Agenda

- 9.30-9.45: Introduction to Liberty
  - Donal O’Shea, Executive Director, Liberty Alliance
- 9.45-10.30: How Liberty addresses Mobile Technical Needs
  - Timo Skyttä, Vice President, Liberty Alliance & Senior Manager, Nokia
- 10.30-11.00: Identity, Trust and Privacy Management and the Role of the Liberty Alliance
  - Hellmuth Broda, CTO Strategic Insight Office, Sun Microsystems
- 11:00-11.30: How Liberty addresses Mobile Business Needs
  - James Vanderbeek, Chair of MRD, Liberty Alliance & Senior Manager, Vodafone
- 11.30-12.30: Product Demonstrations and Case studies
  - Vodafone Trials and Proof of Concept demonstrations
    - Maurice Martin, Vodafone
  - Orange – Liberty-enabled solution for 50+ million subscribers
    - Pierre-Yves Cloux, Orange
- 12:30-12:50 Question and Answer Session
  - Moderator: Simon Nicholson, former Chair of Liberty BMEG and Director at Sun Microsystems
- 12:50-13:00 Lottery
Introduction to Liberty

Donal O’Shea
Executive Director, Liberty Alliance
What is the Liberty Alliance?

The Liberty Alliance is the only global body working to define and drive open technology standards, privacy and business guidelines for federated identity management.
Value Proposition and Members

- Need to be connected anytime, anyplace - without compromising security or control of personal information

- Liberty Alliance provides the technology, knowledge and certifications to build identity into the foundation of mobile and Web-based communications

- 150+ diverse member organizations:
  - Government organizations
  - End-user companies
  - System integrators
  - Software and hardware vendors
Board and Sponsor Members
Mobile Membership Momentum

- More than 400 million mobile customers:

- 80% of the SIM card industry:

- 55% of Mobile network infrastructure, and 85% of WCDMA network infrastructure:

- Around 50% of the mobile phone market:
Activities

- Technical Specifications and Implementation Guidelines
- Interoperability and conformance testing
- Business guidelines and case studies
- Policy guidelines
- Developer resources and User Groups
- Adoption and evangelism
- Liaison and collaboration with other organizations
Management Board

- Defines Mission / Scope
- Drives Execution Timetable
- Allocates Budget

Staff

Marketing
- Determines market requirements for Alliance core specifications
- Drives Business Guidelines
- Drives positioning and outreach to media, analysts and external organizations

Technology
- Understands current standards; drives convergence
- Delivers, maintains & evolves core Liberty specifications

Policy
- Policy / regulatory environment input
- Helps design audits compliance approach
- Liaison to govt. and external policy organizations

Services
- Defines & manages process for creating new service specifications
- Includes gathering of market requirements as well as specification development

Conformance
- Defines and manages process for validating vendor interoperability
- Manages Conformance Testing Program
Timeline of Achievements

Q3/2002
- ID-FF 1.0 completed

Q2/2003
- Public IOP with 20 products
- ID-FF 1.1 contributed to OASIS
- First Business Guidelines

Q4/2003
- Conformance program
- Services Group formed

Q1/2005
- ID-WSF2.0 draft
- SAML2.0
- Legal framework document
- New mobile business guidelines

Q2/2004
- 9 products pass Liberty conformance testing
- Collaboration with 6 new industry bodies

Q3/2004
- Public IOP of ID-FF & ID-WSF (10 companies)

Q4/2004
- Strong Authentication work starts
- 12 products pass Liberty conformance testing, of which 5 for ID-WSF

Q1/2004
- First ID-WSF implementations announced
- Mobile Business Guidelines and ID Theft study

Q4/2003
- 9 products pass Liberty conformance testing
- ID-FF 1.2 contributed to OASIS

Q1/2003
- Strong Authentication work starts
- 12 products pass Liberty conformance testing, of which 5 for ID-WSF

Q2/2004
- 9 products pass Liberty conformance testing
- Collaboration with 6 new industry bodies

