Identity, Privacy and Trust Management for e-Government

Dr. Hellmuth Broda
Chief Technology Officer
EMEA
Member, Sun Vision Council
Hellmuth.Broda@Sun.COM

itapa

Presence and Future

28 Oct 2003
Hotel FORUM
Bratislava

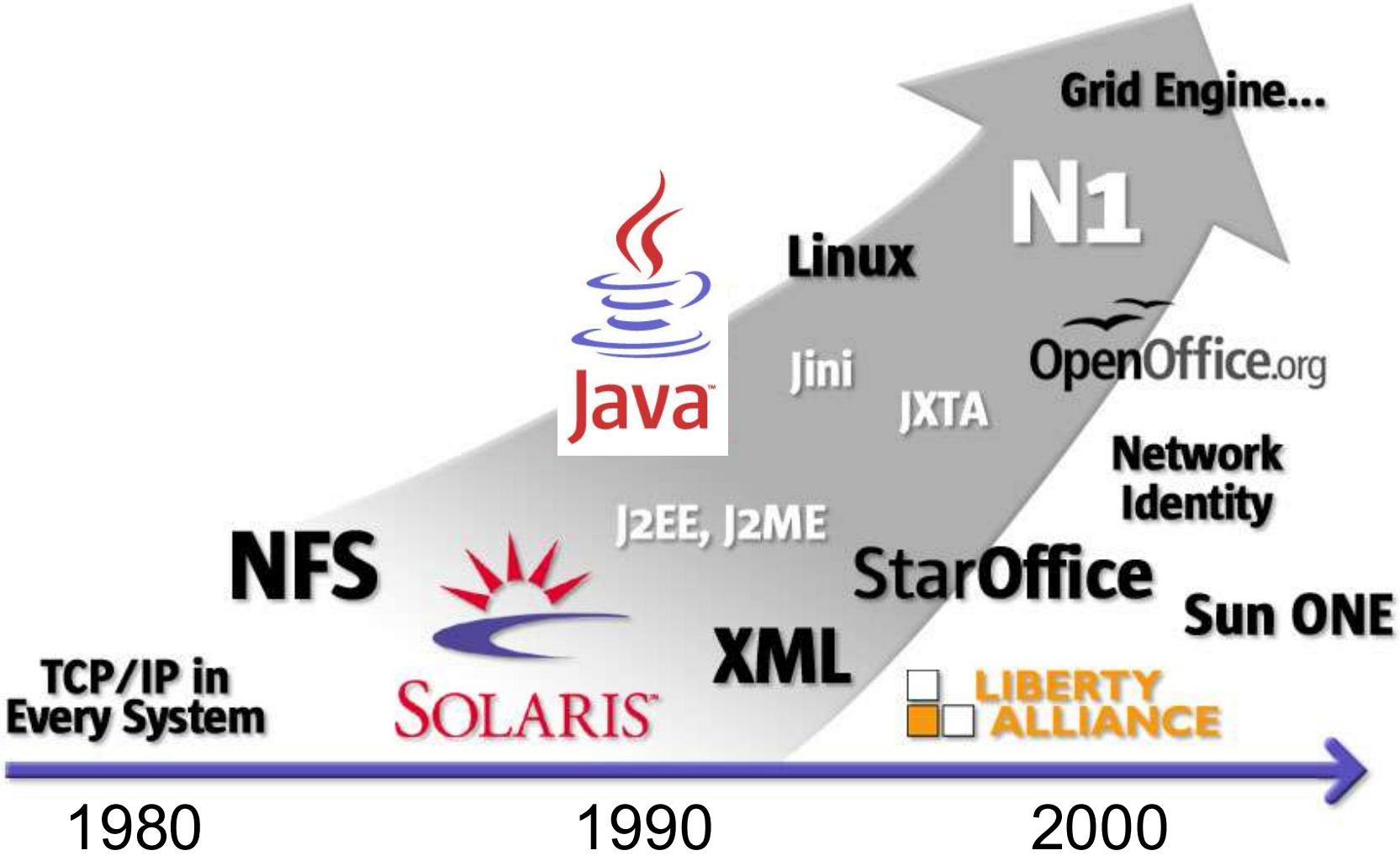
Sun microsystems
We make the net work.

