ITU-T

International Telecommunication Union

Privacy, Security, and Trust 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

Member, Swiss Academy of Engineering Sciences; VP, Scientific Advisory Board

ITU-T Workshop on "Digital Identity for NGN"
Geneva, 5 December 2006

Life With An Identity Mess

- A typical intensive IT user has 21 passwords
  - 49% write their passwords down or store in a file on their PC
  - Majority use common words for passwords; 67% rarely or never change their passwords
  - *Source: NTA Monitor Password Survey, UK; zdnet.com
- Password proliferation increases Help Desk Calls
  - In a non-automated support model, password reset costs range from $51 to $147 for the labor alone (Gartner)
  - In an average 10,000 employee size company, about 45% of help-desk calls are requests for password resets. (Meta Group)
- Identity Silos (Source: Sun Customer Survey)
  - Typical IT: 10 different apps or services that contain identity profiles
  - Over 80% of companies have no Identity synchronization solution

ITU-T

How Did Computing Live Without Identity?

Location was an implicit proxy for Identity

Enter Liberty

Liberty Alliance provides the means to build the Common Framework for Federated Identity Management

- 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?

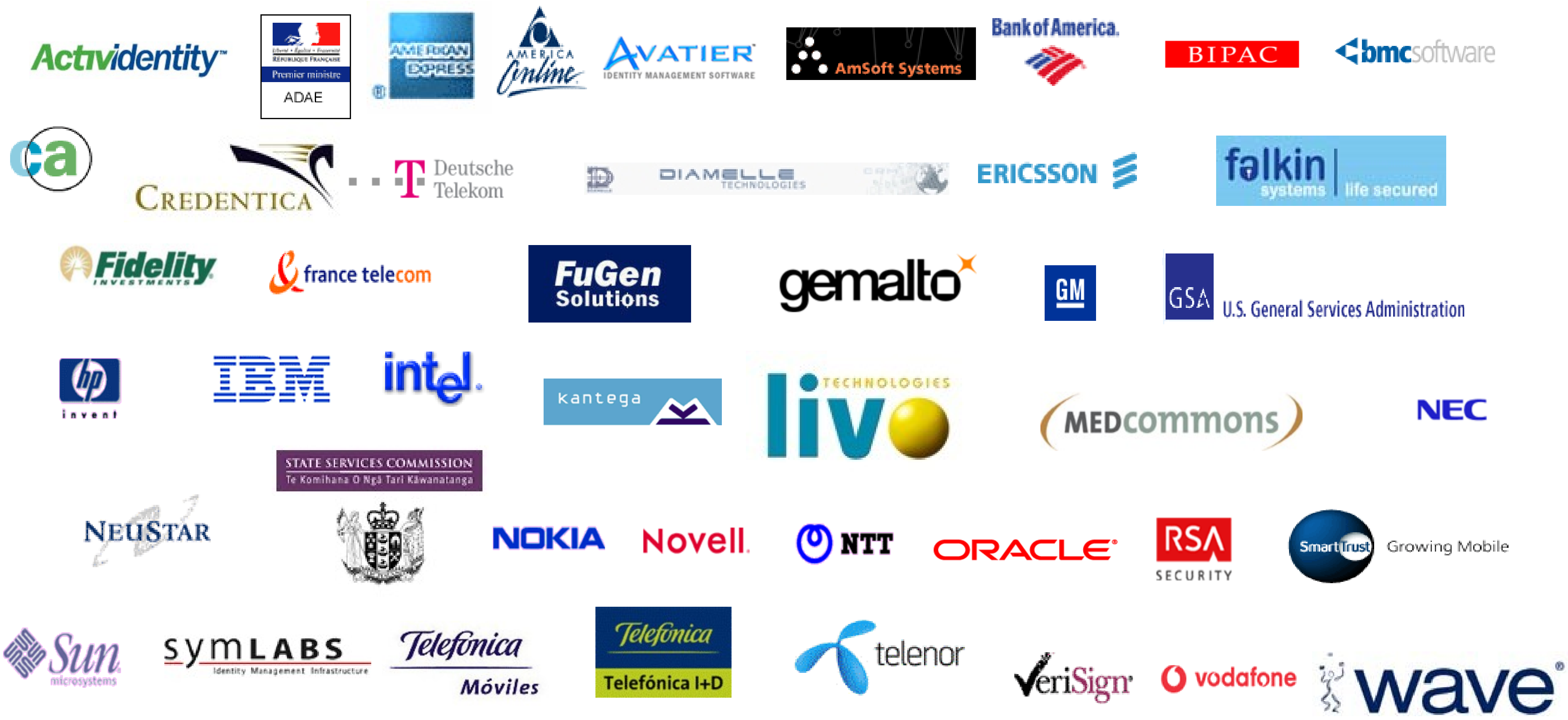
- Consortium developing open standards
  - For federated identity management
  - In coordination with other standards groups
- Develops open specifications that anyone can implement
  - Liberty does not deliver specific products or services
- Conformance testing & certification to ensure interoperability
  - 30+ Liberty-enabled products and services currently available

