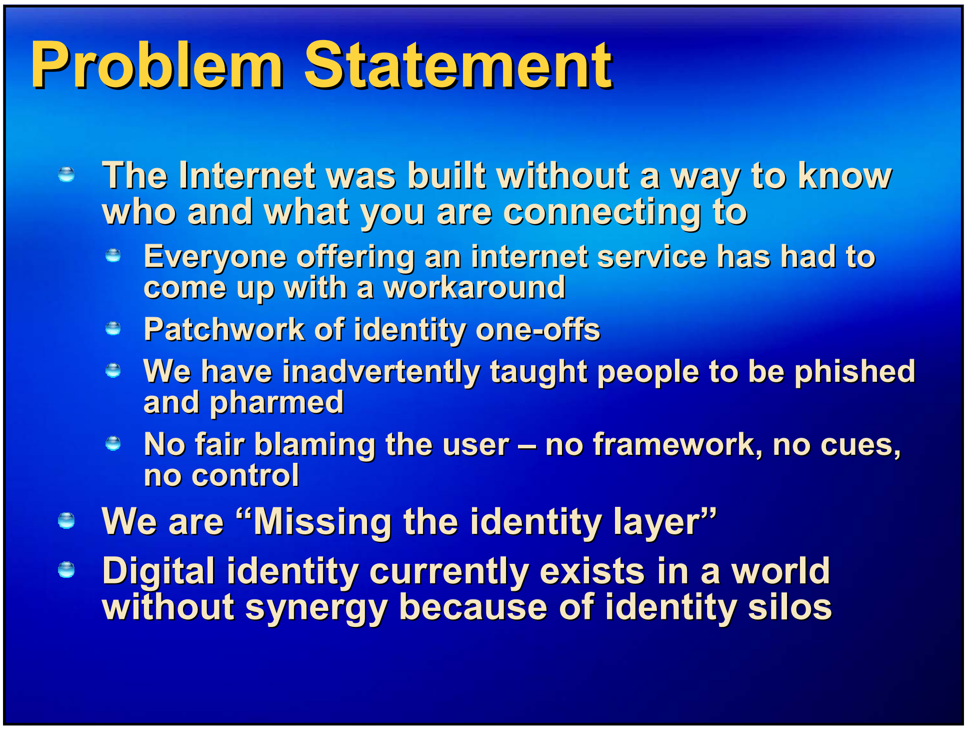
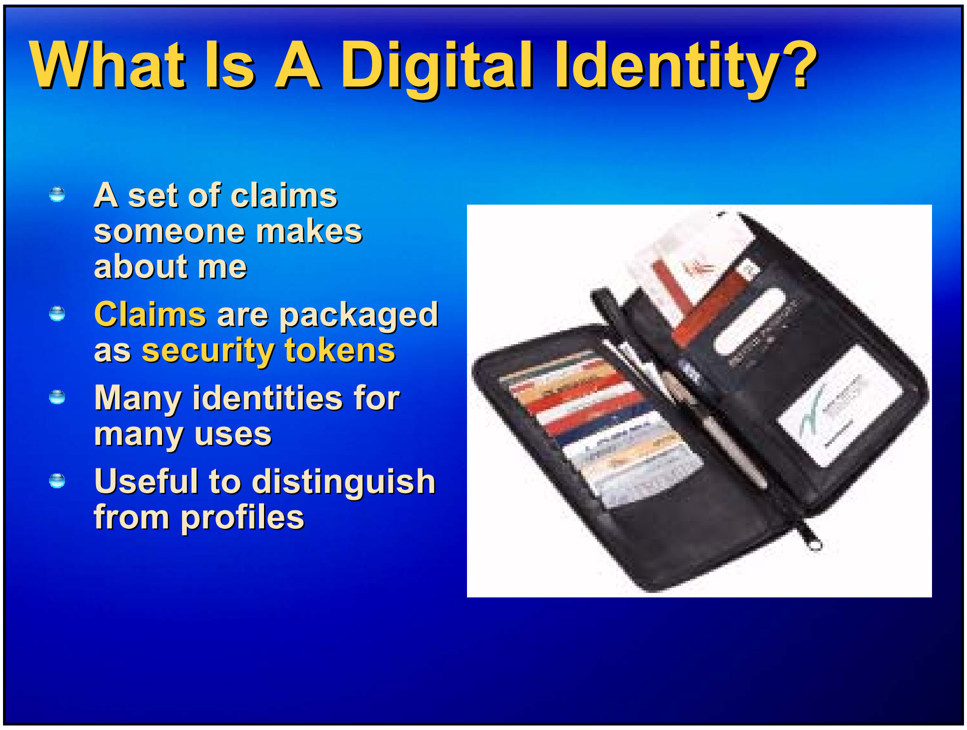
The Identity Metasystem and Cardspace