Q3/2004
- Public IOP of ID-FF & ID-WSF (10 companies)
Most Recent Announcements

- Availability of ID-WSF 2.0 Drafts, and convergence of Identity Federation into SAML 2.0 (February 11)

- Availability of New Mobile Business Guidelines and EU-Focused Legal Framework (February 14)
Liberty Alliance Interoperable Products

- Current products listed at the Liberty Alliance Web site:
  http://www.projectliberty.org/about/enabledproducts.php

- The following member companies offer Liberty Alliance interoperable products (passed the conformance tests):
Examples of Liberty-Enabled Deployments

- AOL,
  - Identity Web services Radio and Photo applications

- France Telecom
  - Orange – Identity Federation Framework for 50 million mobile subscribers
  - Wanadoo – Federated micro-payment service for 10 million French online subscribers
Examples of Liberty-Enabled Deployments

- **General Motors**
  - Uses federated identity to simplify outsourcing and improve internal process efficiency
  - Within the company, different portals can be accessed by means of Single Sign-On

- **Bluewin**
  - Largest Internet Service Provider in Switzerland
  - Swisscom subsidiary
  - Circle of Trust enabled from the Bluewin portal for 2 million customers
>400 million
Liberty-enabled identities and clients

2005 estimate, source: Liberty Alliance
How Liberty addresses Mobile Technical Needs

Timo Skyttä
Vice President, Liberty Alliance
Senior Manager, Standardisation, Nokia
The role of Mobile Content is ever growing
- Mobile Content will come from Internet domain
- Provided by multi-national companies with well recognized brand

Strong and growing industry interest - Operators are looking for an efficient solution for 3rd party/service provider interfacing

In order to provide
- Faster integration work and lower costs
- Easier access to more users / new revenues via operator partnerships
- Solve the inter-operability issues among services providers

Generally, Internet – Mobile convergence taking place via Web Technologies
High-level ecosystem requirements

• Identity Management framework
  • To solve privacy issues
  • To be able to link different identities (telco, internet) with each other
  • To be able to authenticate and authorise transactions in non-trusted/unsecured environment
  • To facilitate easy of use - avoiding multiple registrations to services

• Easy and standard interfacing to 3rd parties using main stream Internet technologies (Web Services, xml/soap -> Liberty ID-FF/ID-WSF)
Some current challenges for Mobile Industry (related to Identity Management)

- Consumer awareness and concern over generic privacy and misuse use of personal information is growing, need for a “trusted” environment
- A mass market phone doesn’t have full keyboard, and is not likely to have one in the foreseeable future -> information entry difficulties -> service adoption problems
- User’s want personalized services to get quicker access to the content they want, mobile phone screen is small, can present only a limited amount of information – personalization is key, do not compromise user’s privacy unnecessarily when doing this
- To solve Identity Management, including personalized service access, do not create a mobile specific, but a mobile aware solution. This drives adoption both in Mobile and Fixed internet
- Make the life of user and service/content provider easy, but trusted and secure

---

- Number portability makes it difficult to associate a phone number to a certain provider of services – needs to invent a new reference mechanism
- Tightening privacy legislation in EU – use of MSISDN (phone number) as an identifier automatically attached to outgoing HTTP requests is not an option
The "Mobile Internet" - challenges

**Enterprises, Internet Service Providers**
- High integration costs for authentication, charging, personalization
- "Mobile Internet" in isolation from the Internet

**Mobile Operators**
- Large investments in service infrastructure but cross-industry, end-to-end offerings to Internet players are yet to be brought to market

**Users, Application developers**
- Operator environment always needs to be understood
- Connectivity to Internet and Extranet services challenging

---

**Application Development**
- Fragmentation, loss of mass-market appeal

**Charging**
- **Presence, Location**
- **Profile**
- **Messaging**
- **Authentication**
- **Browsing**

**Client Applications**
- xSP 1
- xSP 2
Web Services Concept

xSP’s, Enterprises
- Easy integration. Less costs.
- Less sensitive to differences between operators
- Services more attractive through single sign-on

Mobile Operators
- Easy integration. Easy for xSP to join operator portal
- More revenue from services. More traffic

Developers, ISV’s
- More value for customers because more services and better user experience
- Privacy protection

- Standard WS Framework (Liberty)
- Application Development
- Client Applications
- Web Services Middleware

- Charging
- Presence, Location
- Profile
- Messaging
- Authentication
Why is Federated Important?