We Make The Net Work

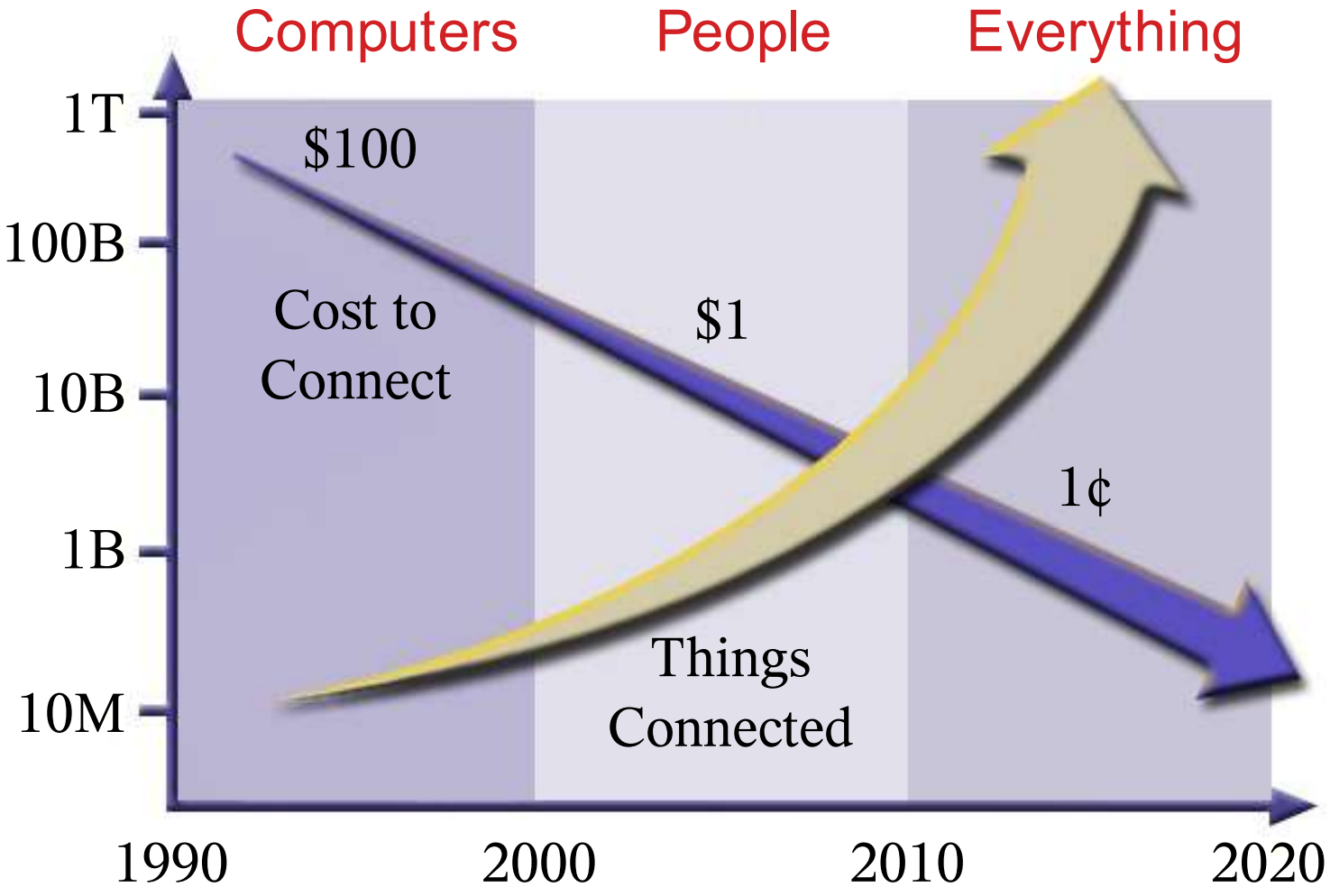
Sun's Vision

Everything and Everybody Connected to the Network

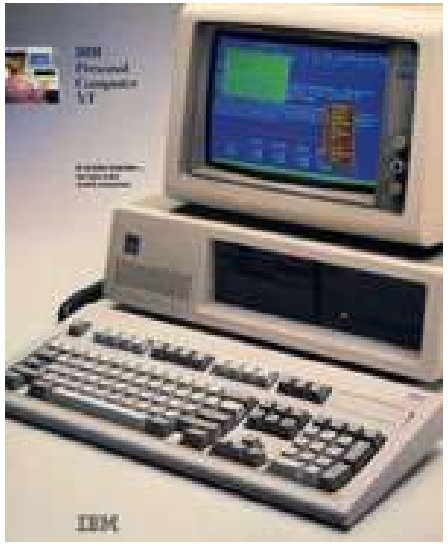
Innovation Pays



The Revolution

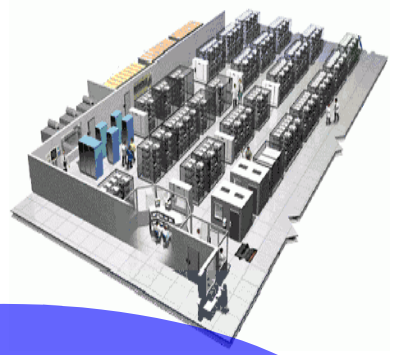


Networks will decompose the PC



Networked displays

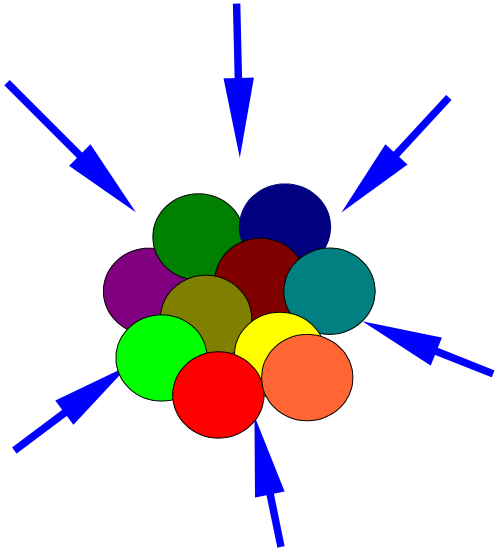
Services

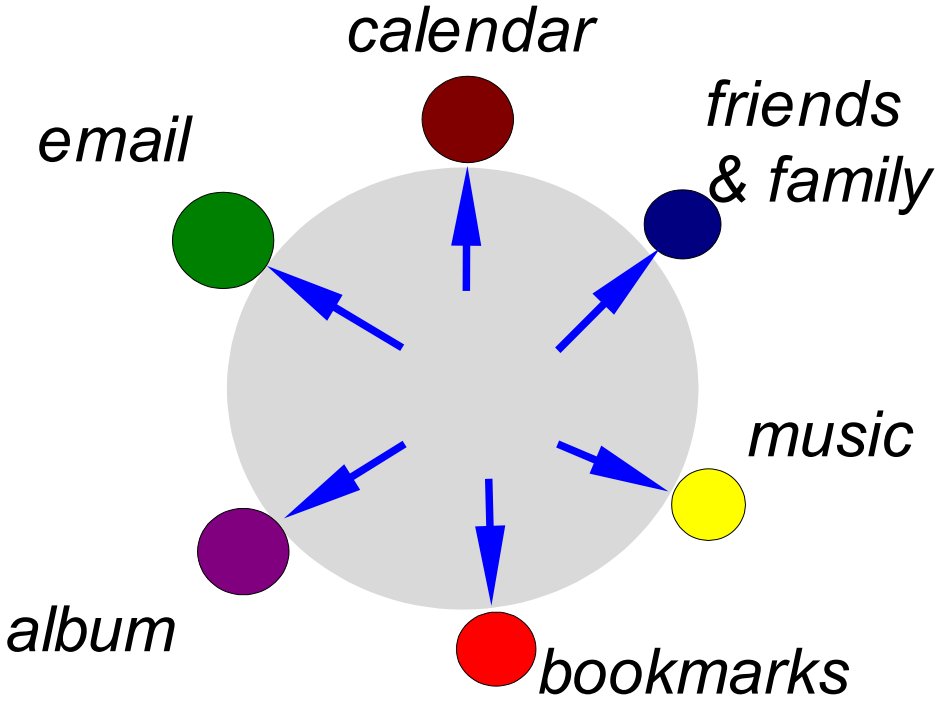


Internet

Storage

All about state





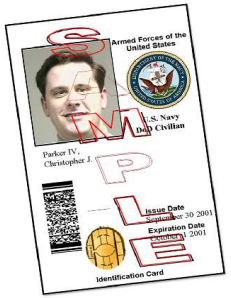
Personal Computer
State Attractor

Personal Network
State Distributor

...The Über-device?

Ultimate Mobility Vision

Secure Access Points Everywhere



Secure Javacard Authentication

Sun today uses 20,000 Sun Rays

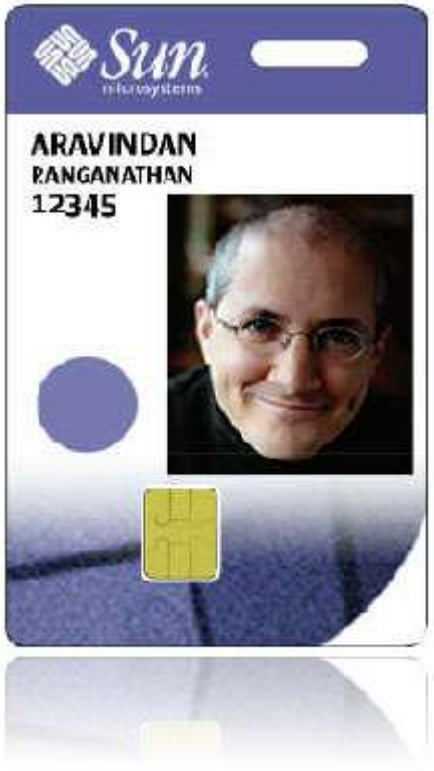
Completely Stateless

JavaCard

A universal ID- and Function Card is Replacing Single Usage Cards

- Employment Card/ Entry Card
- Sun RayMT Server mobile Dial-In Card
- PKI-Authentication with Token Card/x509
- Safeword Challenge/ Response Card
- ePurse/Money Card

=



What Is a Web Service ?

- Web services are modular software components written in any language, but expressed through standard interfaces
  - XML wrapper around the service written in Java or other language
  - SOAP to communicate between services
  - WSDL to describe a service in a registry
  - UDDI to define the registry
- Applications can be built with any combination of web services located anywhere
- Services can be registered and discovered all across the intranet or Internet

Web Services in the Future

- Getting to Heathrow from a meeting in downtown London
- Concert of your favourite musician
- Planning a meeting of 15 executives from different companies
- Traffic info that works (real time)
  - And across different modes of travel
- Family vacations . . .

How Can We Get There?