Chris Bunio
Senior Architect
Microsoft
Trondheim, Norway
May 8, 2007



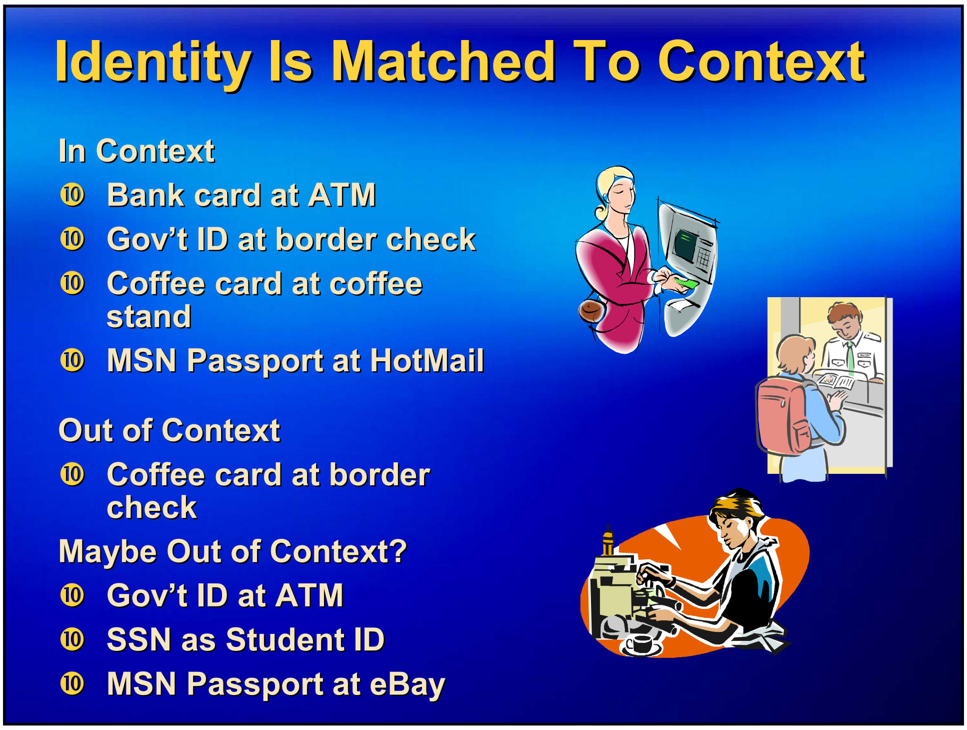
Problem Statement

- The Internet was built without a way to know who and what you are connecting to
  - Everyone offering an internet service has had to come up with a workaround
  - Patchwork of identity one-offs
  - We have inadvertently taught people to be phished and pharmed
  - No fair blaming the user – no framework, no cues, no control
- We are “Missing the identity layer”
- Digital identity currently exists in a world without synergy because of identity silos



What Is A Digital Identity?

