, certificates that were issued e. g. by a Certification authority

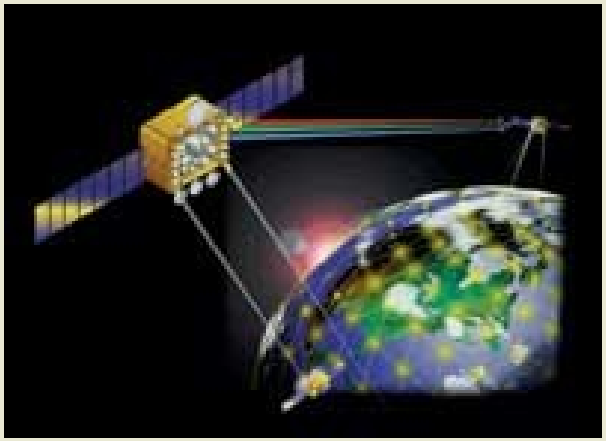
How People Will Trust Policies

- Policy and its audit have to be guaranteed and certified by a approved public or private independent organization, *e. g.:*
  - Federal or State data protection agency
  - TÜV (private institution)
  - Audit firm
  - Chamber of Commerce
  - Postal Service or other basic service provider, . . .
- This can be achieved with defined processes and responsibilities similar to ISO 9000

ϕ Trust is based on policies and the audit of those -- *not* just on security

Liberty's Structure Promotes Privacy and Security

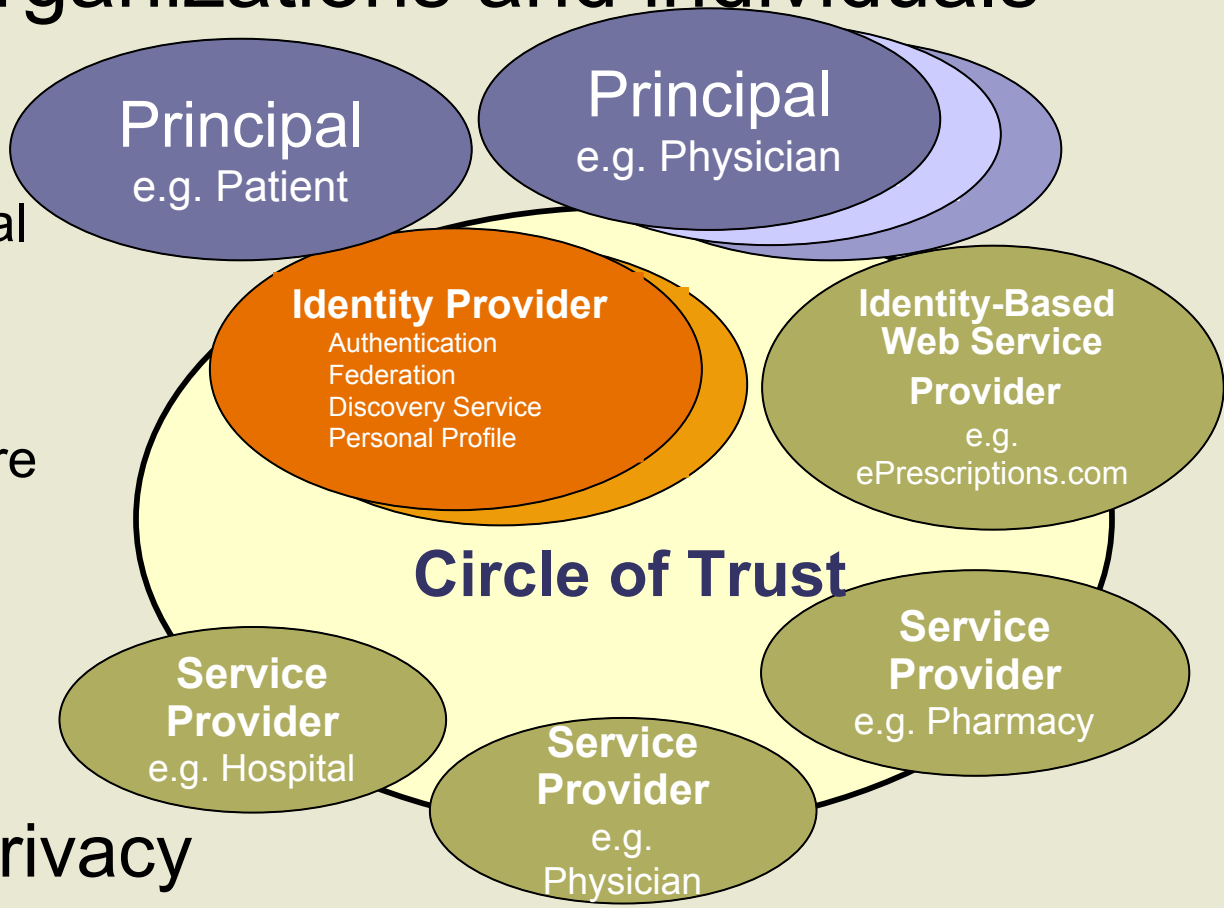
- Federated structure means no single centralized data storage that would be vulnerable to attack
- End user has more control of data because permissions travel with data, guiding its use
- No global identifier--model protects against unauthorized data sharing