- The biggest obstacle is lack of interoperability
- Without standards interoperability is not achievable
- Web Services offer standards for heterogeneous SW/HW environments
- Architecture needed for integratability

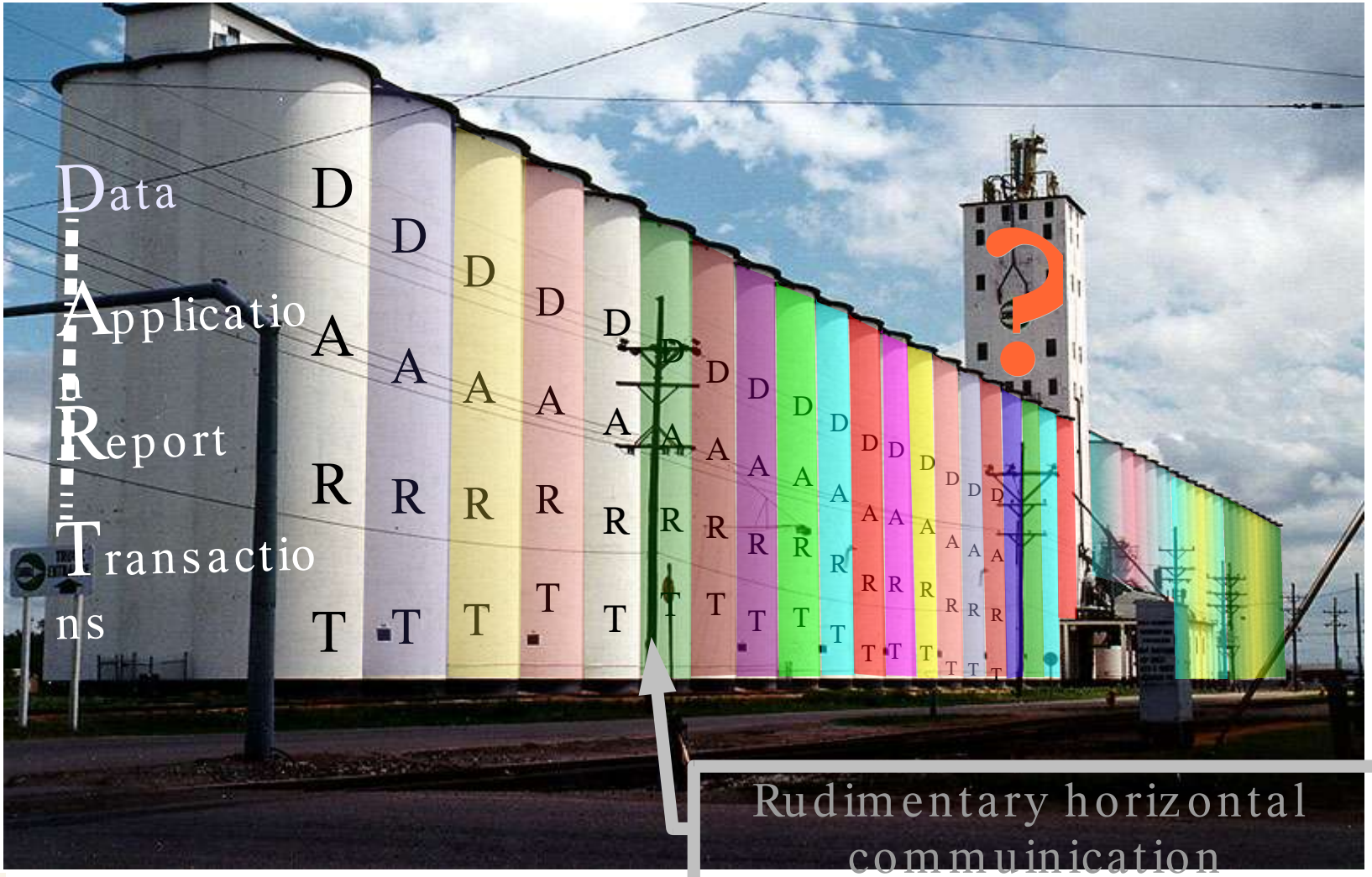
Where Are We Today?

- Services only for humans (*For Your Eyes Only* --- not other services)
- Application silos make cooperation impossible
- Identity silos fragment user information

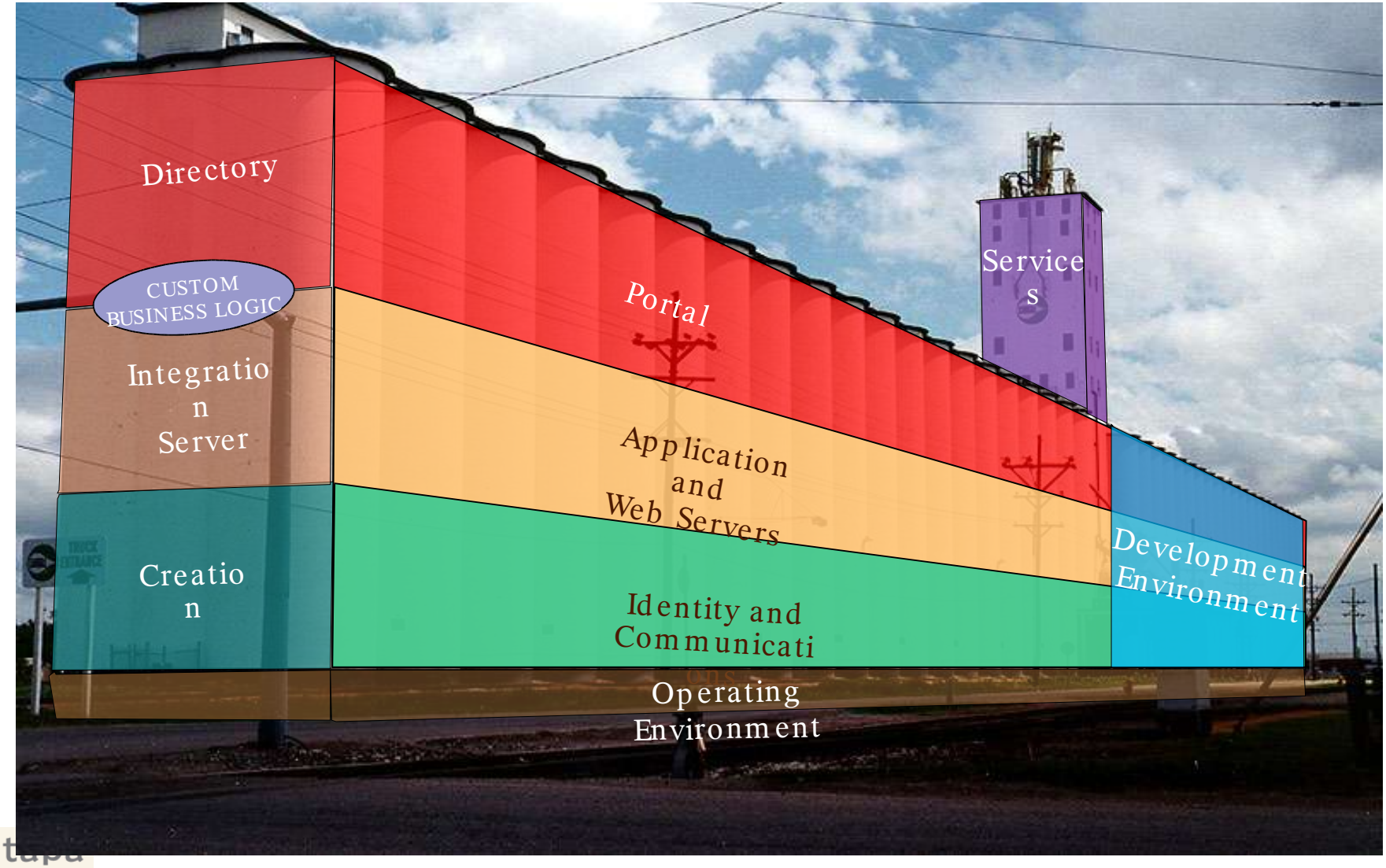
Today's Collection of Net Identity Silos

How We Have Been Building Systems

Our World of Application Silos



Future Architectures (Java E. S.)



Commerce on the Internet

What keeps customers from doing commerce over the internet?