- A set of claims someone makes about me
- Claims are packaged as security tokens
- Many identities for many uses
- Useful to distinguish from profiles



Identity Is Matched To Context

In Context

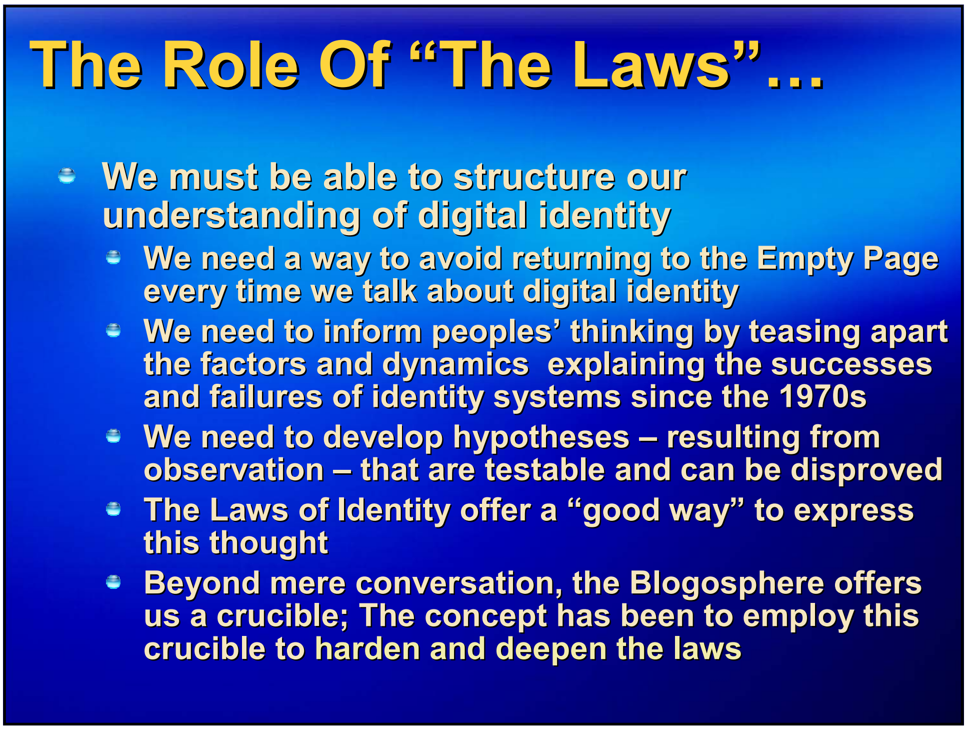
- Bank card at ATM
- Gov't ID at border check
- Coffee card at coffee stand
- MSN Passport at HotMail