**Centralized Model**
- Network identity and user information in single repository
- Centralized control
- Single point of failure
- Links similar systems

**Open Federated Model**
- Network identity and user information in various locations
- No centralized control
- No single point of failure
- Links similar and disparate systems
<table>
<thead>
<tr>
<th>Separate Cards with Each Bank</th>
<th>Linked Cards within Bank Networks</th>
<th>Seamless Access Across all Networks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bank A ATM Card</td>
<td>Bank ATM Network A</td>
<td>Bank A ATM Card</td>
</tr>
<tr>
<td>Bank B ATM Card</td>
<td>Bank ATM Network B</td>
<td>Bank B ATM Card</td>
</tr>
<tr>
<td>Bank C ATM Card</td>
<td>Bank ATM Network C</td>
<td>Bank C ATM Card</td>
</tr>
</tbody>
</table>

**Individual Accounts with Many Web Sites**

**Federated Accounts within Circles of Trust**

**Linkage of Circles of Trust**
Federated Identity Management

- Federation reflects how relationships are kept in the real-world
  - Not all identity information is held in one place
  - No centralized single point of failure
  - Opportunity for any trusted business or entity to become a trusted identity provider
  - More than single sign-on
  - It’s how personal information is authenticated, shared and managed
<table>
<thead>
<tr>
<th>Liberty's Architecture</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Liberty Identity Federation Framework (ID-FF)</strong></td>
</tr>
<tr>
<td>Security Assertion Markup Language (SAML) 2.0</td>
</tr>
<tr>
<td>Enables identity federation and management through features such as identity/account linkage, simplified sign on, and simple session management</td>
</tr>
<tr>
<td><strong>Liberty Identity Services Interface Specifications (ID-SIS)</strong></td>
</tr>
<tr>
<td>Enables interoperable identity services such as personal identity profile service, contact book service, geo-location service, presence service and so on.</td>
</tr>
<tr>
<td><strong>Liberty Identity Web Services Framework (ID-WSF)</strong></td>
</tr>
<tr>
<td>Provides the framework for building interoperable identity services, permission based attribute sharing, identity service description and discovery, and the associated security profiles</td>
</tr>
<tr>
<td>Liberty specifications build on existing standards (SAML, SOAP, WS-Security, XML, etc.)</td>
</tr>
</tbody>
</table>
Before Identity Mgmt

- Timo must log-in to portal with an ID and password
- After selecting a TV site he must log-in again
- Log-in’s like above can require 80+ clicks and more than 30 seconds of time on a typical mobile phone keypad
- Users often give up in frustration, limiting use of mobile data services
After Identity Mgmt

- Timo has chosen to link his three favorite sites
- When Timo logs into the portal, the mobile operator automatically authenticates him
- Timo clicks on the TV and is automatically signed-on
- Timo goes to his bookmarks and instantly logs-on to his email
Liberty Federation Use Case

0. Service, please!

1. Request assertion

2. Who are you?

3. I’m Lois

4. Authentication assertion
Liberty ID-FF 1.1/1.2 Single Sign-On
Liberty Enabled Client/Proxy (LECP) for WAP 1.*

- "Legacy Phones"
- Network level authentication (MSISDN, IP address, etc.)
- "Legacy Phones" sends an HTTP request.
- The request is intercepted by a device labeled as "Operator".
- The Operator sends a Liberty Authn request to the Identity Provider.
- The Identity Provider responds with an SAML assertion.
- The response is sent back through the Operator to the xSP.