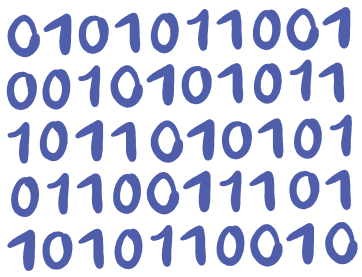
- Know who you are talking to (identity crisis)
- Globally accepted and secure payment systems
- Risk but not trust management
- Privacy concerns

Identity and Business

Identity is the most basic element in a high-value relationship with customers, employees, citizens or business partners

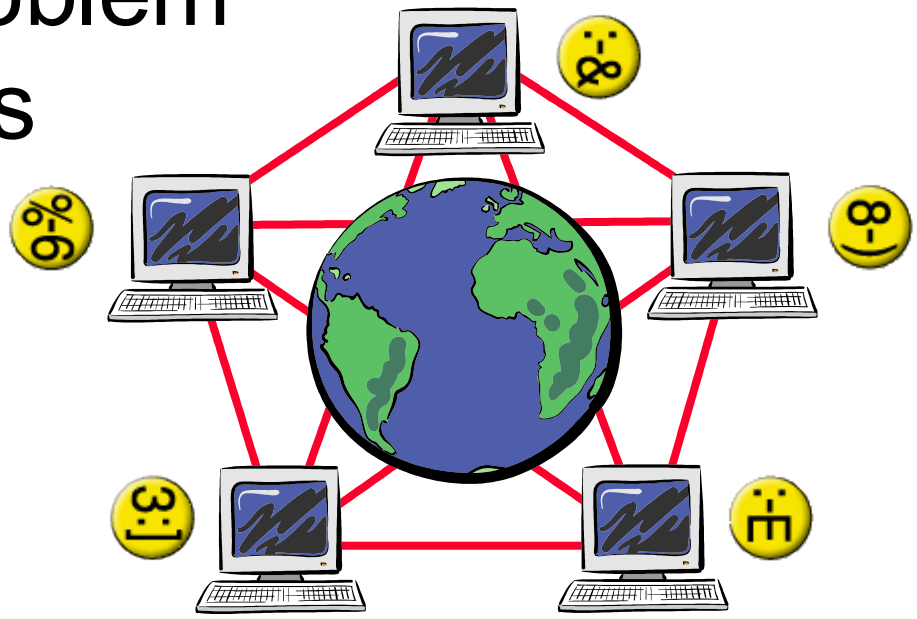
What Has to Be Identified?

- Persons (real people) in their roles
- Legal entities (companies, agencies, corporations, . . .)
- Things (air quality monitoring sensor, traffic counter, . . .)
- RFID tags; DRM
- Software services, agents, . . .



Identity Theft – Fastest Growing Crime

- Fed. Trade Commission is worried
- Today, solutions offered only for parts of the problem
- Ebay examples



A Network of Things

Auto ID – RFID Tags

Note: By 2005 WallMart will only accept merchandise with RFID tags attached!

Wide Range of Applications

AutoID has applications in virtually every industry

Retail

- Lower Labour Costs
- Reducing Inventories
- Locating Products
- Real-time supply/demand data
- Smart Shelves
- Customer Convenience

Healthcare/Pharma

- Tracking Hospital Equipment
- Patient ID and Tracking
- Preventing Medical Errors
- Tracking Samples, Vials etc.
- Environmental Monitoring (e.g. Blood Samples)
- Anti-Counterfeit Measures
- Product Recalls

Transport / Logistic

- Asset Utilization & Tracking
- Volume Planning
- Automated Sorting
- Automated Data Capture
- Shipment Route Tracing
- Delivery Reliability/Efficiency
- Contract Pricing Verification
- Reduced Claim Cost

Government

- Homeland Security
- Military/Defence Asset Tracking

Manufacturing

- Quality Control
- Lot Tracking
- Recalls
- Government Regulations
- Inventory Accuracy
- Labor & Material Costs
- Asset Utilization
- Supplier Management
- Customer Relations
- Supply Chain Mgmt
- Inventory
- Gray Market, Theft
- Shrinkage
- Shop Floor Execution

Other

- Payment Security
- Theme Park Applications
- Farm Animal Tracking

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

How We Can Build Trust

- The biggest concern of the principal/patient/customer is **privacy**
- Privacy is not just a technical issue
- It is about managing the **trust** of the principal/patient/customer
- What does an architecture for privacy and trust management look like?

Architecture for Trust Management

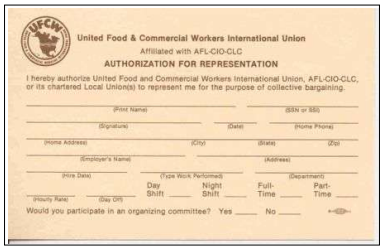
Definitions

Identity Management

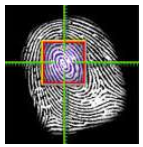
Security Management

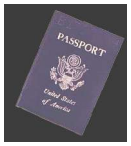
Policy

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

A combinationof 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

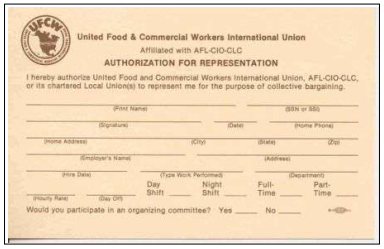
Real World Example: Drivers License

Identity Management

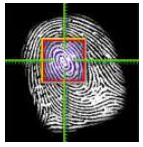
Security Management

Policy

Authorization



Authentication



Identity

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

Architecture for Trust Management

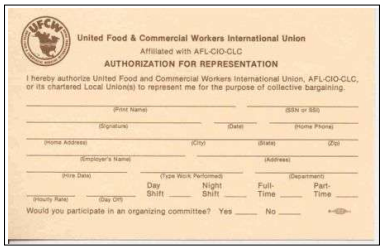
Digitally Speaking . . .

Identity Management

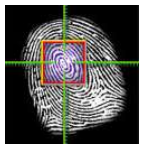
Security Management

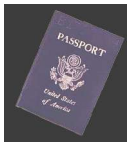
Policy

Authorization

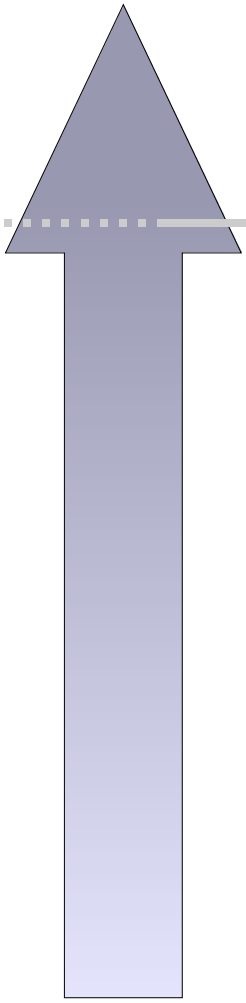

United Food & Commercial Workers International Union
Affiliated with AFL-CIO-CLC
AUTHORIZATION FOR REPRESENTATION
I hereby authorize United Food and Commercial Workers International Union, AFL-CIO-CLC, or its chartered Local Union(s) to represent me for the purpose of collective bargaining.
Would you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