LIBERTY ALLIANCE INTEROPERABLE

- Addresses business & policy issues of identity
  - Guidelines, best practices documents, checklists
  - Support for global privacy regulations built into specs

Who is the Liberty Alliance?

- Global collection of diverse member organizations representing leaders in IT, mobility, government, manufacturing, finance and consumer services. About 145 members total
- Management Board and Sponsor members include:

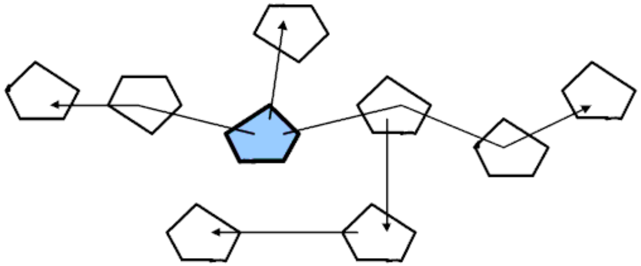


ITU-T

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?



*The Sopranos

ITU-T

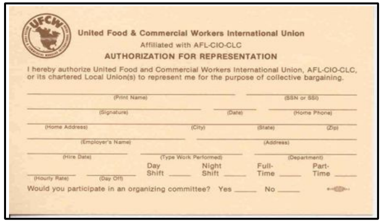
Architecture for Trust Management

Identity Management

Policy

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

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.

(Print Name) (SSN or SSI)

(Signature) (Date) (Home Phone)

(Home Address) (City) (State) (Zip)

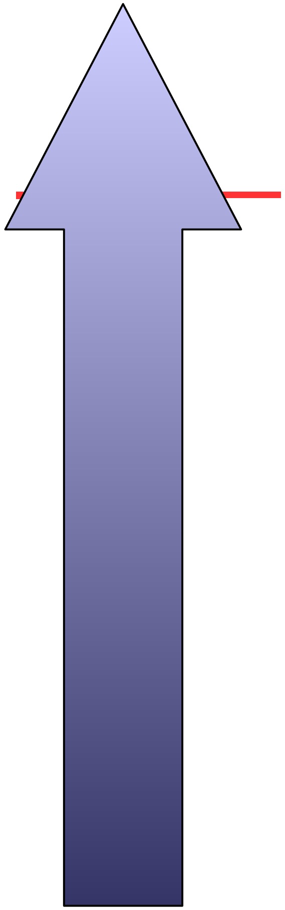
(Employer's Name) (Address)

(Hire Date) (Type Work Performed) (Department)

(Hourly Rate) (Day Off) Day Shift ____ Night Shift ____ Full-Time ____ Part-Time ____

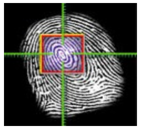
Would you participate in an organizing committee? Yes ____ No ____

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



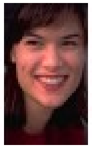
Security Management

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)

