



Security and Identity Management

Goodwin Ting
Chief Technologist
Sun Microsystems Federal

Nebraska Digital
Government
Summit – 2004



Agenda

- Security - What and Why
- 5 Key Security Requirements
- Enabling Technologies
- Identity Management – What and Why
 - Single Sign-On
 - Identity Synchronization
- Federated vs. Non-federated ID Mgmt
 - Liberty and Passport
- Q&A

Ask your users: “What is security?”

The stuff I have to get around to get my job done.

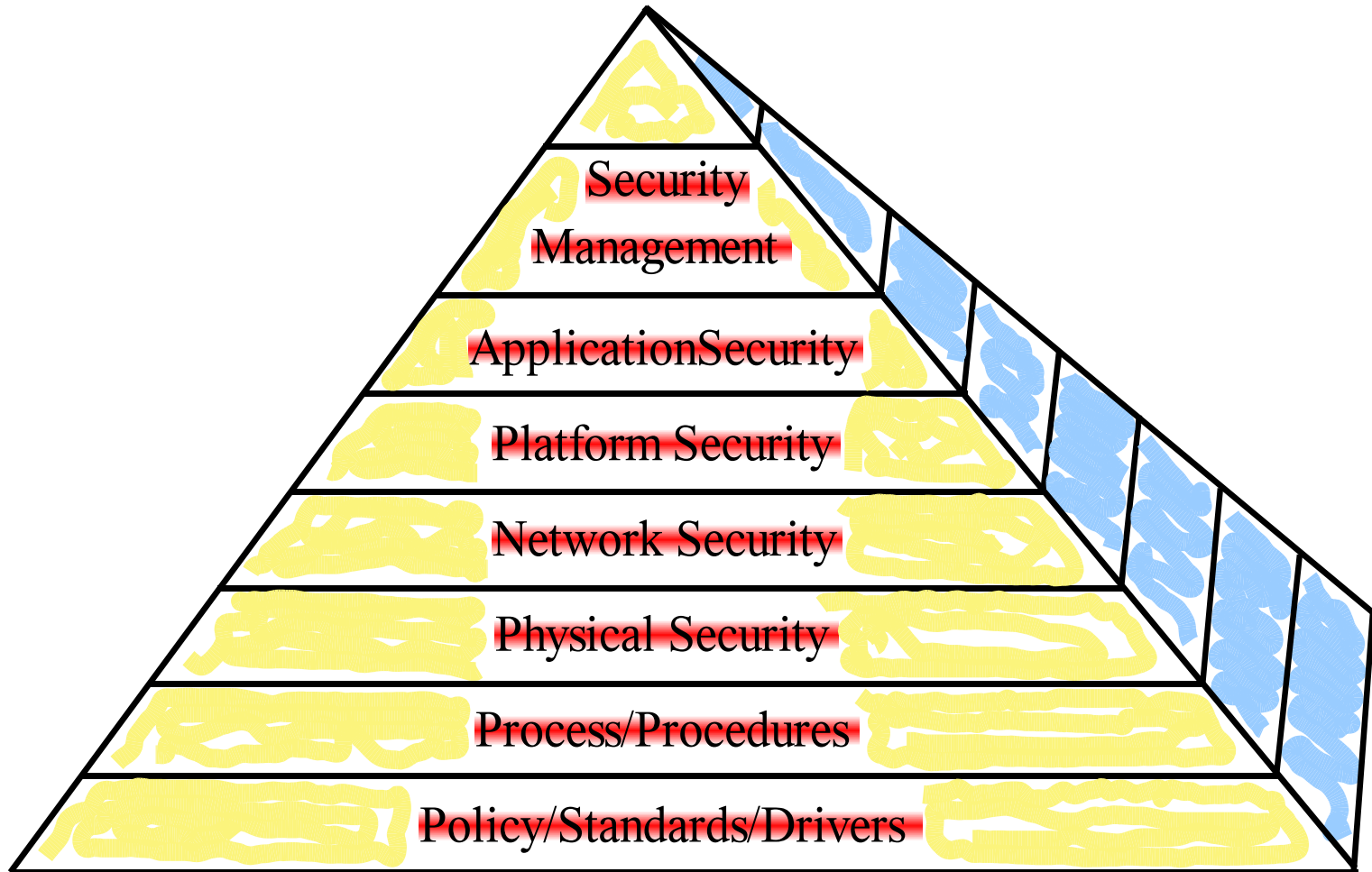
The stuff the sys admins do.