Out of Context

- Coffee card at border check

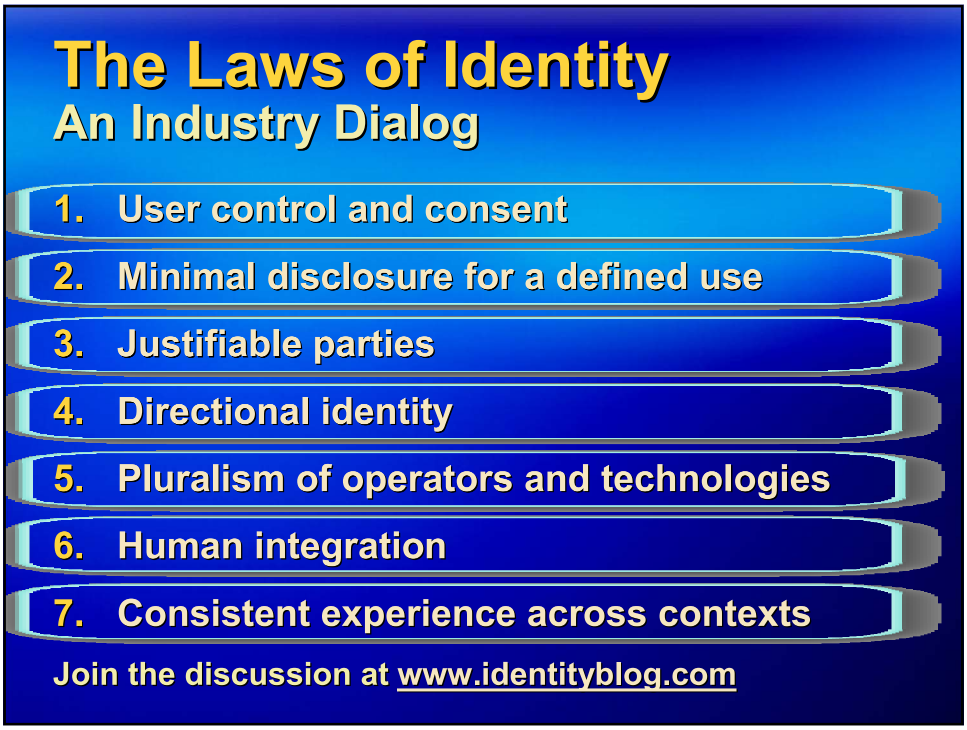
Maybe Out of Context?

- Gov't ID at ATM
- SSN as Student ID
- MSN Passport at eBay



The Role Of "The Laws"…

- We must be able to structure our understanding of digital identity
  - We need a way to avoid returning to the Empty Page every time we talk about digital identity
  - We need to inform peoples' thinking by teasing apart the factors and dynamics explaining the successes and failures of identity systems since the 1970s
  - We need to develop hypotheses – resulting from observation – that are testable and can be disproved
  - The Laws of Identity offer a "good way" to express this thought
  - Beyond mere conversation, the Blogosphere offers us a crucible; The concept has been to employ this crucible to harden and deepen the laws