ITU-T

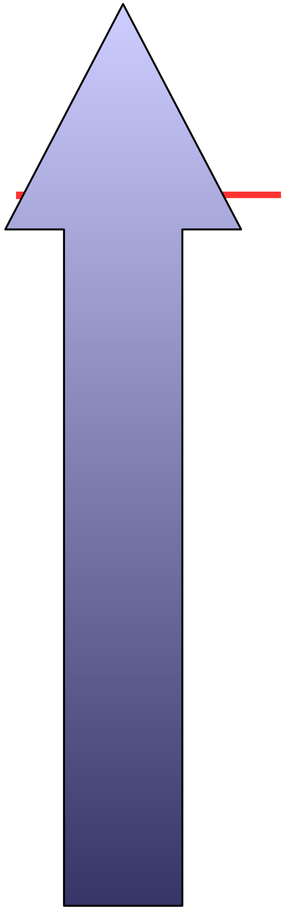
Architecture for Trust Management

Real World Example: Drivers License

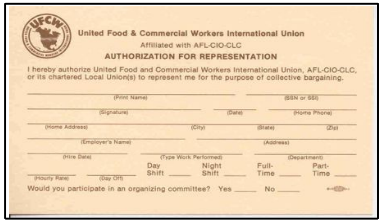
Identity Management

Policy

4. The fact that we do have police; the rules that allow me to drive with my national license in other countries



Authorization



United Food & Commercial Workers International Union
Affiliated with AFL-CIO-CLC
AUTHORIZATION FOR REPRESENTATION

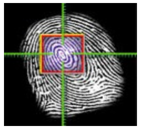
I hereby authorize United Food and Commercial Workers International Union, AFL-CIO-CLC, or its chartered Local Union(s) to represent me for the purpose of collective bargaining.

(Print Name) (SSN or SSI)
(Signature) (Date) (Home Phone)
(Home Address) (City) (State) (Zip)
(Employer's Name) (Address)
(Hire Date) (Type Work Performed) (Department)
(Hourly Rate) (Day Off) Day Shift ____ Night Shift ____ Full-Time ____ Part-Time ____
Would you participate in an organizing committee? Yes ____ No ____

3. The policeman will then see which kind of vehicle you are authorized to drive and if you are allowed to drive the one you are operating now

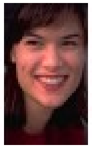
Security Management

Authentication



2. Assertion of validity: The policeman compares the document with you. Result: “A Yes/No answer”

Identity



1. Name, address, picture identify the driver and provide together with the document the credentials expressing that the carrier is identical to the person that passed the driving tests

ITU-T

Architecture for Trust Management

Digitally Speaking . . .

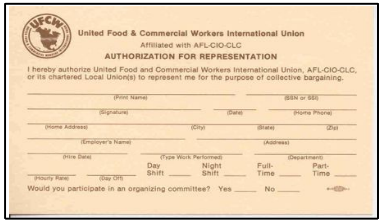
Identity Management

Security Management

Policy

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

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.

(Print Name) (SSN or SSI)

(Signature) (Date) (Home Phone)

(Home Address) (City) (State) (Zip)

(Employer's Name) (Address)

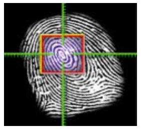
(Hire Date) (Type Work Performed) (Department)

(Hourly Rate) (Day Off) Day Shift ____ Night Shift ____ Full-Time ____ Part-Time ____

Would you participate in an organizing committee? Yes ____ No ____

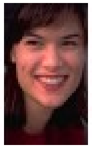
3. Determination of access rights to systems, applications and information: Match credentials against profiles, ACLs, policy