How it Happens

Circle of Trust – organizations and individuals

- Business relationships based on Liberty architecture & operational agreements
- Enables patients, physicians and healthcare organizations to safely share information in a secure and apparently seamless environment



Without violating privacy

The Liberty Advantage

- Wide-spread adoption
  - ≤1 billion identities under Liberty protocols
  - Multiple vendor competition
  - Freedom of choice
- Convergence with other standards
  - e.g., SAML2.0, Shibboleth
- Federated authentication model
  - No central point of failure
- Built on standards
  - Works with existing legacy systems and future development plans
- Privacy & security best practices
  - Create trust for all participants
- Conformance testing & certification
  - Provides for multi-product interoperability

Benefits Of Liberty Standards

- Better information sharing among patient, physician, health insurance, pharmacy
  - ♣ Leads to better patient outcomes
  - ♣ Information is timely and coordinated
- Easier for doctor to use electronic systems
  - ♣ No re-authentication required
- More secure for patient
  - ♣ Personal health information shared in controlled manner
- Overall, better service to patient

Liberty's Global Membership

- ~ 150 diverse member companies and organizations representing leaders in IT, mobility, government, service provision, system integration and finance
- Management Board and Sponsor members include:

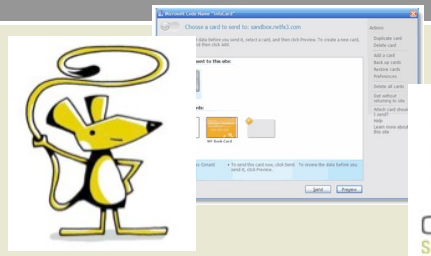
Accomplishments

- *The* de-facto standard for Identity Federation foundation and Web Services
- Over 1 billion federation-enabled touch-points
- Numerous case studies of successful deployments – annual IDDY awards
- Global membership representing: enterprise deployers, vendors, governments, and non-profit organization
- Published Business and Policy guidelines for best practices in legal, privacy, and business deployments
- World-recognized “Liberty Interoperable” test and certification program.