Diagram: A flowchart illustrating the single sign-on process involving Liberty Authn request and response with SAML assertions.
Liberty ID-FF 1.1/1.2 Single Sign-On
Browser Post/Artifact profiles for WAP 2.0

“Smart phones”

Network level authentication (MSISDN, IP address, etc.)

Operator

Identity Provider

Authentication by any means

Http request

Liberty Authn request

Authn req

Authn resp with SAML assertion

Authn resp with SAML assertion

xSP
Identity Federation Framework

<table>
<thead>
<tr>
<th>Identity Federation Framework</th>
<th>ID-FF 1.1/1.2, SAML2.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enables Identity federation and management through features such as identity/account linkage, simplified sign on, and simple session management</td>
<td></td>
</tr>
</tbody>
</table>

- Spec. released 7/02
  - Browser and WAP profiles
- Opt-in
- Single Sign-on and Log out
- Profiles for “thin” clients
- Open source Java based IPL
- Submitted to OASIS SAML TC
- RSA Interop. Event 4/03
- +30 products available
- Next Generation: SAML 2.0
Personalized Service Access – finding food when hungry

During the transaction fav-cuisine.com never learns my real identity, in fact it most likely does not need to know any identity at all, just be able to access information about me.
What is ID-WSF?

- Framework for locating and invoking identity based Web services
- Identity Web services:
  - Associated with a Principal’s Identity
  - Can be Invoked using a Principal’s Identity
- Permissions-based Attribute Sharing
  - Invoking Services under control of user
    - At the DS and at the WSP
- Interaction Service to reach to user
ID-WSF – Key Concepts

- **Web Services Client (WSC):** typically, the invoker/consumer of an identity service
- **Web Services Provider (WSP):** typically, the provider of an identity service
- **Data Services Template (DST):** provides an extensible framework to produce new Identity Services above the protocol stack, allowing interoperability e.g.: ID-Personal Profile and ID-Employee Profile
- **Discovery Service (DS):** Facilitates the registration and subsequent discovery of Identity services
The Identity Federation and Identity Web Services Frameworks

**ID-FF**: The SP interacts with the IdP through Jane’s browser to obtain the identity credential for Jane.

**ID-WSF**: The SP (acting as a WSC) interacts with the DS and Jane’s WSPs in order to invoke services at the WSPs on Jane’s behalf.
Hey, CoolToys.com wants to buy some electronics.

Is this OK?

Yes, that's fine.

Hey, CoolToys.com wants to charge $5,235.03. Is this OK?

Ask Jane if... Is OK?

Jane says it's OK.

Transaction Approved

Hmm... Jane's rules say that if the charge is over $300 to confirm with her...
Identity Web Services Framework

<table>
<thead>
<tr>
<th>Identity Federation Framework</th>
<th>ID-FF 1.2, SAML2.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enables Identity federation and management through features such as identity/account linkage, simplified sign on, and simple session management</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Personal Profile</th>
</tr>
</thead>
<tbody>
<tr>
<td>Employee Profile</td>
</tr>
</tbody>
</table>

Identity Web Services Framework (ID-WSF)

Provides the framework for building interoperable identity-based web services.

- **Discovery, Interaction**

- **Permission based attribute sharing**
- **Services Template**
- **Personal & Employee Identity Profiles**
- **Released Nov `03**
  - Available for public download
- **Already supported in 5 conformance-tested implementations**
Identity Service Interface Specifications

<table>
<thead>
<tr>
<th>Identity Federation Framework</th>
<th>Service Interface Specifications (ID-SIS)</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID-FF 1.2, SAML2.0</td>
<td>Personal Profile</td>
</tr>
</tbody>
</table>

- Enables Identity federation and management through features such as identity/account linkage, simplified sign on, and simple session management.