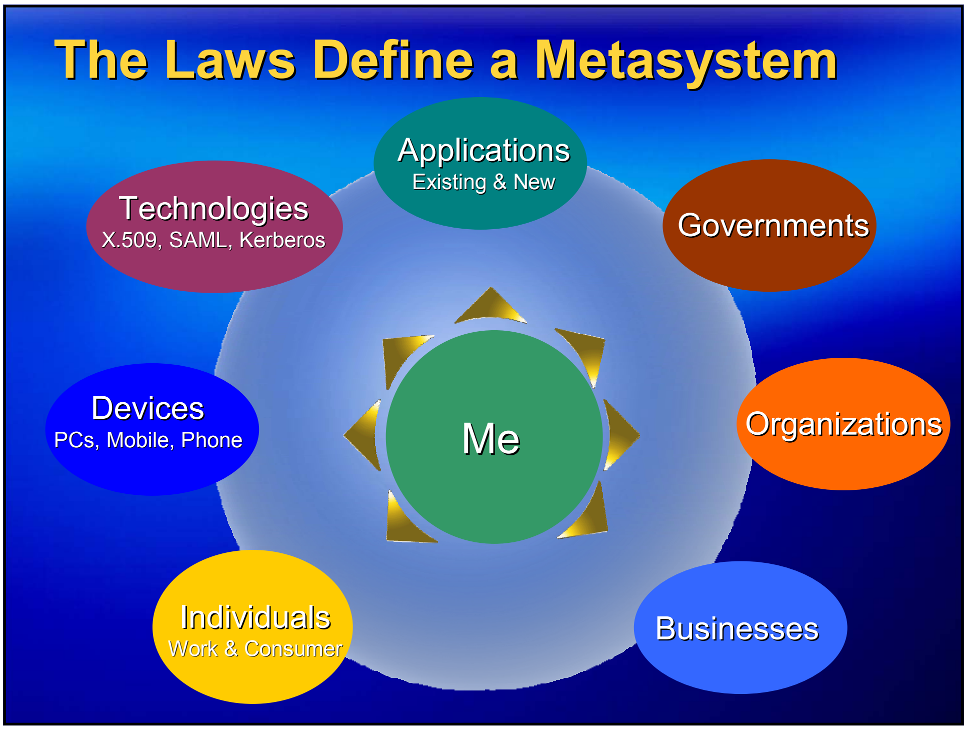


The Laws of Identity

An Industry Dialog

1. User control and consent
2. Minimal disclosure for a defined use
3. Justifiable parties
4. Directional identity
5. Pluralism of operators and technologies
6. Human integration
7. Consistent experience across contexts