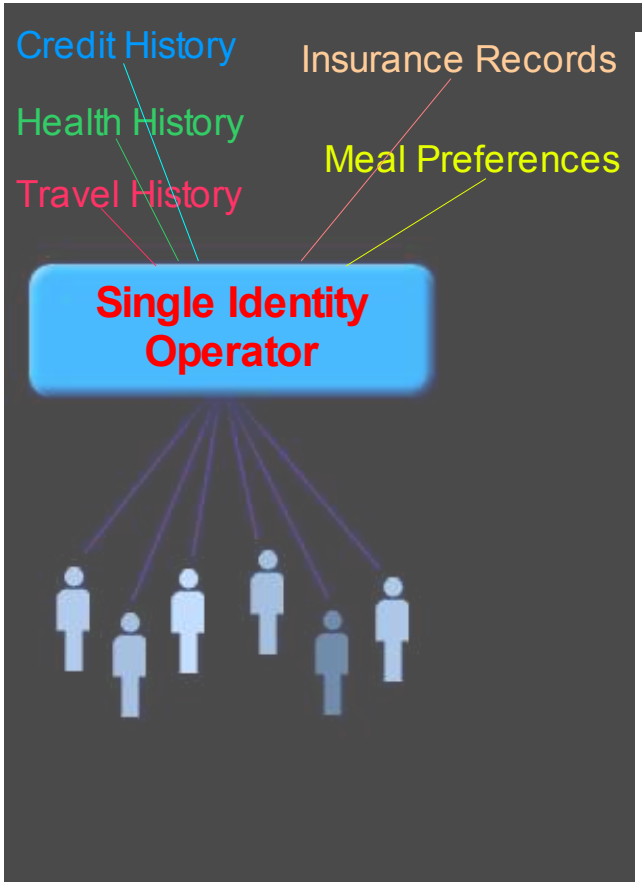
How People Will Trust Policies

- Policy and its audit 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, . . .)
- Policies and their transactions are insured. Insurances cover for possible policy violations and fraud
- Liability and non-repudiation solved

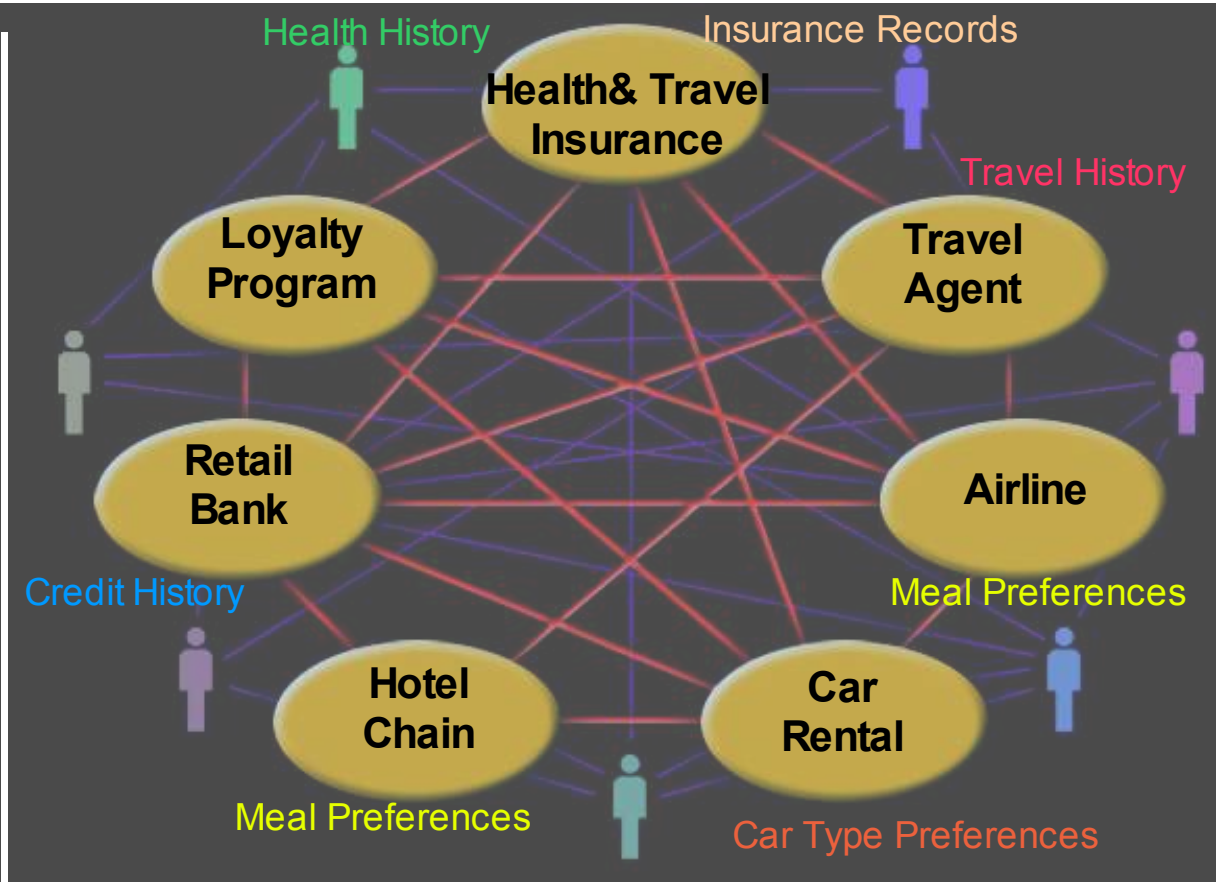
Trust is based on policies and the audit of those -- *not* just on security