Part of the cost of doing business.

We don't do security stuff here.

I don't know. I never thought about it.

Security Infrastructure



Why Does Security Matter?

Confidentiality

It goes only where I send it

Only the person I intended to gets it

Integrity

What you get is what I sent

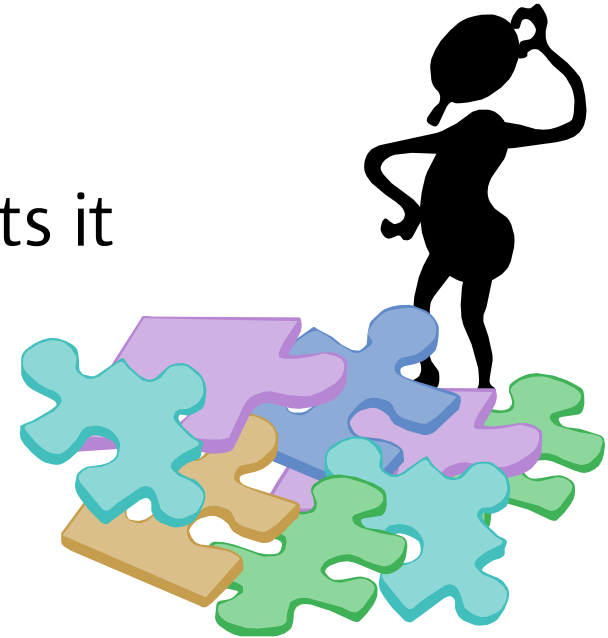
What you sent is what I get

Accessibility

I can get to my data/applications/services

Non-repudiation

I can't deny doing something ex post facto



Five Security Requirements

Identification
Authentication
Authorization
Access Control
Auditing



Identification:

("Who Are You?")

Something you know

Challenge/response

Name/password, Encryption card

Something you have

Tokens, Smartcards

Something you are

Biometrics, RFID/AutoID



Authentication

(“Can you prove it?”)

Single and multi-factor authentication

May be combined with identification

(e.g. Biometrics)

Passwords

A.K.A. self-authentication

Which are actually a fairly weak authentication mechanism

Certificates and Certifying Authorities

Authorization

(“Once you're in, what can you do?”)

Role based

Based on your function in the organization

Policy based

Based on legal and organizational constraints

Workflow/event based

Based on organizational processes

Individual rules based

Based on specifically who you are

Access Control

(“What can you get to?”)

Just because you are authorized does not mean you have access.

Change of permission(s) on some resource

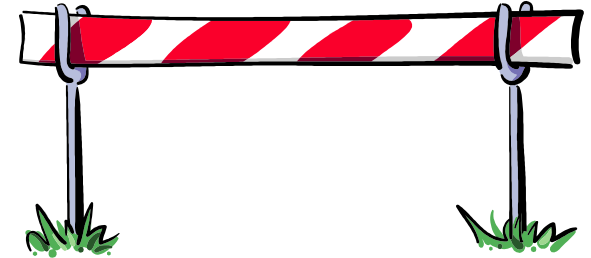
Never got a key/password

ACLs

New users

Shared folders

Can be data (the nouns) or applications (the verbs)



Auditing

(“What happened?”)