Identity Web Services Framework (ID-WSF)

- Provides the framework for building interoperable identity-based web services.
- Discovery, Interaction

- Interface and data schema
- Horizontal or vertical
- Will be defined in parallel
- First service tracks:
  - Personal Profile
  - Employee
  - Contact Book
  - Geolocation
  - Presence
  - Gaming

- (SAML) HTTP WS-Security WSDL XML Enc
- WAP XML SSL/TLS SOAP XML Sig
Liberty Web Services enables operator's position on the Internet

- PC Applications
- Device Applications
- Portal
- Authentication & WS Discovery
- Messaging
- Location
- Charging
- Payment
- SME’s
- ‘Fortune 500’
- Service Providers (Web sites)
- Credit Card Companies
- Banks
- Exposed Operator
- Mobile Assets

Legend:
- Consumer or Corporate Applications
- Web services Provider
- Web services Consumer
Identity, Trust and Privacy Management and the Role of the Liberty Alliance

Hellmuth Broda
Dr. Hellmuth Broda
Spokesperson, Liberty Alliance
Chief Technology Officer, Strategic Insight Office
Sun Microsystems Inc.
The Changing Ordering Paradigm*

- Digital identity is becoming the ordering principle for network computing

Who is this guy? Can we trust him?

*) This and the next 3 slides based on ideas from a presentation by Phil Becker, Digital ID World
Importance of Identity

- Why is the loss or lack of identity so disruptive?
- Without identity we have no ability to organize or control activity
- Identity is the central organizing paradigm for networks
How Did Computing Live Without Identity?

- *Location* was an implicit proxy for Identity
Role of Identity

- **While**
  - Perimeters dissolve
  - Applications get distributed
  - Access is anywhere, anytime, through any device . . .

- **Identity enables security, control, manageability and accountability in a distributed network**
What keeps customers from doing commerce over the internet?

- Know who you are talking to (identity crisis)
- Globally accepted and secure payment systems
- Risk but not trust management
- Privacy concerns
Identity Mess in Real Life

Focus
23.Aug.04
Today’s Collection of Net Identity Silos

Joe’s Fish Market.Com
Tropical, Fresh Water, Shell Fish, Lobster, Frogs, Whales, Seals, Clams
What Has to Be Identified?

- Persons (real people) in their roles
- Legal entities (companies, agencies, corporations, . . .)
- Things (air quality monitoring sensor, traffic counter, . . .)
- RFID tags; DRM
- Software services, agents, . . .
A Network of Things: Auto ID – RFID Tags

Note: By 2005 WalMart will only accept merchandise with RFID tags attached!
Privacy Concerns Kill Or Delay Projects

- **Swiss EasyRide**
  - Delayed also due to consumer concerns on the privacy of the location and time information

- **Benetton RFID tags in clothes' labels**
  - Public consumer group pressure led Benetton to abandon plans

- **“Consumers Against Supermarket Privacy Invasion and Numbering”** delay Prada store RFID project
  - Project is for up-to-date inventory

Source (2,3): Wired News 8 Apr 03
Identity Theft – Fastest Growing Crime

- Fed. Trade Commission is worried
- Today, solutions offered only for parts of the problem
- Ebay examples
Common Security and Privacy Concerns

- Business, agencies, end-users are losing trust in web-based services
- Privacy concerns
  - 60% won't buy on-line
  - Fear of information correlation and mis-use
- Security failures
  - ID-theft is #1 complaint
  - Bad password management aids hackers
Dangers On the Net Today

- Identity Theft
- Phishing
- Spam
- Data on the net
  - Easy and inexpensive to gather, store, analyze, transmit and re-use
  - Inherently global – no boundaries
How We Can Build Trust

- The biggest concern of the principal/patient/customer is
  **privacy**

- Privacy is not a technical issue

- Privacy does not mean that “nobody knows nothing about me”

- It is about managing the trust of the principal/patient/customer by sticking to the agreed scope and holding the information in trust

- What could an architecture for privacy and trust management look like?
Definitions

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

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

Assertion of validity of a set of credentials. Credentials express a person’s identity. “A Yes/No answer”

Basic set of information that creates a “unique” entity (a name with a corresponding set of attributes).
4. The fact that we do have police; the rules that allow me to drive with my national license in other countries

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

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

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
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 are guaranteed and certified by an approved public or private agency (federal data protection agency; TÜV; Chamber of Commerce, Postal Service, or other basic service provider, . . .)