Join the discussion at www.identityblog.com



The Laws Define a Metasystem

Applications
Existing & New

Technologies
X.509, SAML, Kerberos

Governments

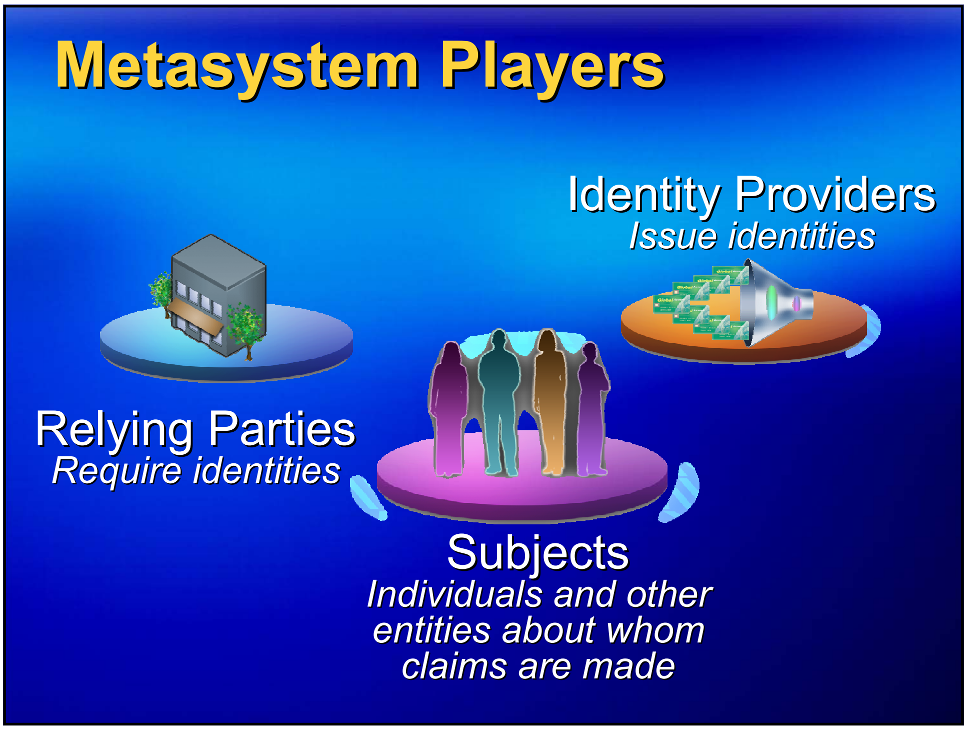
Me

Devices
PCs, Mobile, Phone

Organizations

Individuals
Work & Consumer

Businesses

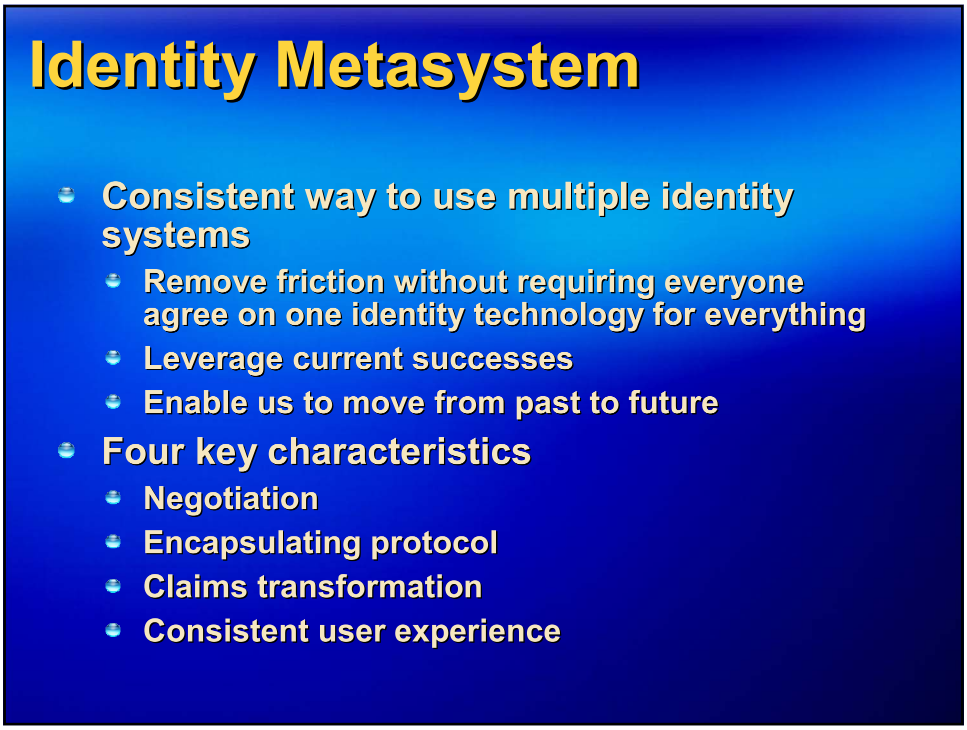


Metasystem Players

Identity Providers
Issue identities

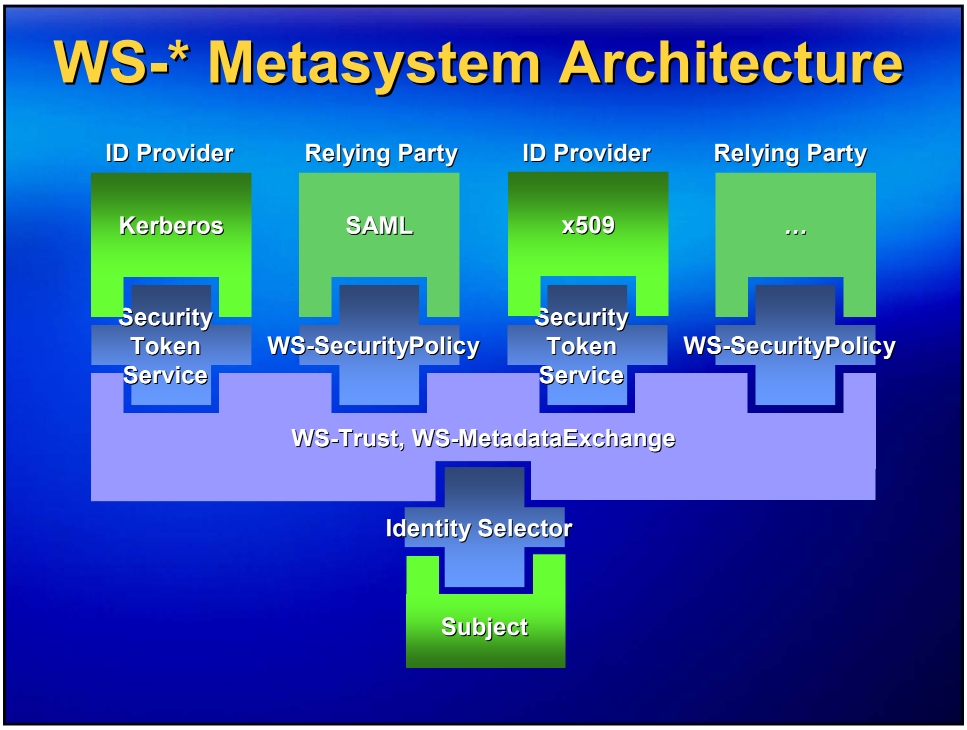
Relying Parties
Require identities

Subjects
Individuals and other entities about whom claims are made



Identity Metasystem

- Consistent way to use multiple identity systems
  - Remove friction without requiring everyone agree on one identity technology for everything
  - Leverage current successes
  - Enable us to move from past to future
- Four key characteristics
  - Negotiation
  - Encapsulating protocol
  - Claims transformation
  - Consistent user experience



