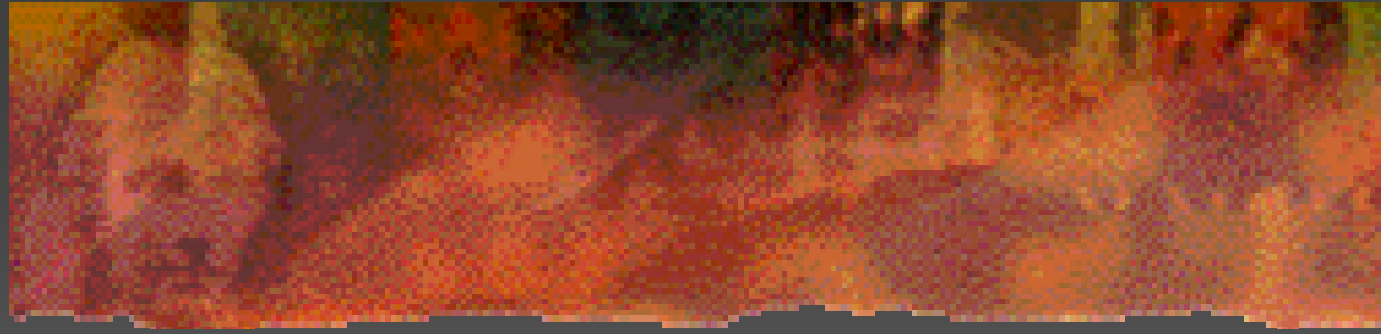
HSPD-12
Technology & Privacy Panel

January 19th, 2005

Howard A. Schmidt



"Without Security there is no Privacy"
"Privacy is a goal, Security is the means to achieve this"

Security and the End-User Landscape

Current password behavior leaves end-users vulnerable.

- Over 60% of end-users usually use the same one or two passwords.*
- Only 16% change their passwords more often than once a year.
- 13% frequently have to request their password because they have forgotten it.*
- Thousands of compromised "hacked accounts" per day (at major ISP)
- $200,000 per month in password re-set expense (at major ISP)

Consumers are concerned about security.

- Over 50% of end-users want anti-virus protection and other value-added services (anti-spam, etc.) with their ISP.*
- Most end-users use the anti-virus that comes bundled with their ISP.
- 66% have paid for upgrades or made additional security software purchases.*
- Security is the number one concern with personal services such as banking.

*Data from Forrester Devices & Access Survey, April 2003

Common Attacks

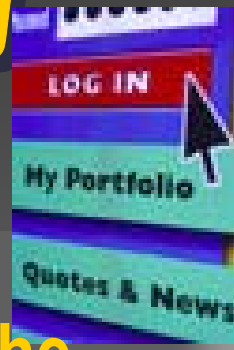
- E-mail spoofing the header of an e-mail appears to have originated from someone or somewhere other than the actual source. Spam distributors and criminals often use spoofing in an attempt to get recipients to open and possibly even respond to their solicitations.
- Password trap (PAS.wurd trap) *n*. A program or Web site that uses a legitimate-looking interface to fool users into providing their passwords.
- Phishing is the term coined by criminals who imitate legitimate companies in e-mails to entice people to share passwords or credit-card numbers, where people are directed to Web pages that looked nearly identical to the government/companies' sites.

Security Concerns
Impacting Growth of Online Commerce

The end-user has become the weakest link in the trust chain!

- What is needed:
  - Encryption
  - Authentication
  - Proof of identification
    - 1997 in the form of digital signatures
    - 2005 two-factor authentication is the recommended approach

The Keys to Securing Your Privacy



There are four key components to securing information:

- Authentication — You need to make sure that both the sender and recipient are who they say they are.
- Data privacy — You need to ensure the confidentiality of information as it moves around the public Internet.
- Non-repudiation — Authenticated users in a transaction should not be able to deny actions they have taken.
- Authorization — Unauthorized users should not be able to see information they're not supposed to see.

Why two-factor authentication?