- Policies and their transactions are insured. Insurances cover for possible policy violations and fraud

- Liability and non-repudiation solved

Trust is based on policies and the audit of those -- *not* just on security
Liberty Alliance solves the identity crisis

- The only global body working to define and drive open technology standards and guidelines for federated identity
- Addresses business, policy and technical issues associated with federated identity
- Alliance of global organizations working together to enable the deployment of identity-based web services
- Reduces the complexity in e-Business
The Importance of Identity

- The most basic element in a high-value relationship with customers, employees, citizens or business partners
- Has to be managed with great care to proactively fight fraud and identity theft
  - Secure solutions are essential
  - User consent must be supported
- Common mechanisms to handle Identities are required:
  - Technically, to enable interoperability and seamless user experiences
  - Legally, to enable a business relationship between different entities in a distributed environment
The Importance of Identity

- Proper Identity Management makes a difference!
  - Fraud and Identity Theft prevention:
    - A distributed system can help, and so can the attribute and profile information sharing.
  - Secure and trusted usage and sharing of:
    - Personal and Business identity information
    - Financial data
    - Employee and Company data for both remote and local intranet domain access
**Key Concepts**

- **Federation** – The act of establishing a relationship between two or more entities, an association comprising any number of Service Providers and Identity Providers.

- **Principal** – A person or “user”, a system entity whose identity can be authenticated.

- **IdP, Identity Provider** – A service which authenticates and asserts a Principal’s identity.

- **Single Sign-On (SSO)** – The Principal’s ability to authenticate with one system entity (Identity Provider) and have that authentication honoured by other system entities, often Service Providers.

Further definitions from the Glossary, found at: [http://www.projectliberty.org/specs/liberty-glossary-v1.3.pdf](http://www.projectliberty.org/specs/liberty-glossary-v1.3.pdf)
Key Concepts

- **Circle of Trust** – a group of service providers and identity providers that have business relationships based on Liberty architecture and operational agreements and with whom users can transact business in a secure and apparently seamless environment. Circles of Trust represent the second wave of identity federation, after SSO and federated account linking.

- **DS** – Discovery Service – a service which provides Identity based Discovery of Web Service Providers

- **IS** – Identity Service – a service invoked through or with a user’s identity

Further definitions from the Glossary, found at: [http://www.projectliberty.org/specs/liberty-glossary-v1.3.pdf](http://www.projectliberty.org/specs/liberty-glossary-v1.3.pdf)
Where to Safeguard User's Information

Single Point Model

- Credit History
- Health History
- Travel History

Open Federated Model

- Health History
- Insurance Records
- Meal Preferences
- Loyalty Program
- Travel Agent
- Airline
- Retail Bank
- Hotel Chain
- Car Rental
- Car Type Preferences
- Meal Preferences
- Credit History
- Travel History
Circle of Trust Concept
Appel à candidatures n°3 - 2004 : AMOA élaboration d’un dossier d’architecture de référence mettant en œuvre le modèle Liberty Alliance

Objet : Assistance à maîtrise d’ouvrage pour l’élaboration d’un dossier d’architecture de référence mettant en œuvre le modèle Liberty Alliance phases I et II

Pour s’inscrire :

- envoyer un courriel exclusivement à l’adresse suivante : adae@adae.pm.gouv.fr
- envoyer des documents de présentation de la société (références, CV...).