Authentication



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

Identity



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

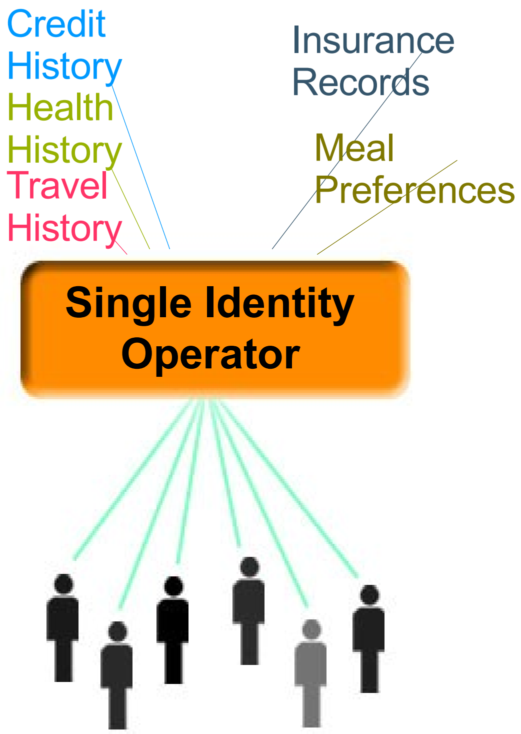
How People Will Trust Policies

- 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

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

Where to Safeguard User's Information



Credit History

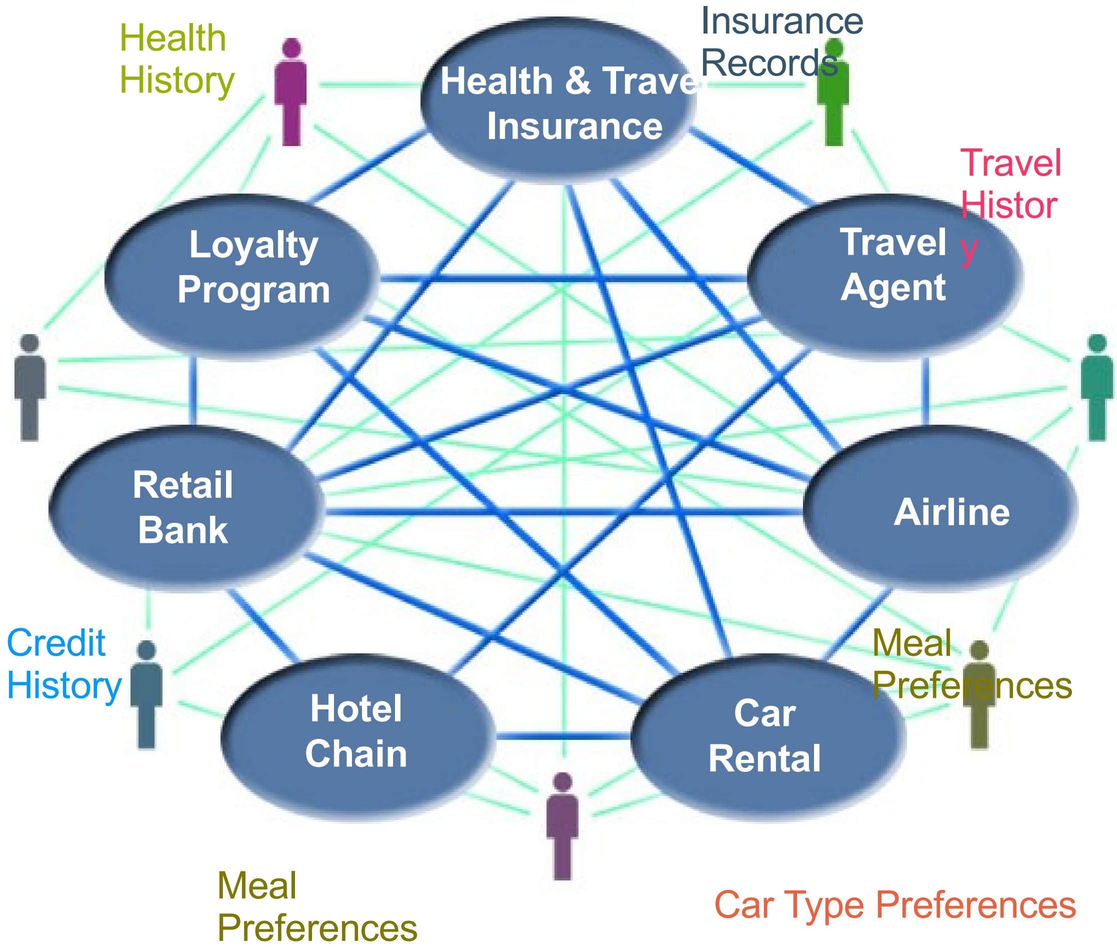
Health History

Travel History

Insurance Records

Meal Preferences