Liberty Directions

- Educate the market
- Addressing Identity Management needs for a Web 2.0 Environment – including:
  - Full range of Identity Management use-case scenarios – individual to enterprise
  - Anonymous-to-strongly authenticated credential standards and privacy policies
  - Worldwide privacy and government liaison
  - Web-scalability – smallest-to-largest systems
  - Open and heterogeneous solution requirements
  - Rich IdM client functionality for flexible deployments
- Help drive adoption

Need to Bring Together Disparate Identity Efforts



- New identity-related technologies are entering the market
- The development of generic web services standards has lagged behind identity web services standards
- Participation in open dialog between leaders followed “silo” development
- Despite recent convergence trends, only Liberty technologies have a certification program

Through an Open Approach

- Drive interoperability throughout the Internet Identity Layer
- Open the doors to collaboration
  - ♣ Open up meetings
  - ♣ Open up public forums & lists
  - ♣ Grow liaison relationships with new communities
  - ♣ Publish a huge inventory of previously confidential material
- The Concordia Program™
  - ♣ A public call for interop use cases for heterogeneous environments
  - ♣ Expand certification program to meet the requirements

OPENLIBERTY
SECURE IDENTITY WEB SERVICES

LIBERTY ALLIANCE PROJECT

Liberty ID-WSF 2.0
Marketing Requirements Document
Version: 1.0

identity commons®

CONCORDIA IN IDENTITATE

LIBERTY ALLIANCE INTEROPERABLE

Concordia's Overarching Goal & Value

- Drive development of a ubiquitous, interoperable, privacy-respecting layer for identity
  - ♣ Helps drive deployment costs down
  - ♣ Assures implementers and deployers better success, greater productivity
  - ♣ Leads to more commercial products and open source offerings=healthy market
  - ♣ Opportunity for better realization of new service offerings
- Assure interoperability across this layer
  - ♣ Deliver confidence to implementers and deployers in implementing today, successful interoperability tomorrow
- Open development process assures strong, cross-sector, cross-geography participation

If we don't act …

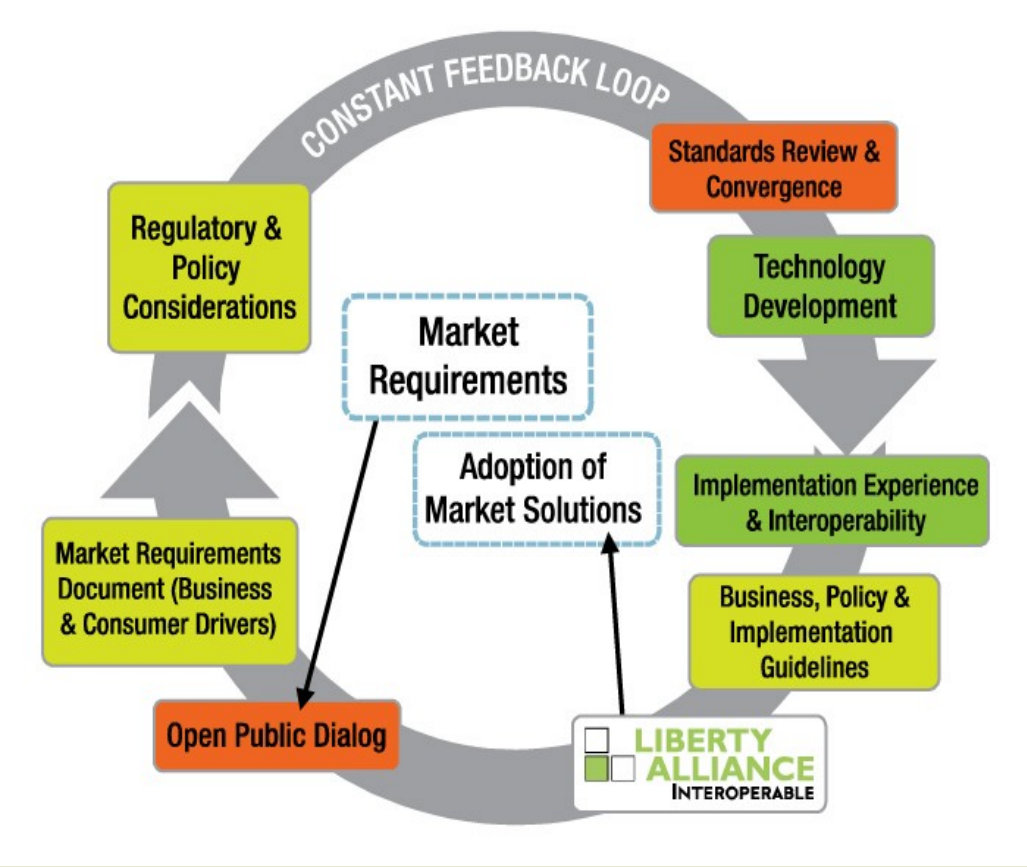
- Loss of privacy
- Compliance regulations
- Unifying disparate models
- Lack of interoperability
- Integrating with legacy systems