Date limite de dépôt de candidatures : jeudi 22 avril à 18h.
In general, Liberty enables the usage of existing, analyzed and well-known security mechanisms

Confidentiality
- Messages may need to be kept confidential and inhibit unauthorized disclosure, either when transit or when stored persistently

Integrity
- Messages need to arrive at the intended recipient with data integrity
- Unauthorized changes shall not be made without detection

Authentication
- May be required by a receiver to process the message; sender may require the authentication of the response

Anti-replay
- Message responses must correspond to message request (no “man in the middle” attack)

Privacy requirements
- Enabling the disclosure of personally identifiable information under user control
Security & Privacy Guidelines

- **ID-WSF Security & Privacy Overview**
  - An overview of the security and privacy issues in ID-WSF technology and briefly explains potential security and privacy ramifications of the technology used in ID-WSF

- **Privacy and Security Best Practices**
  - Highlights certain national privacy laws, fair information practices and implementation guidance for organizations using the Liberty Alliance specifications.
  
  final_privacy_security_best_practices.pdf

- **Legal Guidelines (coming up)**
Liberty Member Activities

- Technical Specifications and Implementation Guidelines
- Interoperability and public conformance testing
- Business guidelines and case studies
- Policy guidelines
- Developer resources and User Groups
- Adoption and evangelism
- Liaison and collaboration with other organizations
Privacy Enabled Trusted Third Party Transactions Are Achievable Now!
Who Does What? Business Opportunities (1)

- Identity Service Provider (national, international Example: HubID by Communicator)
- Business Relationship Management inside a Circle of Trust (national, international Example: Neustar)
- Management of relationships between Circles of Trust (national, international)
<table>
<thead>
<tr>
<th>Business Opportunities (2)</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Trusted Third Party Services (incl. Logistics) (national, international)</td>
</tr>
<tr>
<td>- Policy audit and seal of approval (national, international)</td>
</tr>
<tr>
<td>- Web page seal (international)</td>
</tr>
<tr>
<td>- Clearing</td>
</tr>
<tr>
<td>- International payment systems for small amounts</td>
</tr>
</tbody>
</table>
If we do not start to take privacy concerns seriously we might as well abandon web services.

Trust is the highest valued part of a business relationship.

We have to plan and build privacy management into our systems from the very beginning.
Privacy Needs to be Managed

- Like Security, Privacy cannot be just “installed” -- and forgotten
- It has to be continuously managed
- The published policies and the adherence to those to be regularly auditet
- Successful companies will have a Chief Privacy Officer (CPO)
What Liberty Can Help to Solve

- End-to-end identity management:
  - Identity theft
  - Phishing
  - Spam
- Builds
  - Trust with auditable privacy policies
  - Circles of trust for businesses, governments, and consumers
Outlook

- Identity Management will be as ubiquitous as TCP/IP
- Needed: Definition of secure, auditable and certifiable infrastructures to run Identity Services
- Needed: Definition of well documented and auditable identity management processes which can be certified
The Principal's Reaction We Want to Avoid . . .
Spread of Liberty
Is the “Calling of Our Time”

- George W. Bush January 20, 2005
Thank You

Hellmuth.Broda@Sun.COM
How Liberty Addresses Mobile Business Needs

James Vanderbeek
Senior Manager Strategy, Vodafone
Business Requirements Chair, Liberty Alliance
The Liberty Alliance is unique – it driven by members to solve business issues, not to specify technology for technology sake

- Mobile perspective is well represented
  - Membership
  - Relationship with standardisation bodies
- Newly released Mobile Business Guidelines provide legal framework and highlights business opportunities
New Business Opportunities
Customer Experience
Regulatory
Cost Savings
Access Control

- Access control to applications is a fundamental identity service in the mobile space and may be mobile or provide a bridge between mobile and fixed.

- **Target Markets**
  - Corporate VPNs, Home Banking, Government Portals...

