Liberty, Compliance, and Privacy

Dr. rer. nat. Hellmuth Broda
Distinguished Director and CTO, Strategic Insight Office, Sun Microsystems Inc
Spokesperson and Member, Business Marketing Expert Group, Liberty Alliance
The Changing Ordering Paradigm

- Digital identity is becoming the ordering principle for network computing
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
The Age of Firewall
Keep data within the firewall

The Age of the Intranet/Internet
Managing data inside and outside the firewall

The Age of the Extranet
Managing data through the firewall

The Future: Nothing but Net
Just Access and Entitlement
Understanding the Network

Everything with a digital heartbeat is connected... through dynamically formed relationships governed by privacy, security and trust policies.
Patriot Act/Patriot Act II
HIPAA
Hong Kong Data Protection Act
U.S. Privacy Act of 1974
SEC Rule 17a-4
SB-1386 (CA)
GLB
CAN-SPAM
Sarbanes-Oxley
EU Directives
AB-1950 (CA)
Basel II
Patriot Act/Patriot Act II
HIPAA
Hong Kong Data Protection Act
U.S. Privacy Act of 1974
SEC Rule 17a-4
SB-1386 (CA)
GLB
CAN-SPAM
Sarbanes-Oxley
EU Directives
AB-1950 (CA)
Basel II
Why Business Compliance?
What Is Business Compliance?

- Regulations and law that require companies to re-establish corporate accountability and reinforce confidence.
- US Government's reaction to scandals, such as Enron with laws like Sarbanes-Oxley.
- CEOs and CFOs of public companies now must swear under oath that the financial statements of public companies are accurate and complete.
- Audit committees must establish and maintain internal controls for financial systems and have them certified by public accountants.
What Does This Mean for Companies?

- New demands have been placed on the CEOs and CFOs
- The demands are transparency of the companies finances to the public investors
- Senior executives at companies (primarily public) have to personally attest to the quality of their organization's financial statement
- There is an aggressive schedule set by the new act to provide info to the US. Govt.
- Infractions are SEVERE. Penalty is likely to be felony convictions and substantial fines.
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
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, . . .
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
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 misuse
- 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
Privacy is how personal data is managed
Privacy is freedom from unauthorized intrusion
Privacy is informed choice by customers/employees
Privacy is the subject of law and regulation
Privacy is good data stewardship of personal data
Privacy is business enabling

Privacy is about **Respect** and ultimately **Trust**.
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?
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)
Architecture for Trust Management

Real World Example: Drivers License

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.

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

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.

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

Digitally Speaking . . .

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 a approved public or private agency (federal data protection agency; TÜV; 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
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
Where to Safeguard User's Information

**Single Point Model**
- Single Identity Operator
- Credit History
- Health History
- Travel History
- Insurance Records
- Meal Preferences

**Open Federated Model**
- Health History
- Insurance Records
- Travel History
- Loyalty Program
- Health & Travel Insurance
- Retail Bank
- Travel Agent
- Airline
- Hotel Chain
- Car Rental
- Credit History
- Meal Preferences
- Car Type Preferences
Circle of Trust Concept

Network Identity Provider

- Travel Agent
- Insurance
- Limo Service
- Bank
- Hotel Chain
- Airline
- Car Rental
- Tour Operator

External Federated Partner
- External Federated Partner
- External Federated Partner
- External Federated Partner
- External Federated Partner
- External Federated Partner
- External Federated Partner
- External Federated Partner
Common Security Principles in Liberty

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.
About the Document

- Developed by Liberty’s PPEG
- Based on an example Circle of Trust
- Presents a series of questions for Policy Decision Makers
- Complements Liberty Alliance Privacy and Security Best Practices
Document Organization

- Forming and Managing the Circle of Trust
- Business Purpose(s) of Data Collection
- Relevance of Data Collected and Shared
- Notice to the Principal
- Choices and Consent of the Principal
- Access and Accuracy of the Data
- Security
- Complaint Resolution
Even in Japan, the guideline was introduced
Links

- Deployment Guidelines

- Other Guidelines

- Membership Information
  - http://www.projectliberty.org/membership/

- Liberty Website
  - http://www.projectliberty.org
Privacy Enabled Trusted Third Party Transactions Are Achievable Now!

Request Token

Bank

Clearing

Hans

Logistics Partner

?32179
Privacy and Our Future

• 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 will have to be audited regularly
What Liberty Can Help to Solve

- End-to-end identity management combats:
  - 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
ありがとう
Thank You!

Hellmuth.Broda@Sun.COM