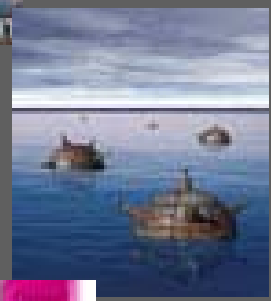
- Keep Data Private while in Transit
- Make Transactions Actionable and Non-repudiable
- Prevent Unauthorized Access to Information
- Enhanced Security
- Ease of Use
- Fewer Administrative headaches
- Flexible Solution for Multiple applications
- Credential Portability

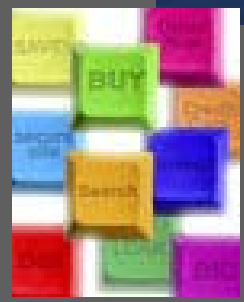
Authentication
The Cornerstone to Security and Privacy

- Authentication is the essential foundation for online activity
  - Establishes trust by proving identities of the participants in a transaction
- Without knowing with a high level of certainty who you are dealing with, it is:
  - Not possible to properly assign access control & other rights
  - Not possible to trust a digital signature
- In many cases it makes no sense to encrypt data if you don't know who's on the other end of the line

Authentication Selection Criteria

- Cost
  - Acquisition
  - Deployment
  - Support
- Usability (User)
  - Ease of use/convenience
  - Portability
  - Multi-use
- Strategic Fit (System)
  - Scalability / Interoperability
  - Level of Security
  - Future flexibility





The Opportunity

An exponentially growing user base…

Employees

Consumers/End-Users

Government/Private Sector Partners

Opportunity for Government to Lead

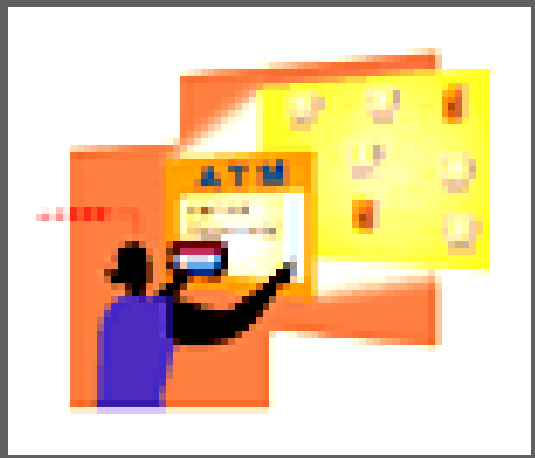
- Can you ensure the success of your business application with…
  - … aggressive business objectives (i.e. business goals, customer satisfaction initiatives, user productivity, etc.)
  - … growing cost sensitivities
  - … growing security concerns
- Can you effectively manage a solution that works for you with…
  - … a growing number of users
  - … an expansive, heterogeneous infrastructure
  - … future scalability concerns