Where to Safeguard User's Information

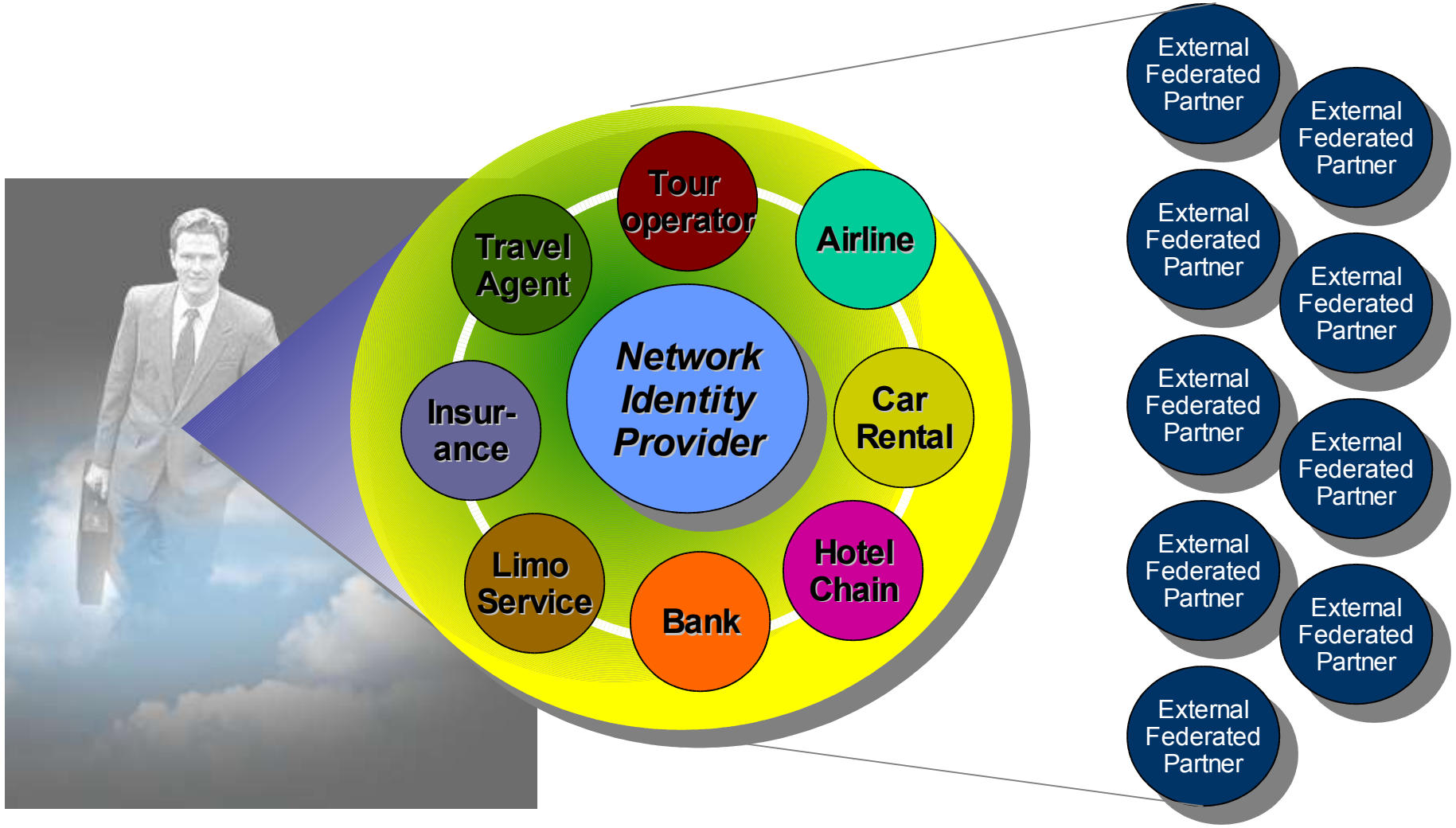
Single Point Model



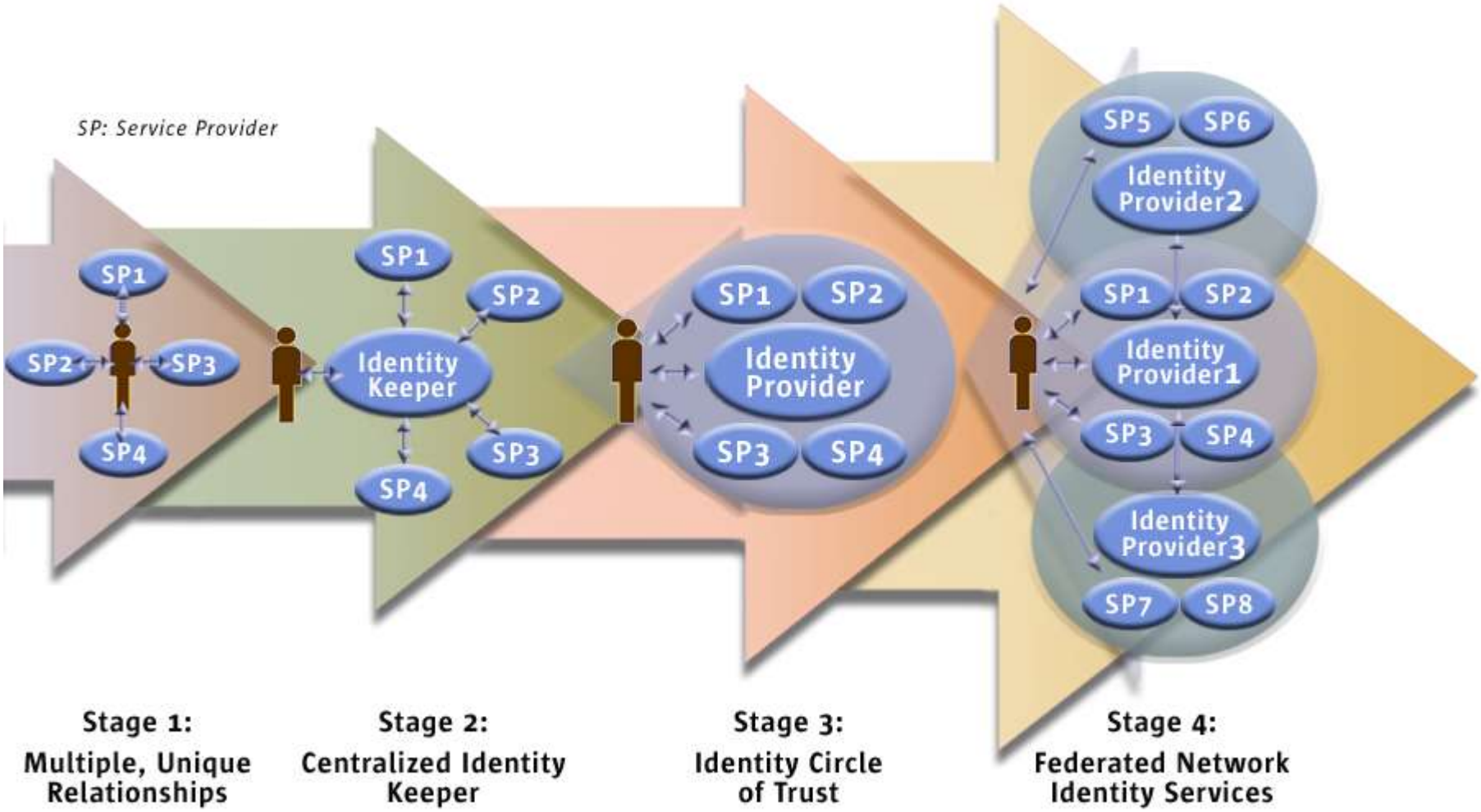
Open Federated Model



Circle of Trust Concept



Network Identity Organic Evolution



Liberty Alliance solves the identity crisis

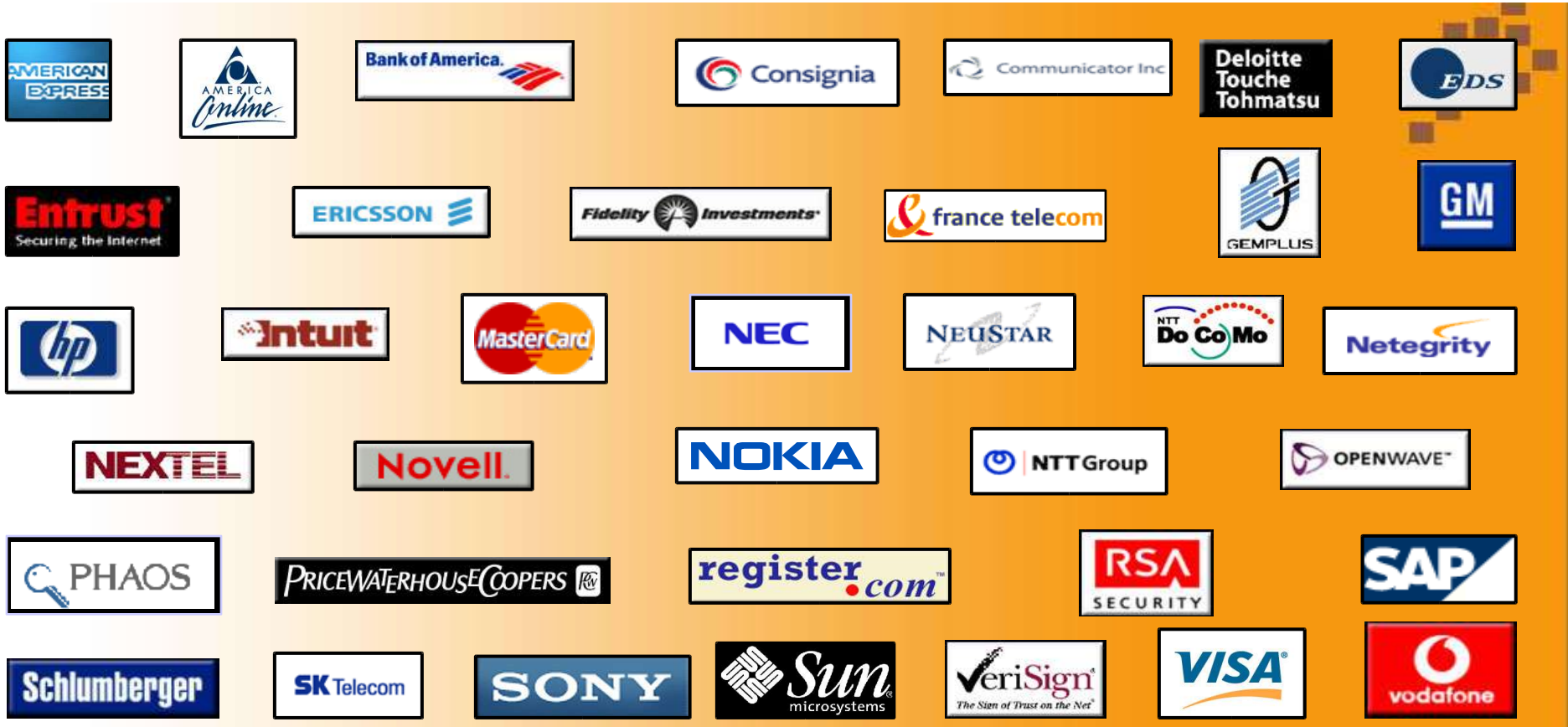
- The only global body working to define and drive open technology standards and guidelines for federated identity
- Addresses business, policy and technical issues associated with federated identity
- Alliance of global organizations working together to enable the deployment of identity-based web services