- **Possible Formats**
  - One-time Password (OTP)
  - Challenge / Response
Access Control

24M Authentication Tokens or a possible…

- Size of Existing Market

**1.4 Billion Mobile Phones**

- Reduced Annual Cost of Authentication
  - Shared infrastructure reduces costs
  - Could approach the cost of passwords

<table>
<thead>
<tr>
<th>Service</th>
<th>Cost (€)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Password</td>
<td>14</td>
</tr>
<tr>
<td>Authentication Token</td>
<td>8-36</td>
</tr>
<tr>
<td>SMS Push</td>
<td>30</td>
</tr>
<tr>
<td>Mobile SIM</td>
<td></td>
</tr>
</tbody>
</table>

**Market Size**
If 1 person in 5 (20%) takes just 1 ID (e.g. Corp VPN or Home Banking), then the Market > 4B €
(280M Users * 15 €)
Remote Payment

- **Remote Payment is the fastest growing, most expensive method of payment**
  - Costs merchants twice what in-person payment does
  - Total Fraud market is many billion dollars

- **Who Pays for Fraud Now?**
  - Merchants pay over 2B Euros, or 90%, of fraud-related costs
    - Losses and Charge-back fees
  - Issuing banks will be liable under 3D Payment rules beginning 2005
    - Cannot pass costs onto credit/debit card holders
  - Users are not directly liable, but Identity Theft costs individuals on average $500 USD and 30 hours to correct per incident (US FTC, 2003)
Identity Services

Liberty provides a framework for permission-based and interoperable data services...

1. Where’s my closest open bank?
2. Who’s this person?
3. What’s the Location service for this person?
4. Where’s this person?
5. Can My Bank get your location data?
6. Here’s your closest bank. Enjoy

Identity Provider

My Bank Service

Location Provider

Discovery Service

Thanks!
“Identity” services = data services

Liberty provides a powerful framework for deployment of internal and third-party services enabling solutions for:

- Interoperability / Roaming
- Privacy Management
- Personalization
- Legacy terminals
New Business Opportunities
Customer Experience
Regulatory
Cost Savings
What my customer wants...

- Increased importance with the advent of higher value and more complex services
- Customers will need to “feel” they can trust service providers
- Better customer experience is a key element of creating and maintaining their trust
  - Ease of use
  - Empowerment
  - Protection / Security
Ease of use

- Mobile devices often have limited screen and keyboards
  - A simple log-on to a portal and e-mail may require over 80 clicks and too much time – many users will not attempt it…

- Liberty enables Single Sign-On that can reduce the above scenario to less than 6 clicks – other features include personalisation and form filling

- The better experience increase the likelihood of customers using the services
Empowerment / Privacy

- Customers are empowered through:
  - Ability to decide what services they wish to enable for SSO
  - Choice of who or what service information about them is provided
  - Flexibility to either set-up or decide transaction by transaction

- Maintaining and securing a customer’s privacy is a key element of trust
  - As already discussed, Liberty is very privacy focused with a separate group to focus on these efforts
    - SPAM
    - Identity Theft
    - Anonymity
New Business Opportunities
Customer Experience
Regulatory
Cost Savings
The lawyers say…

- Compliance with regulations and proactive movement makes liberty even more compelling:
  - Requirements not to send mobile number over the air
  - Data storage and sharing requirements
  - Need to show action on efforts like SPAM, identity theft and phishing
- Liberty provides more than specifications – outreach to major regulatory bodies and implementation guidelines assist deployments
New Business Opportunities
Customer Experience
Regulatory
Cost Savings
Where is the Money???

- The standard approach liberty provides to identity will yield cost savings
  - Elimination of silo approach will reduce development costs and reduce deployment time
  - Standards-based solutions will reduce integration costs and time
  - Less effort will be required for common look and feel to services
  - Developers and partners will benefit from single specification
  - More vendors – More choices = less cost
Demonstrations, Case studies
Q&A Session (Panel)
Federated Identity and Web services NOW:
- Interoperability between business partners
- Built on open standards
- Unique conformance program for Identity Management products – more than 30 successful product tests to date
- Device and platform agnostic

The only group to also address business and Public Policy issues of Identity and Web services:
- Business guidelines
- Privacy controls built into the specifications
- Privacy & security best practices, Legal framework guidance
- Enable compliance with global privacy legislation and industry regulations (i.e. Article 29, HIPAA)

Liberty collaborates with other standards organizations, privacy advocates, governments and policy groups
- Drives convergence