*…**all of which can be mitigated by***

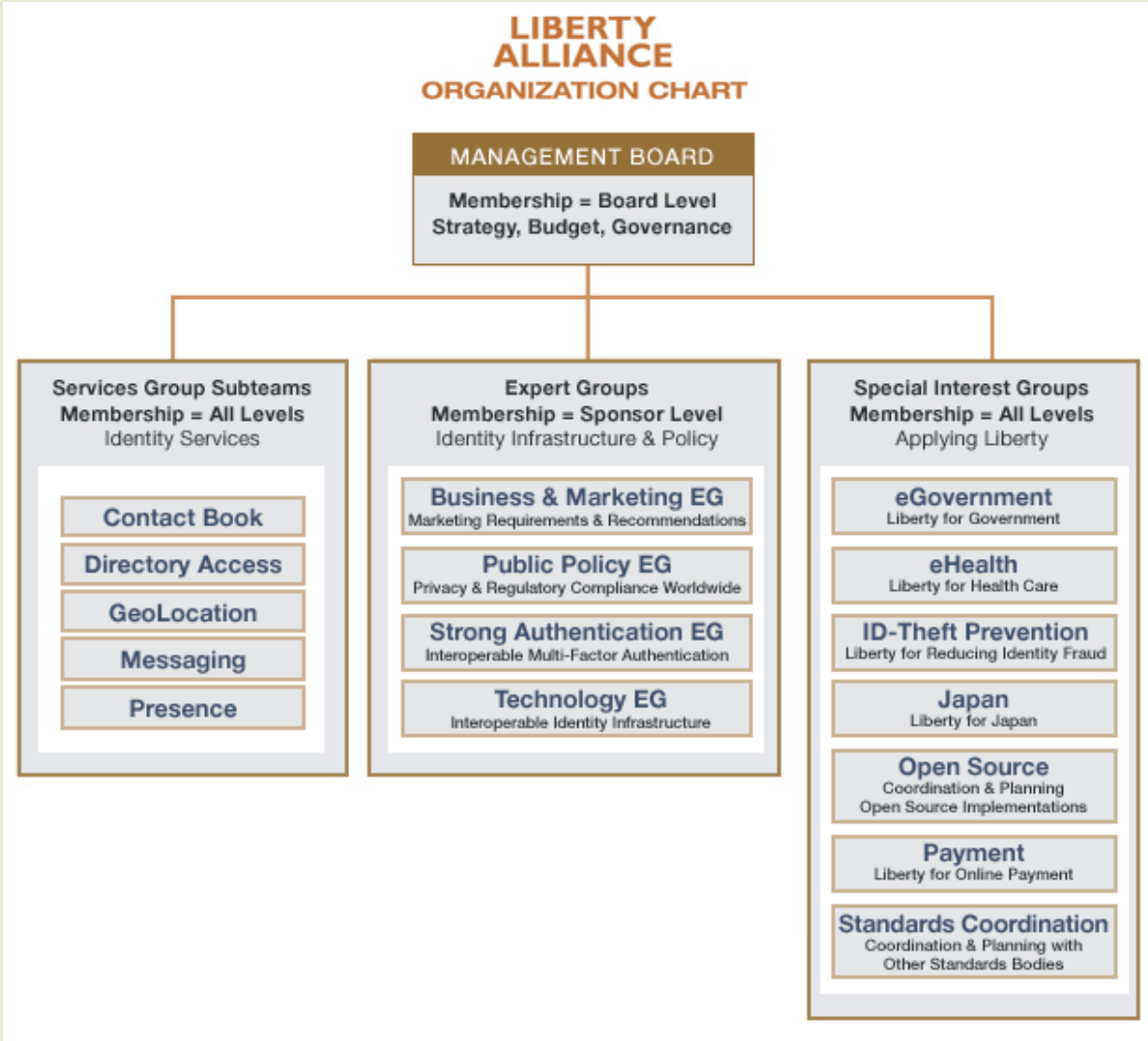
- ♣ Open technology standards
- ♣ Deployment policy guidance
- ♣ Independent 3rd-party certification