Liberty Members

Sun microsystems

LIBERTY ALLIANCE PROJECT

Over 160 for-profit, not-for-profit and government organizations, representing a billion customers, are currently Alliance members
The following represent Liberty's Board Members and Sponsors



Why You Should Join Liberty

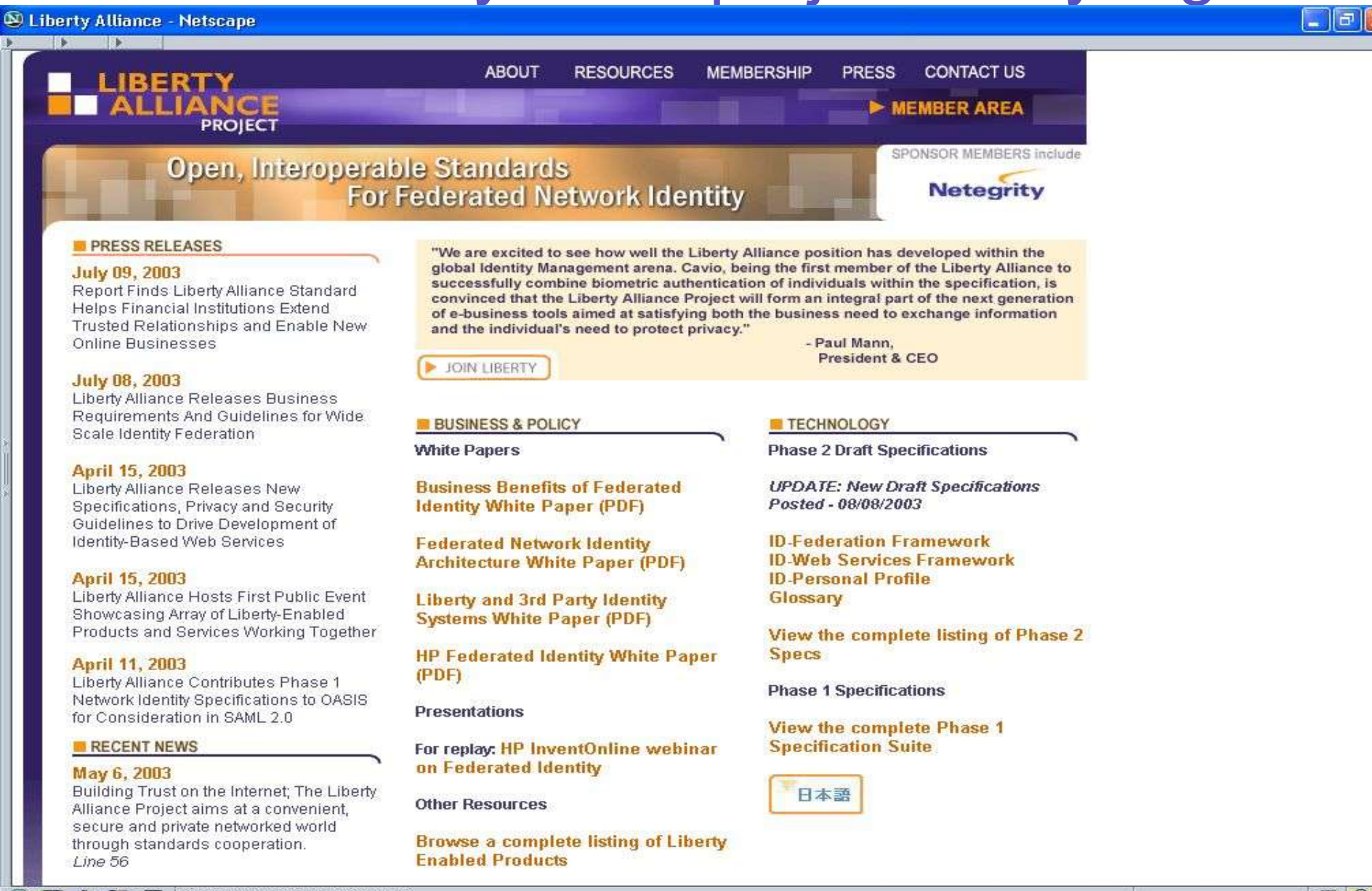
- Accelerate the implementation and increase opportunities of internal and cross organizational processes
- Participate in the development and use of business implementation guidelines
- Influence business and technical specifications to address your business needs
- Control business and technical risks through networking and sharing resources
- Enable your organization to understand and address global privacy concerns
- Partner in a multi-vendor marketplace of compliant products

Sun microsystems

LIBERTY ALLIANCE PROJECT

itapa

To Join Liberty: www.projectliberty.org



Liberty-enabled products and services

Communicator (available)
Computer Associates (Q4*)
DataKey (available)
DigiGan (Q3*)
Ericsson (Q4)
Entrust (Q1 2004)
France Telecom (Q4 2003)
Fujitsu Invia (available)
Gemplus (TBD)
HP (available)
July Systems (available)
Netegrity (2004)
NeuStar (available)
Nokia (2004)
Novell (available)
NTT (TBD)
NTT Software (available)
Oblix (2004)
PeopleSoft (available)
Phaos Technology (available)
Ping Identity (available)
PostX (available)
RSA (Q4)
Salesforce.com (TBD)
Sigaba (available)
Sun Microsystems (available)
Trustgenix (available)
Ubisecure (available)
Verisign (Q4*)
Vodafone (2004)
WaveSet (available)