Single Identity Operator



Health History

Health & Travel Insurance

Insurance Records

Loyalty Program

Travel Agent

Travel History

Retail Bank

Airline

Credit History

Hotel Chain

Car Rental

Meal Preferences

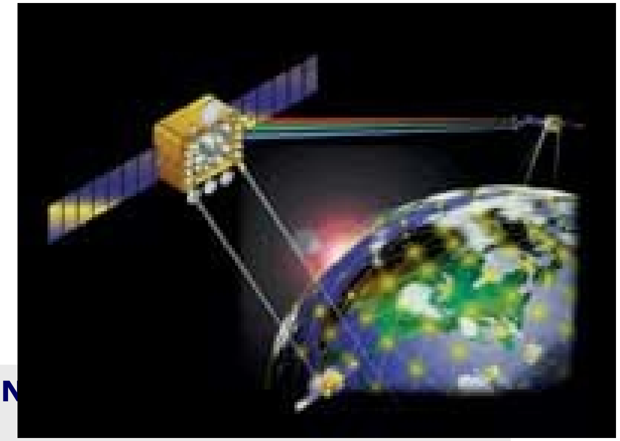
Meal Preferences

Car Type Preferences

ITU-T

Liberty 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

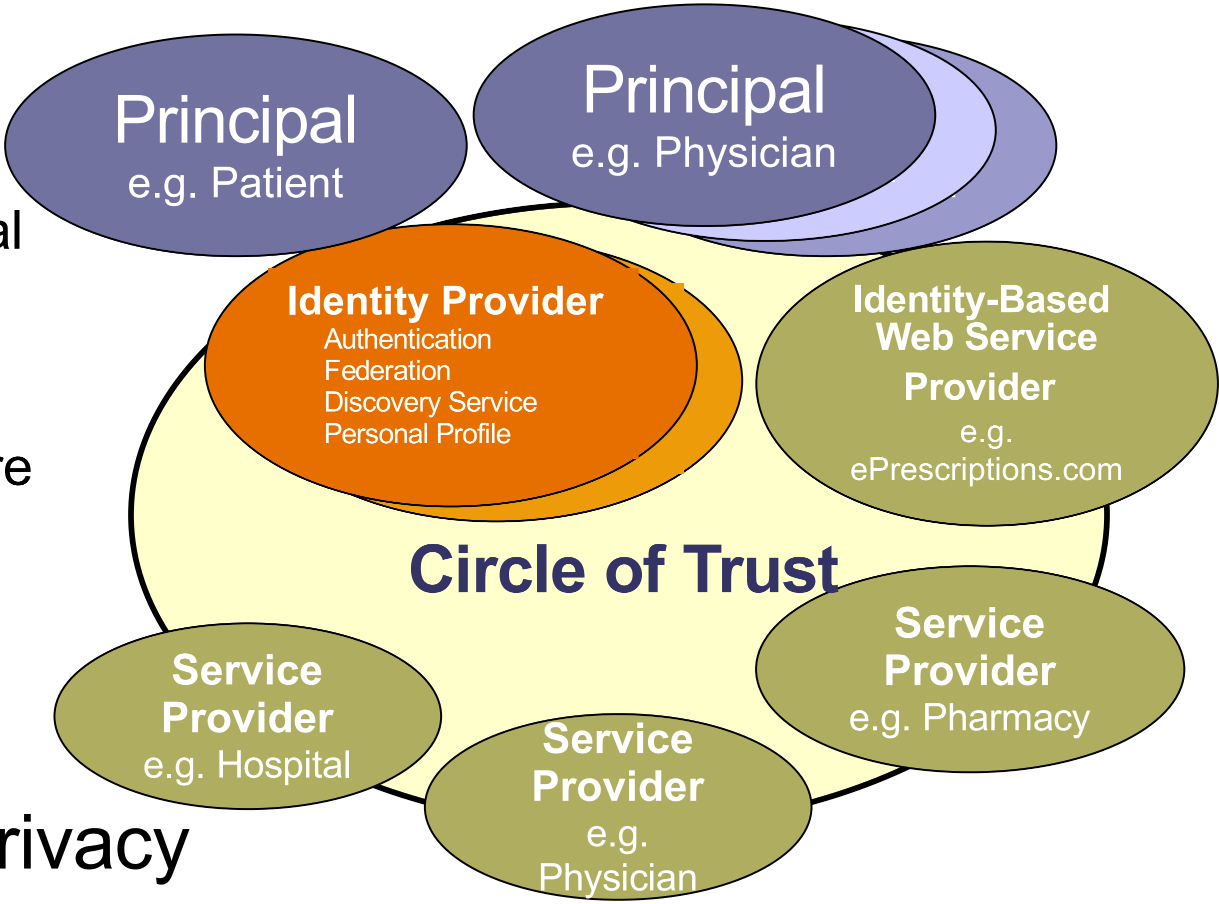


How it Happens

Circle of Trust – organizations and individuals

(example healthcare)