Authorized/unauthorized access

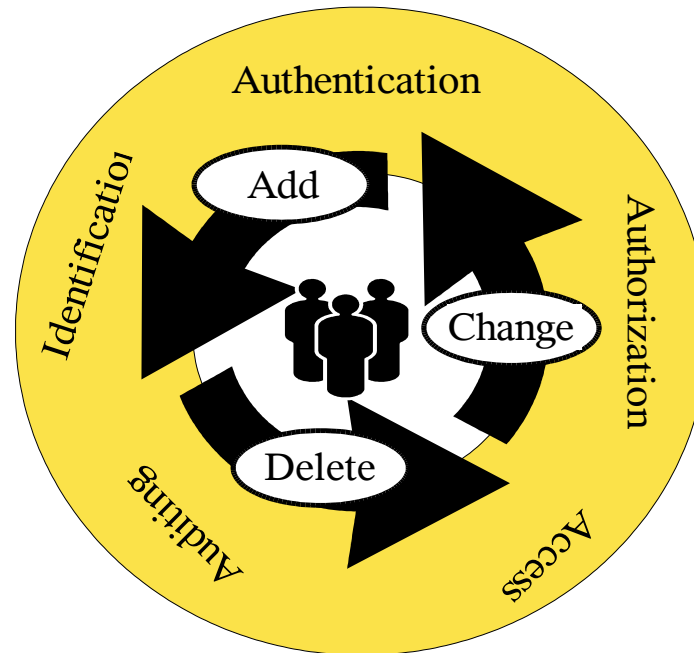
Resource utilization

User education

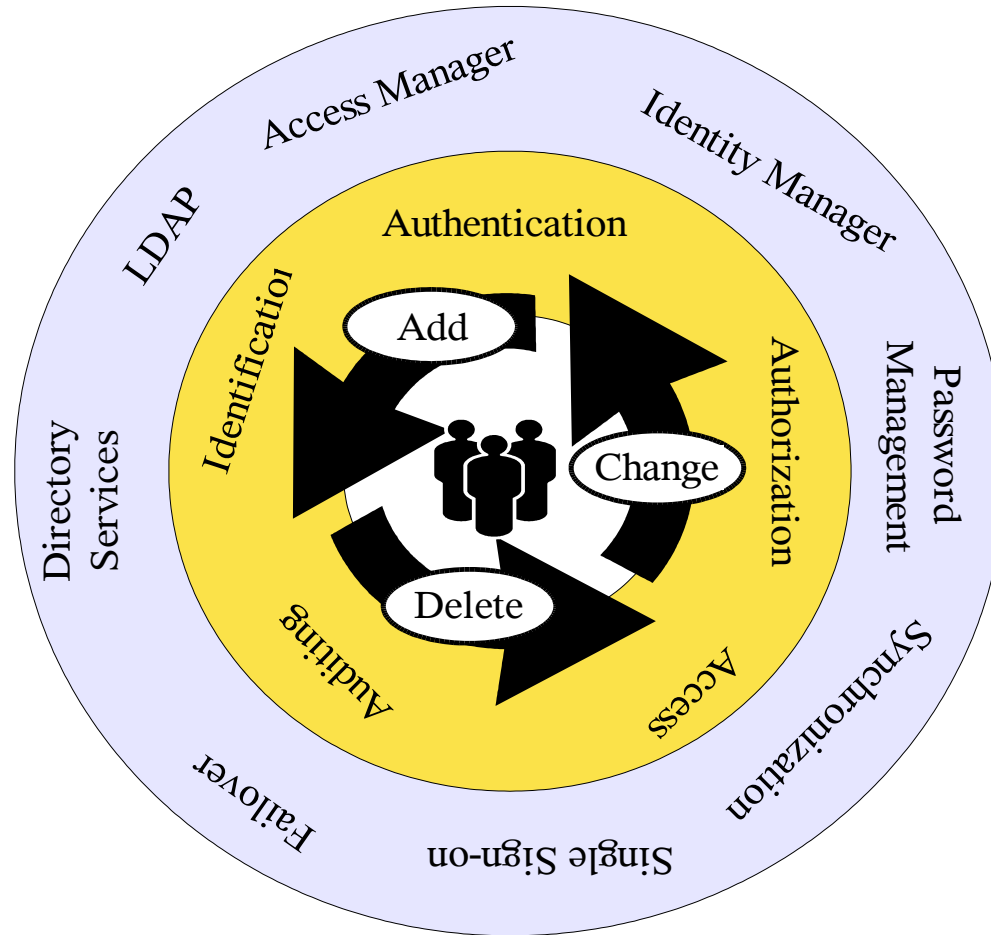
Legal requirements