Federated Consumer Authentication: The Future

Trusted Credential

ISPs

E-Commerce

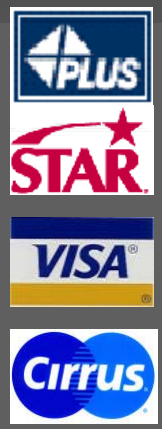


Government Services

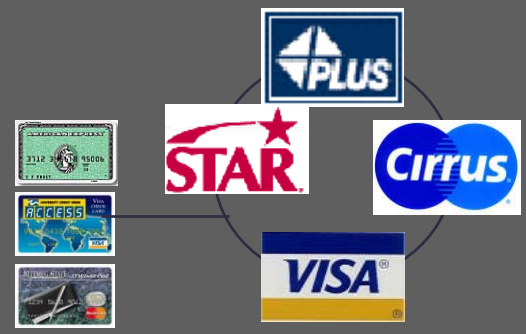
ATM Example

Separate Cards with Each Bank

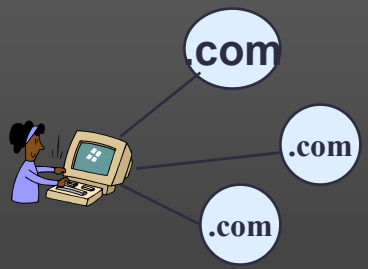
Linked Cards within Bank Networks



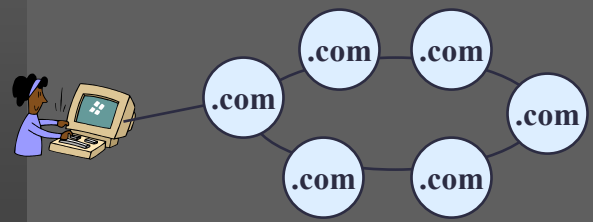
Seamless Access Across all Networks



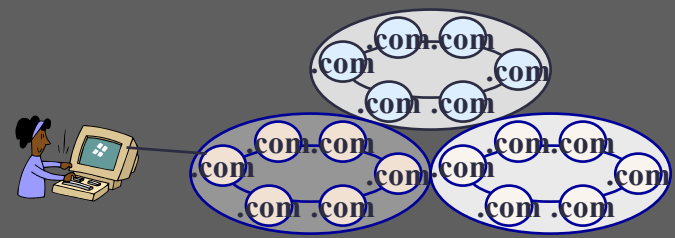
Individual Accounts with Many Web Sites



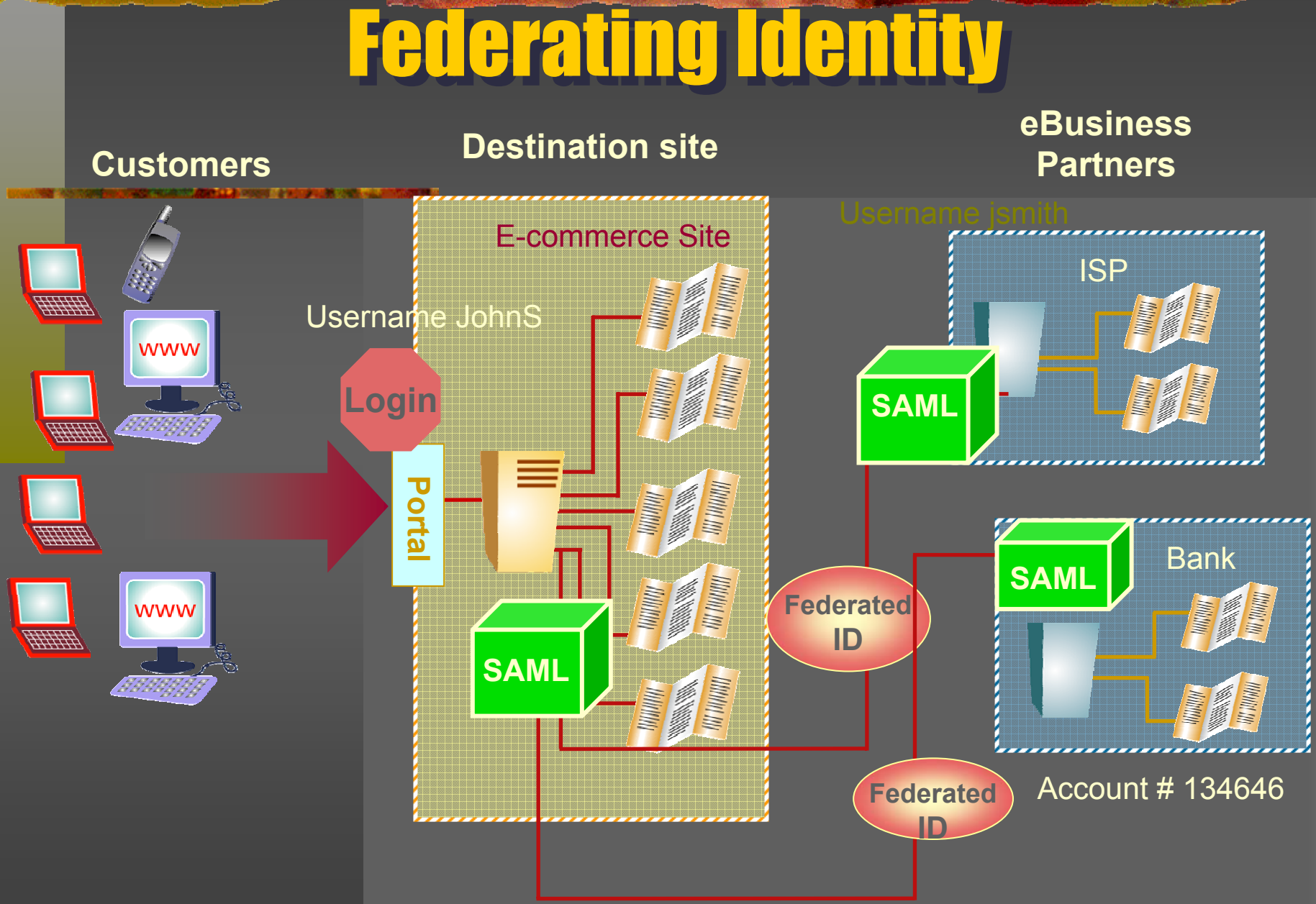
Federated Accounts within Trust Domain



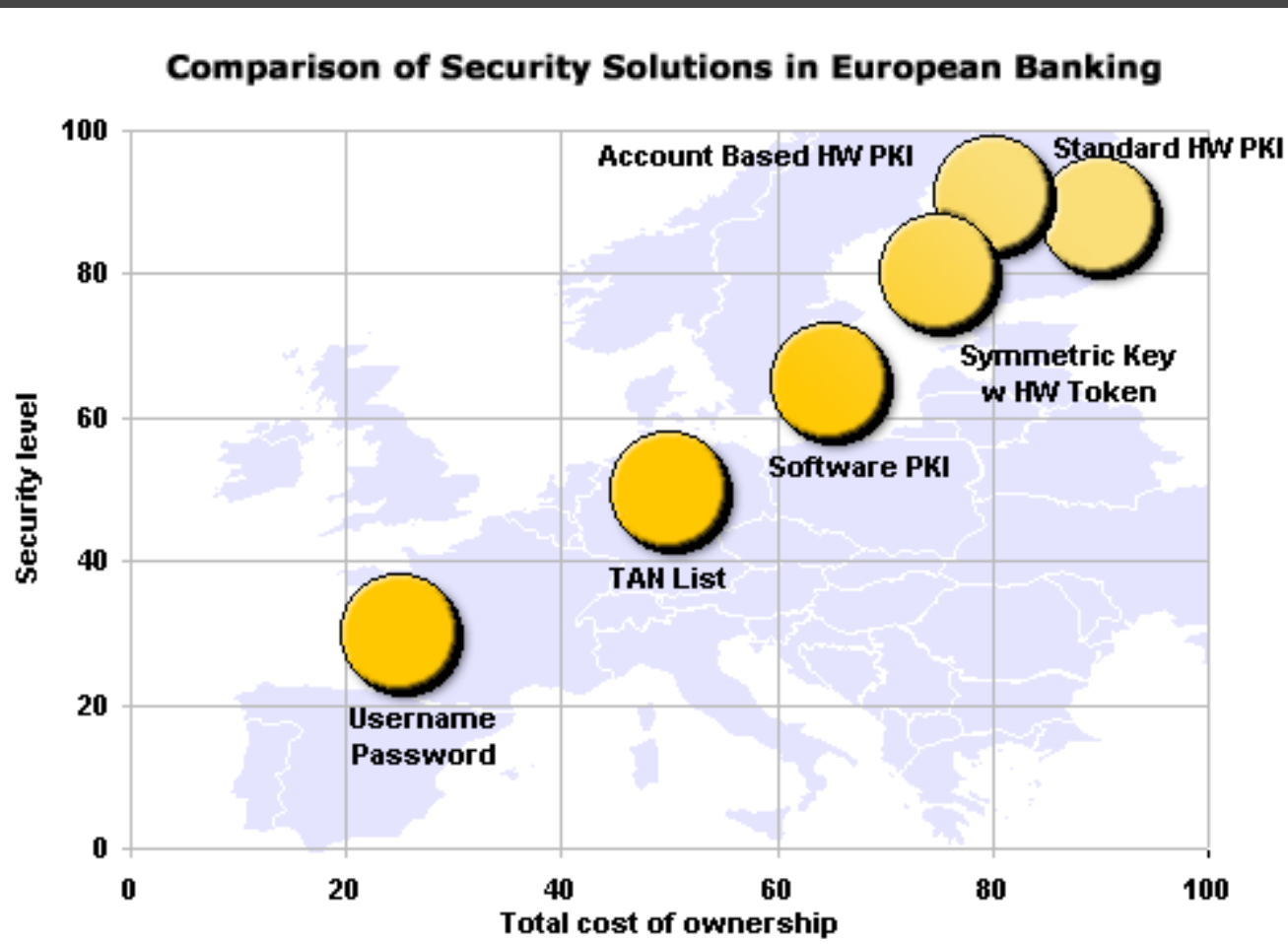
Linkage of Trust Domains



Federating Identity



How do you manage a growing number of users and their secure access to Web resources in a scalable, cost-efficient manner across an untrusted environment?



The American market predominantly uses username/password combinations to authenticate its consumers, European banks have deployed a wider variety of strong authentication solutions to serve both corporate and retail users.

Federated identity benefits

- Can leverage existing identities, won't force a replacement
  - No expense associated with resolving name space issues
- Better protection of user privacy
- Greater choice for users
  - Identity provider and when to federate

- Centralized identity benefits
  - User actually has a single identity across multiple applications
    - Less administrative cost once it's established
  - Simpler to manage for single or limited applications

Federated Model

Thank You!

Howard A. Schmidt