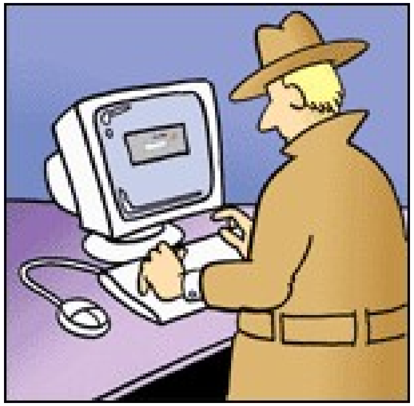
- Business relationships based on Liberty architecture & operational agreements
- Enables patients, physicians and healthcare organizations to safely share information in a secure and apparently seamless environment



Without violating privacy

The Liberty Advantage

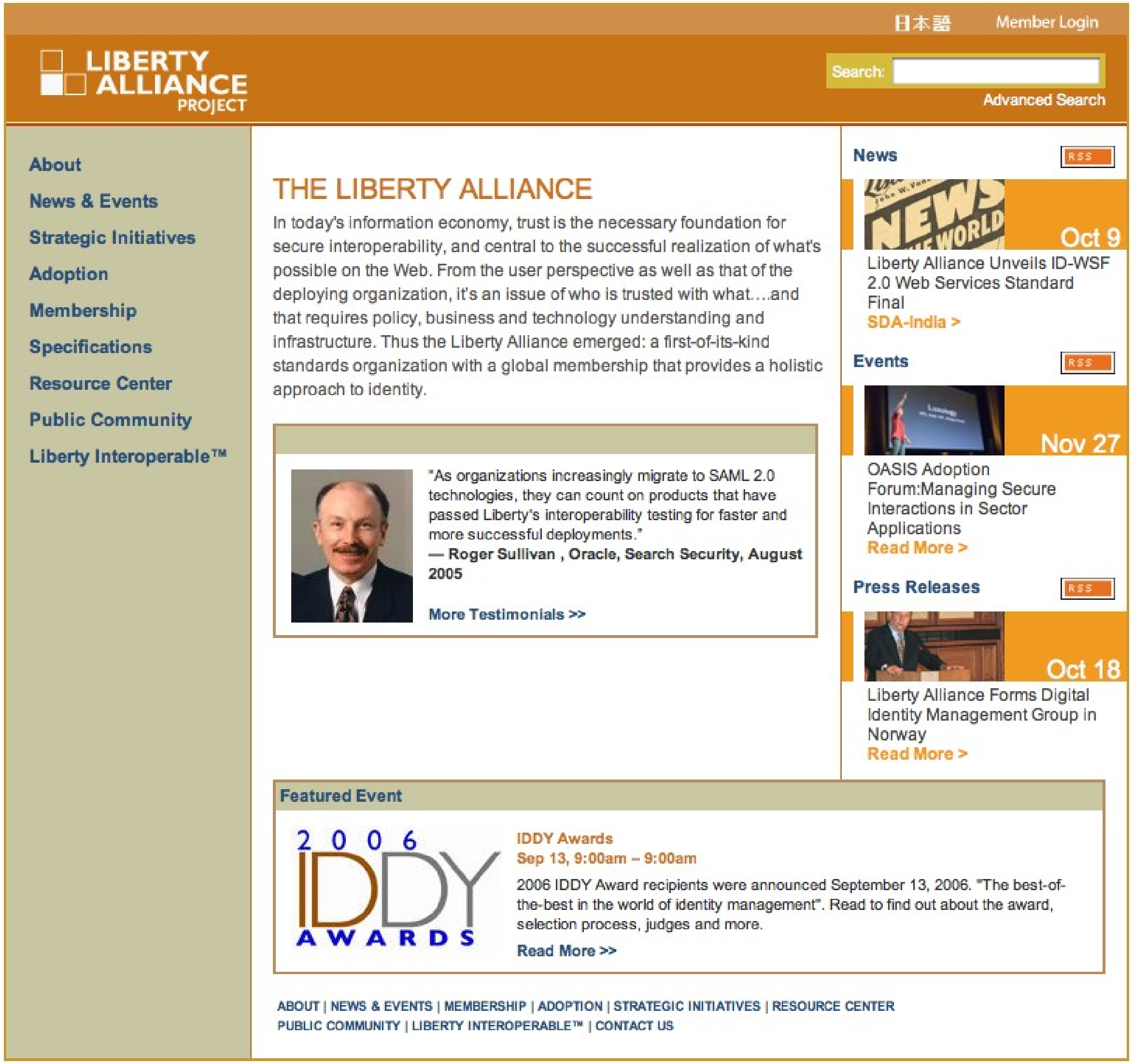
- Wide-spread adoption
  - ≤1 billion identities under Liberty protocols
  - Multiple vendor competition
  - Freedom of choice