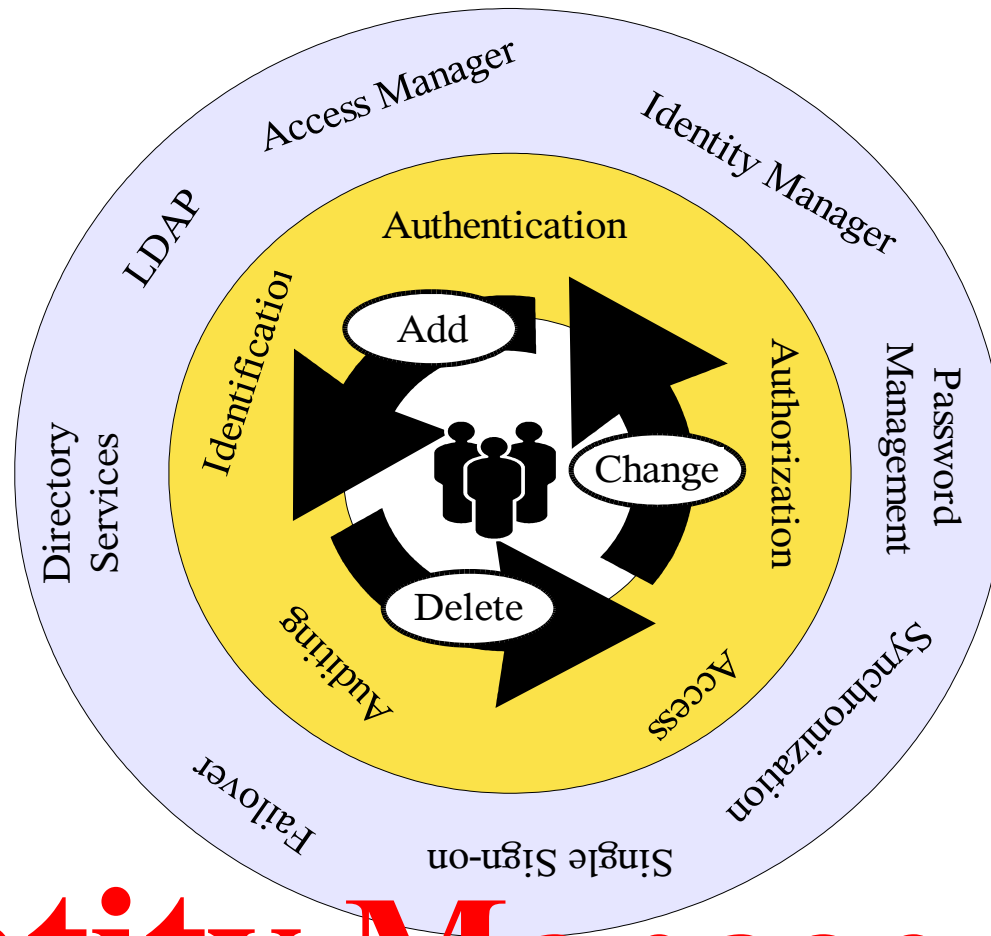
Security Requirements



Enabling Technologies



Putting it into Perspective

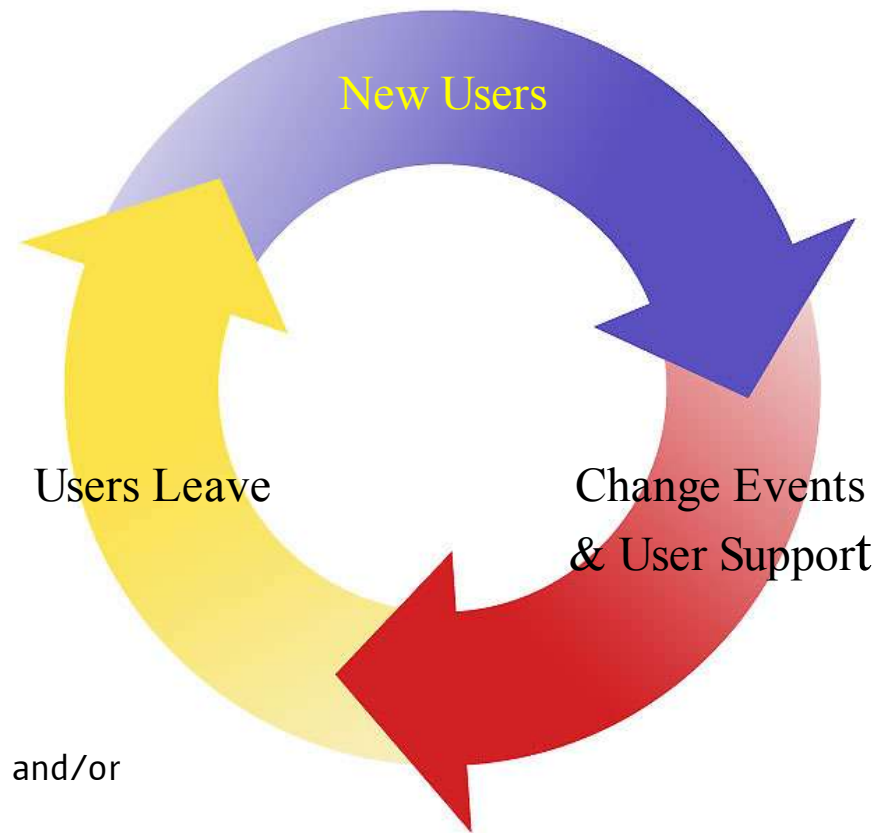


Identity Management

What is Identity Management?