Liberty delivers solutions to real problems

- By …
  - Listening to the Market
  - Collaborating with other relevant groups
  - Documenting the requirement
  - Developing specifications an guidelines to meet the needs
  - Certify the products
  - Continuous evolution and improvement



Organization



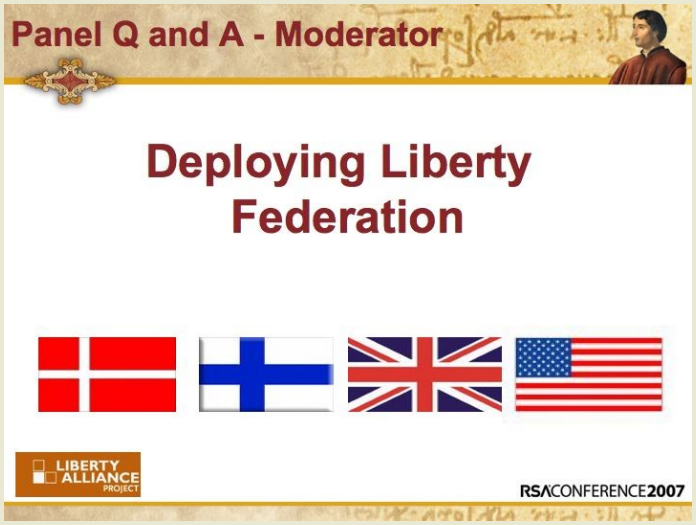
A sampling of vendor adoption

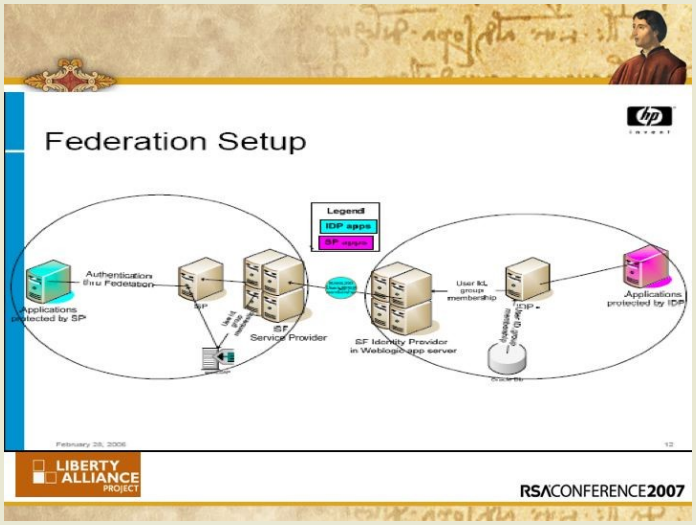
SAML 2.0

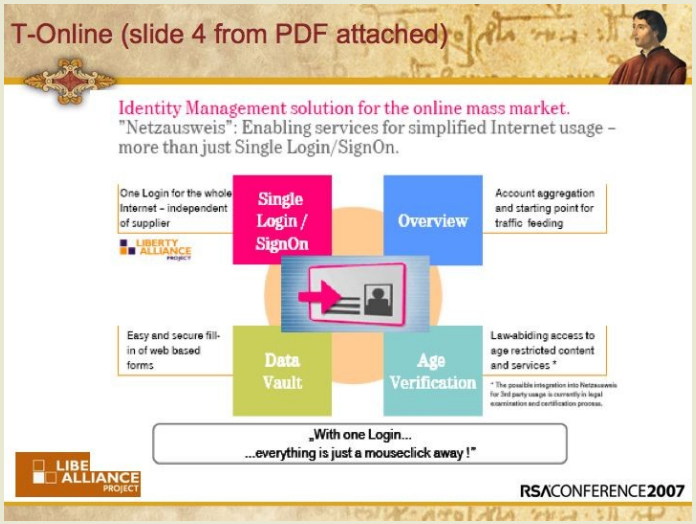
(test procedure v2.0)

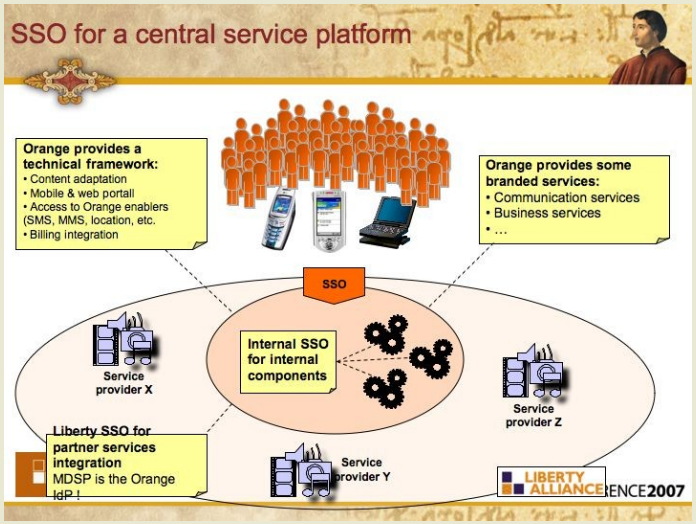
Company	Product	Version	IdP	IdP Extended	IdP Lite	SP Complete	SP Extended	SP Lite	ECP	Attribute Authority Responder	Attribute Authority Requester	Event Date
CA	SiteMinder®	6.0 SP5			■			■				Dec 2006
Entr'ouvert	Lasso	2.0			■			■				Dec 2006
Entrust	Entrust GetAccess™	7.1 SP2	■			■				■		Jul 2006
Ericsson	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

A sampling of deployment case studies









Exciting Current Activities

- openLiberty.org
- Concordia Forum
- Identity Governance Framework – MRD creation
- Advanced Client technical specification enhancements
- IDDY Awards – second year
- Education & workshops
- Membership Agreement changes
- Open mail lists
- Public SIGs
- New Fee Structure
- New Membership Benefits structure

Call to Action: Join Us!

Liberty brings value to our Healthcare members:

- **Federated Identity Management provides "plumbing" standards that:**
  - **Support key elements of interoperability**
  - **Make it much easier for patients, providers and payers to share results of authentication**
  - **Enable easier, faster compliance with government regulations**
- **Conformance and compliance testing that assure base levels of interoperability and functionality**

Become Engaged:

See the specifications and white papers at:
www.projectliberty.org
Become a member!

See also: User centric identity demo at: http://blogs.sun.com/hubertsblog

For more information:
https://www.projectliberty.org/resources/featured_verticals_health.php

Recommendation and Conclusion

- National and international interoperability with trust and privacy is key
- Build on existing standards
- Embrace Federated Identity for role based access and to protect patient's information
- Federated Identity scales much better than hierarchical approaches
- The Liberty Alliance is the ideal boiler plate to build the foundation for an interoperable national health network. Join the Alliance, talk to Sun (founder of the Alliance)