LIBERTY ALLIANCE PROJECT

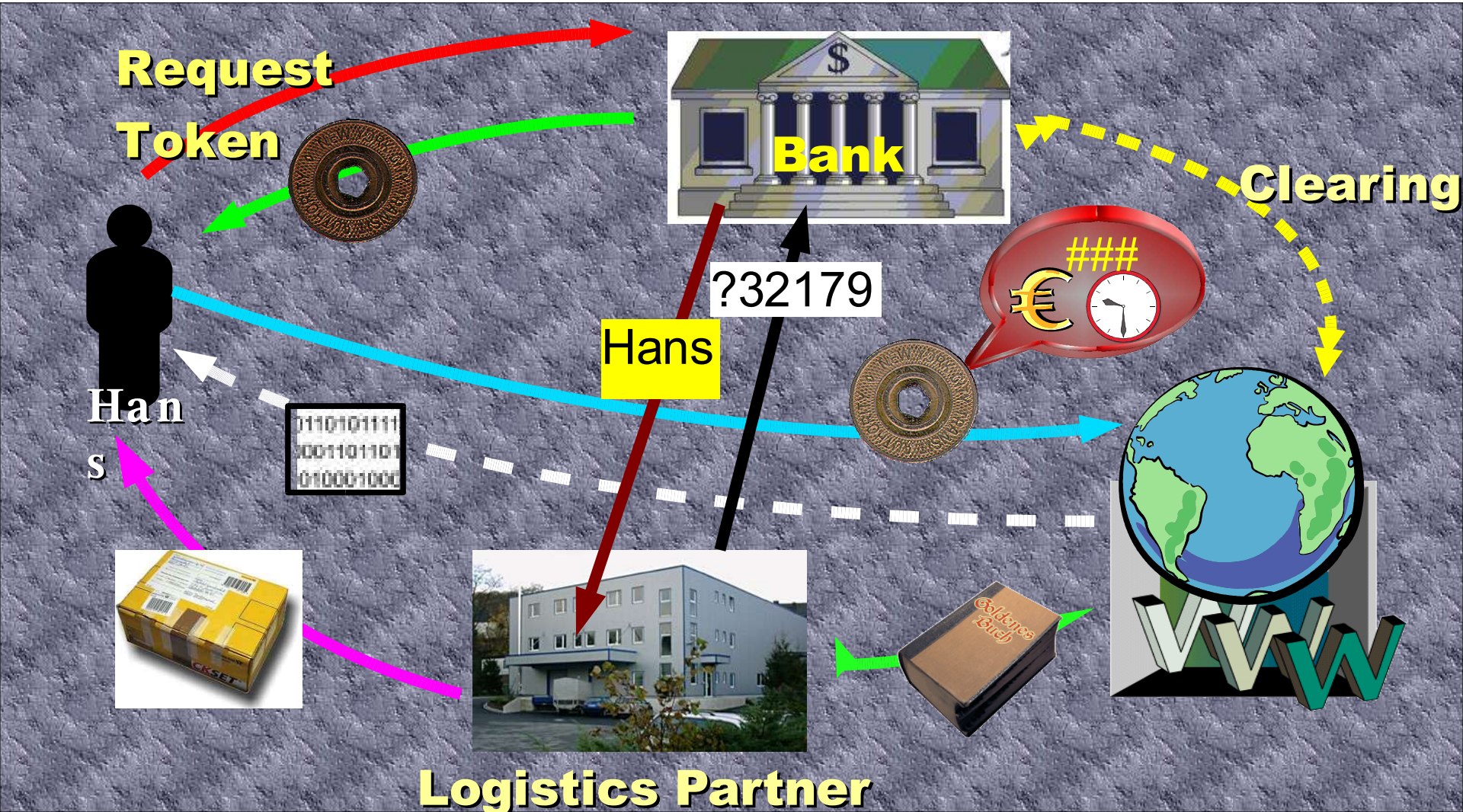
*Delivery dates being confirmed

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 Enabled Trusted Third Party Transactions Are Achievable Now!



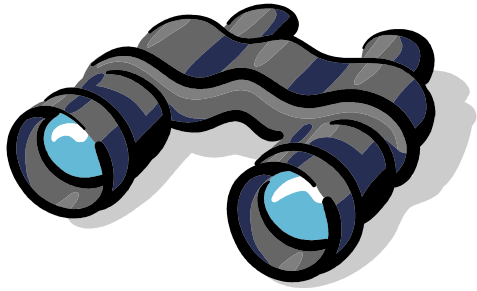
Who Does What? Business Opportunities (1)

- 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)

Business Opportunities (2)

- Trusted Third Party Services (incl. Logistics) (national, international)
- Policy audit and seal of approval (national, international)
- Web page seal (international)
- Clearing
- International payment systems for small amounts

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

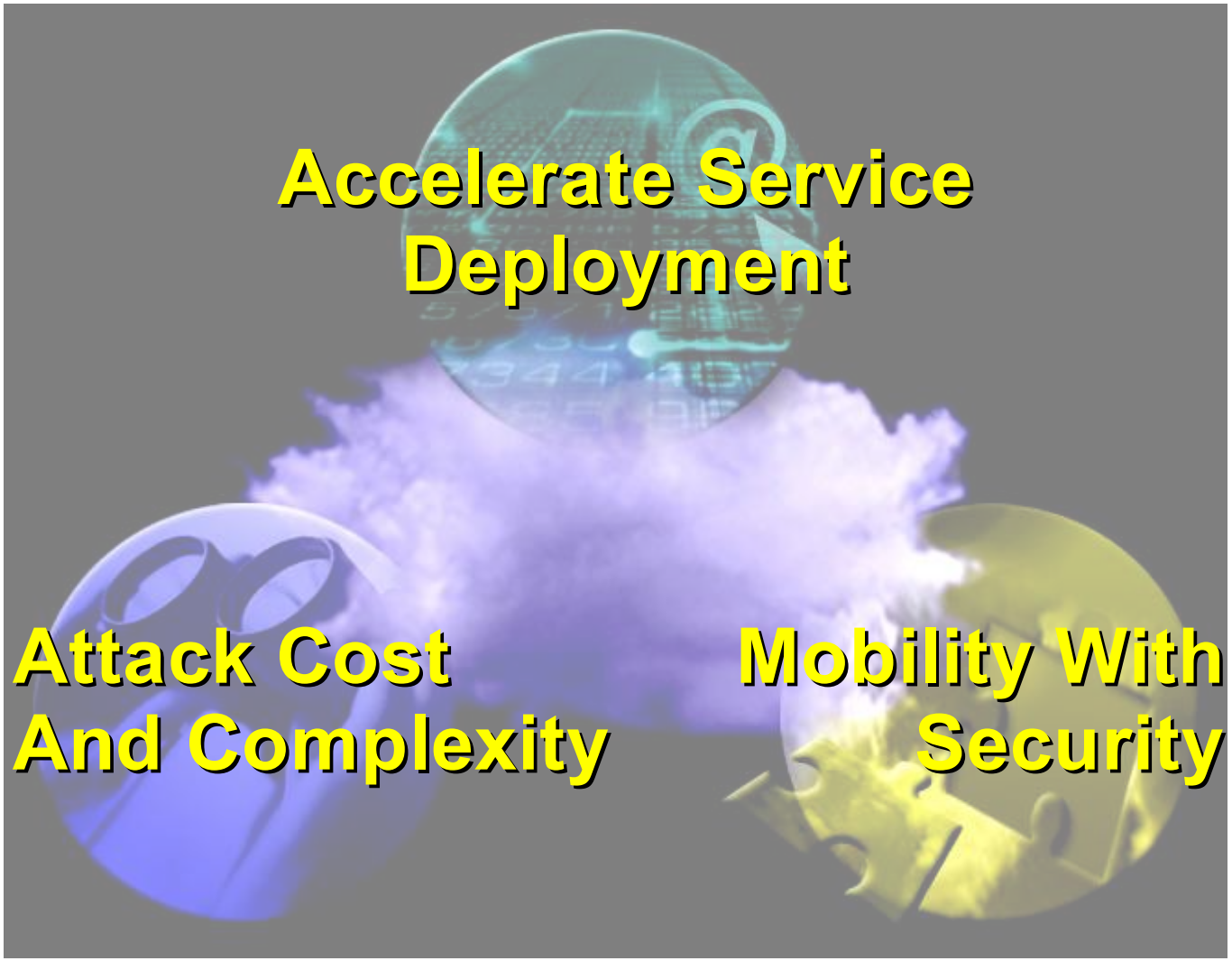
My e-Government Vision

- Governments will offer services centered around the needs of the customer (citizens) across agencies
- Services are perceived as effective, efficient and trustable
- Privacy of the citizens is managed in a professional manner

My Personal Recommendation

- Build services that are trusted by the citizens
- Join the Liberty Alliance
- Do not re-invent wheels, look what others did
- Innovate on new services; don't electrify the status quo
- Every e-Project needs a sponsor at the highest available level
- Make services citizen-centric (not bureaucracy-centric)
- Talk to Sun---we provide open and secure systems and we work with many governments

In Conclusion: Sun's 3 Core Strategies



Ďakujem

Hellmuth.Broda@Sun.COM

www.sun.com

Sun microsystems

We make the net work.