Identity Management is a set of business processes and supporting infrastructures (technologies and operational) for managing the lifecycle of an identity and its relationship to business applications and services.

Dynamic Identity Life Cycle



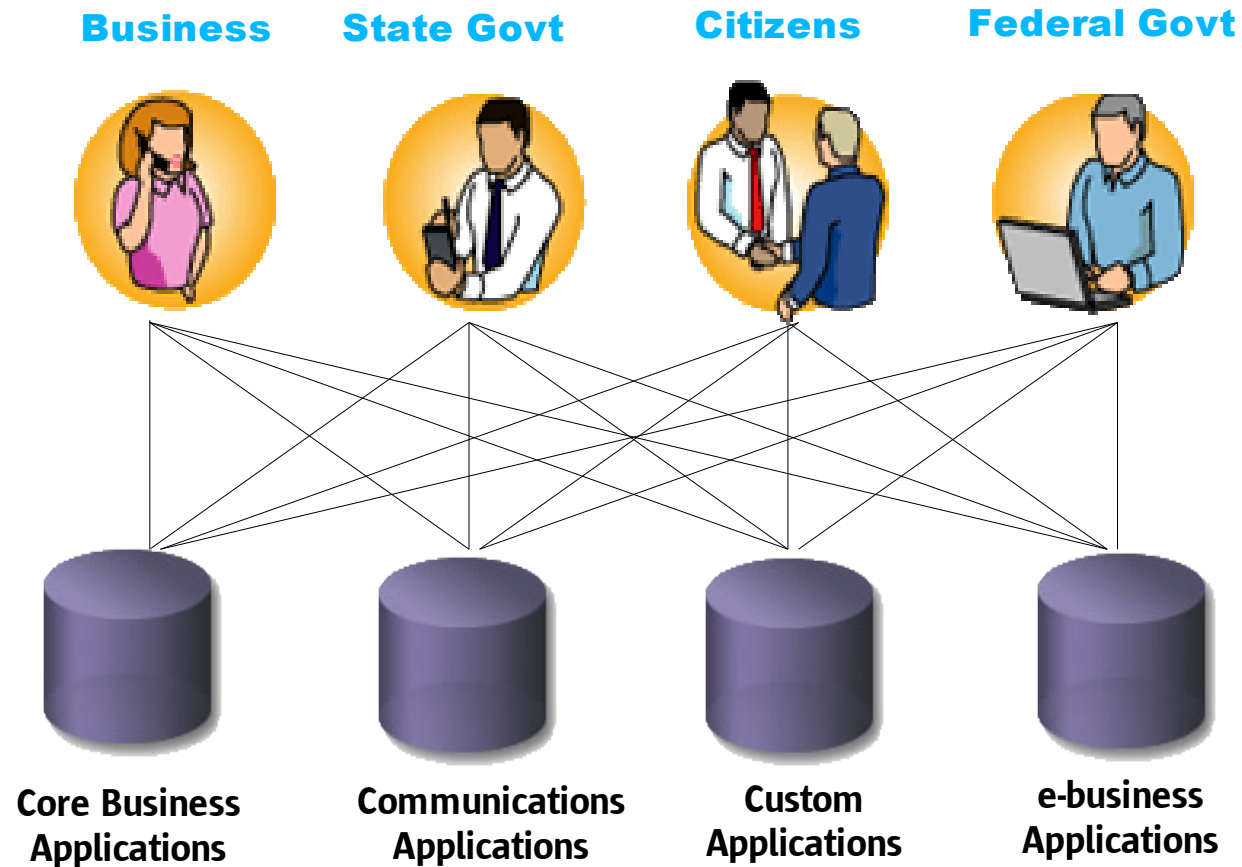
- User entered in HR or user self-registers
- Accounts provisioned to enterprise
- Non-digital assets assigned