- 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

ITU-T

More On Liberty: www.projectliberty.org



- About
- News & Events
- Strategic Initiatives
- Adoption
- Membership
- Specifications
- Resource Center
- Public Community
- Liberty Interoperable™

THE LIBERTY ALLIANCE

In today's information economy, trust is the necessary foundation for secure interoperability, and central to the successful realization of what's possible on the Web. From the user perspective as well as that of the deploying organization, it's an issue of who is trusted with what....and that requires policy, business and technology understanding and infrastructure. Thus the Liberty Alliance emerged: a first-of-its-kind standards organization with a global membership that provides a holistic approach to identity.

"As organizations increasingly migrate to SAML 2.0 technologies, they can count on products that have passed Liberty's interoperability testing for faster and more successful deployments."
— **Roger Sullivan , Oracle, Search Security, August 2005**

More Testimonials >>

News RSS

Oct 9
Liberty Alliance Unveils ID-WSF 2.0 Web Services Standard Final
SDA-India >

Events RSS

Nov 27
OASIS Adoption Forum:Managing Secure Interactions in Sector Applications
Read More >

Press Releases RSS

Oct 18
Liberty Alliance Forms Digital Identity Management Group in Norway
Read More >

Featured Event

2006 IDDY AWARDS

IDDY Awards
Sep 13, 9:00am – 9:00am

2006 IDDY Award recipients were announced September 13, 2006. "The best-of-the-best in the world of identity management". Read to find out about the award, selection process, judges and more.

Read More >>

ABOUT | NEWS & EVENTS | MEMBERSHIP | ADOPTION | STRATEGIC INITIATIVES | RESOURCE CENTER
PUBLIC COMMUNITY | LIBERTY INTEROPERABLE™ | CONTACT US

Liberty Adoption

- T-Com "Netzausweis" (1st prize IDDY award)
- American Express
- General Motors & Fidelity Investment
  - Portal B2E
- Vodafone "Vodafone live!"
- France Telecom
  - Mobile phone c
- Radio@AO
- AD
  - portal
- Sun & BIPAC, Sun & ext. HR
  - Services outsourcing

More than one billion Liberty-enabled identities and devices by the end of 2006…and that's just what we know about

Sessions@AOL
Exclusive studio recordings

Coming Up:
More of your favorite artists

Related Station: Eclectic XL

Artist: Various
Song: Top Hit
Album: Sessions@AOL
Time Remaining:1:18

Find Out More:
More about this artist

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

Examples of Identity Projects

BIOSECURE

Biometrics for Secure Authentication

Project Fact Sheet

TRASER

Identity **based tracking and web-services for SMEs**

fidis

The Future of *Identity* in the Information Society

PRIME

Privacy and Identity Management for Europe

guide

Government User IDentity for Europe

FIDELITY

Federated Identity Management based on LIBERTY

Summary

- In most projects *technology* was rarely the issue
- Legal and business agreements are the hard parts
- It is mandatory to use an open standards based approach
- Shop for Liberty interoperable products and solutions
- Liberty specifications are free and there to be used
- Become a member to contribute to the Liberty work

LIBERTY ALLIANCE PROJECT

LIBERTY ALLIANCE INTEROPERABLE

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 customer's information
- Federated Identity scales much better than hierarchical approaches. Truly enhances business agility
- Join the Alliance at http//:www.projectliberty.org