WS-* Metasystem Architecture

ID Provider

Kerberos

Security Token Service

Relying Party

SAML

WS-SecurityPolicy

ID Provider

x509

Security Token Service

Relying Party

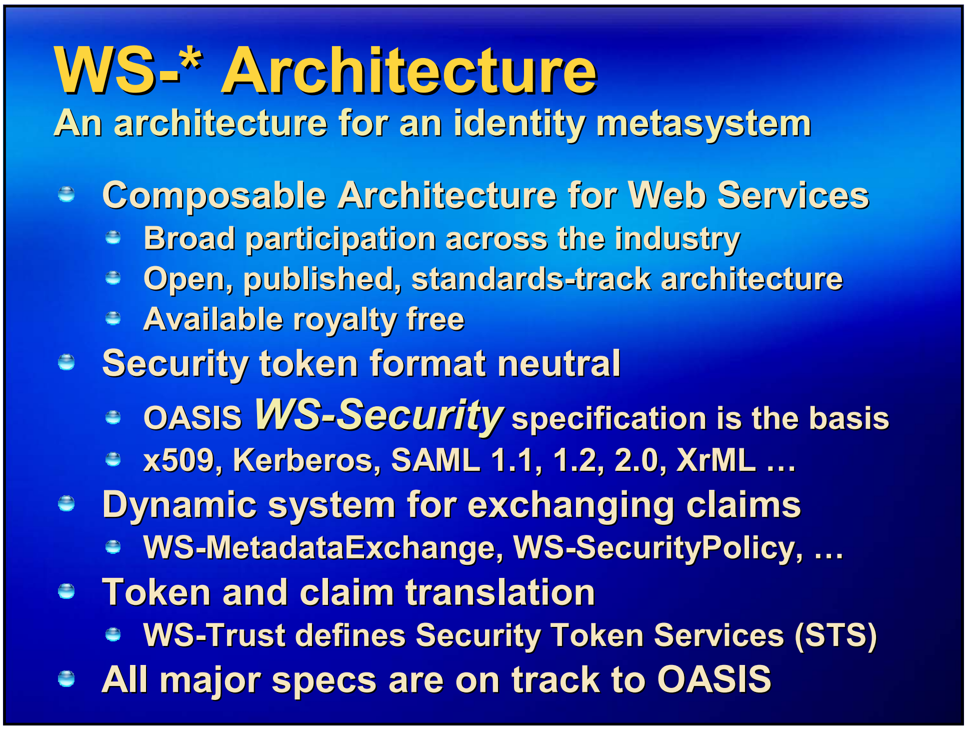
…

WS-SecurityPolicy

WS-Trust, WS-MetadataExchange

Identity Selector

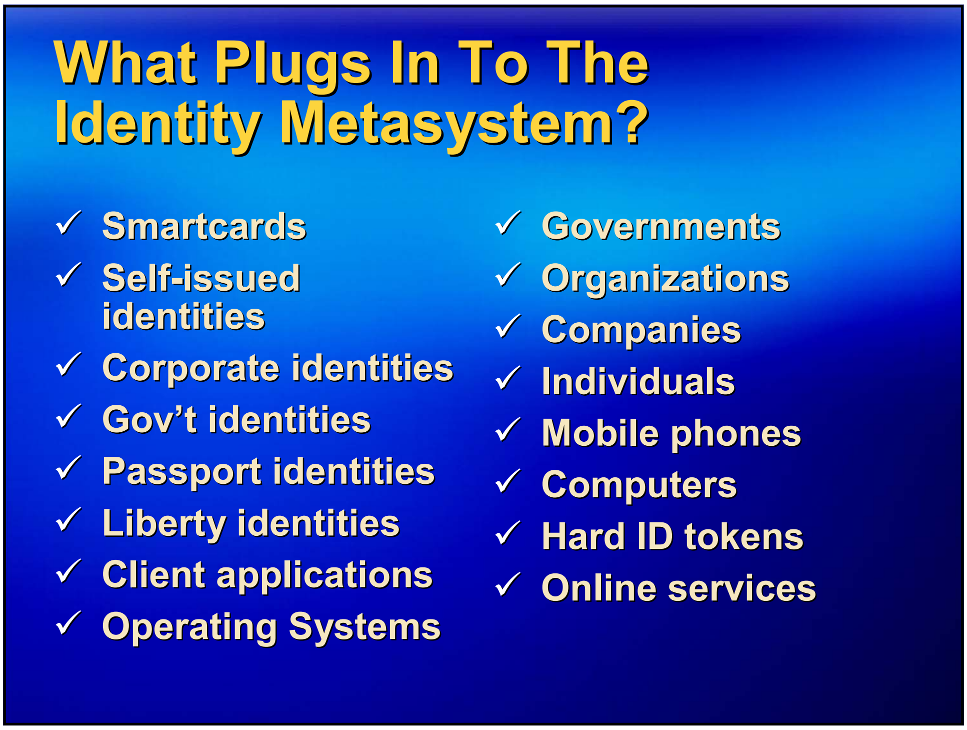
Subject



WS-* Architecture

An architecture for an identity metasystem

- Composable Architecture for Web Services
  - Broad participation across the industry
  - Open, published, standards-track architecture
  - Available royalty free
- Security token format neutral
  - OASIS *WS-Security* specification is the basis
  - x509, Kerberos, SAML 1.1, 1.2, 2.0, XrML …
- Dynamic system for exchanging claims
  - WS-MetadataExchange, WS-SecurityPolicy, …
- Token and claim translation
  - WS-Trust defines Security Token Services (STS)
- All major specs are on track to OASIS



What Plugs In To The Identity Metasystem?

✓ Smartcards
✓ Self-issued identities
✓ Corporate identities
✓ Gov't identities
✓ Passport identities
✓ Liberty identities
✓ Client applications
✓ Operating Systems

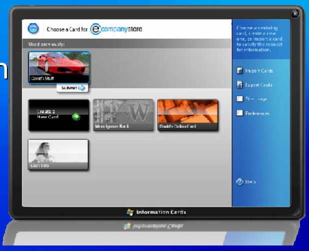
✓ Governments
✓ Organizations
✓ Companies
✓ Individuals
✓ Mobile phones
✓ Computers
✓ Hard ID tokens
✓ Online services

Cardspace

Returning Identity Control to the End User

Easier

- Reduces reliance on usernames & passwords
- Consistent experience for login and registration



Choose a Card for companystore

Choose an existing card, create a new one, or import a card to satisfy the request for information.

Safer

- Helps end users avoid some phishing attacks
- Support for multi-factor authentication

Built on WS-* Web Services Protocols

Microsoft®

Your potential. Our passion.℠

The information herein is for informational purposes only and represents the current view of Microsoft Corporation as of the date of this presentation. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information provided after the date of this presentation.
MICROSOFT MAKES NO WARRANTIES, EXPRESS, IMPLIED OR STATUTORY, AS TO THE INFORMATION IN THIS PRESENTATION.