- User status updated
- User closes account
- Accounts disabled & removed
- Non-digital resources retrieved and/or canceled

- User status changes
- Password changes
- Profile info changes
- New account requests
- Non-digital assets changed

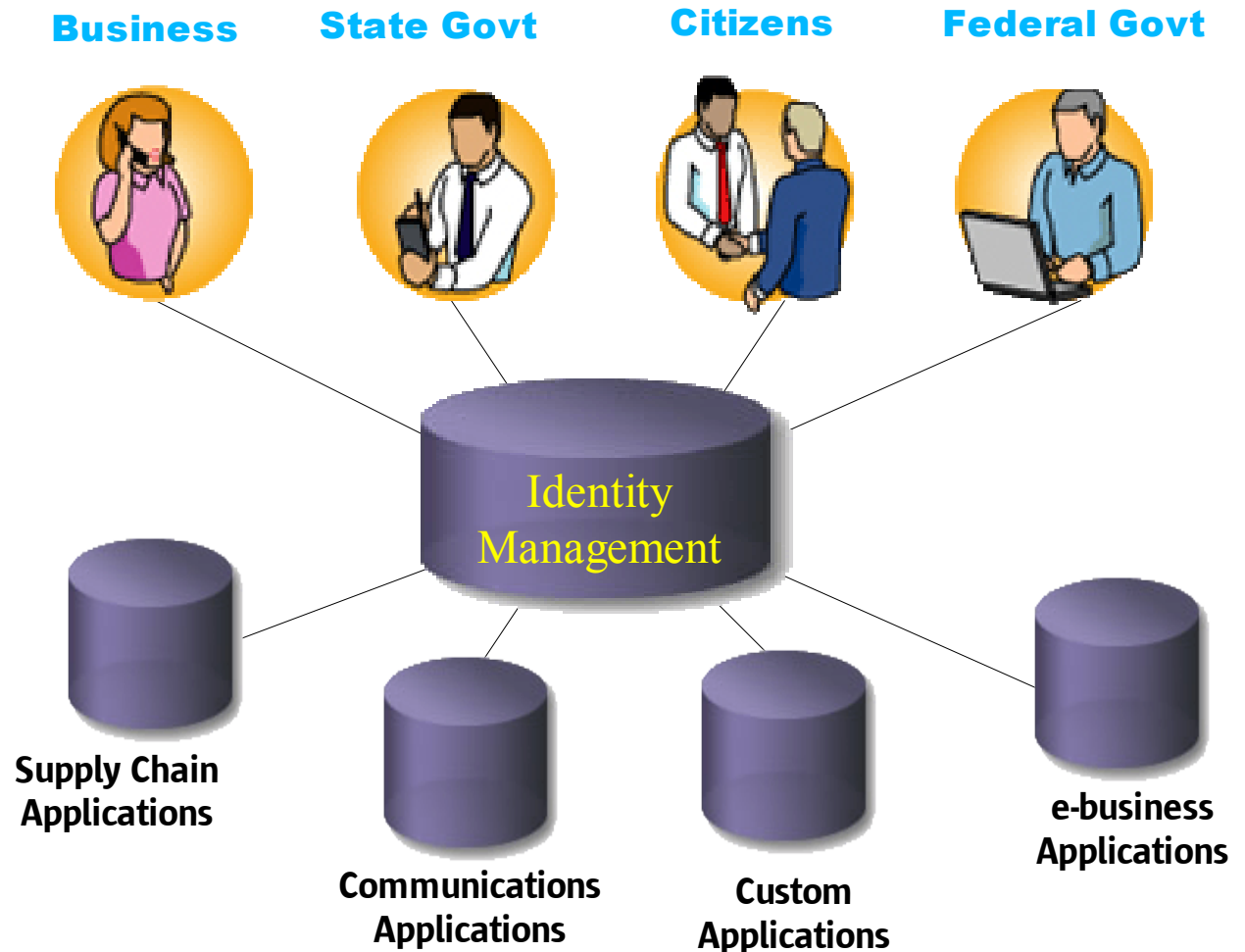
The Identity Crisis: Complexity

- Multiple Communities
- Identity Silos
- Identity Proliferation
- High Admin Costs
- Operational Inefficiencies
- User Profile Control & Ownership
- Adhoc Privacy, Security
- Regulations & Compliance

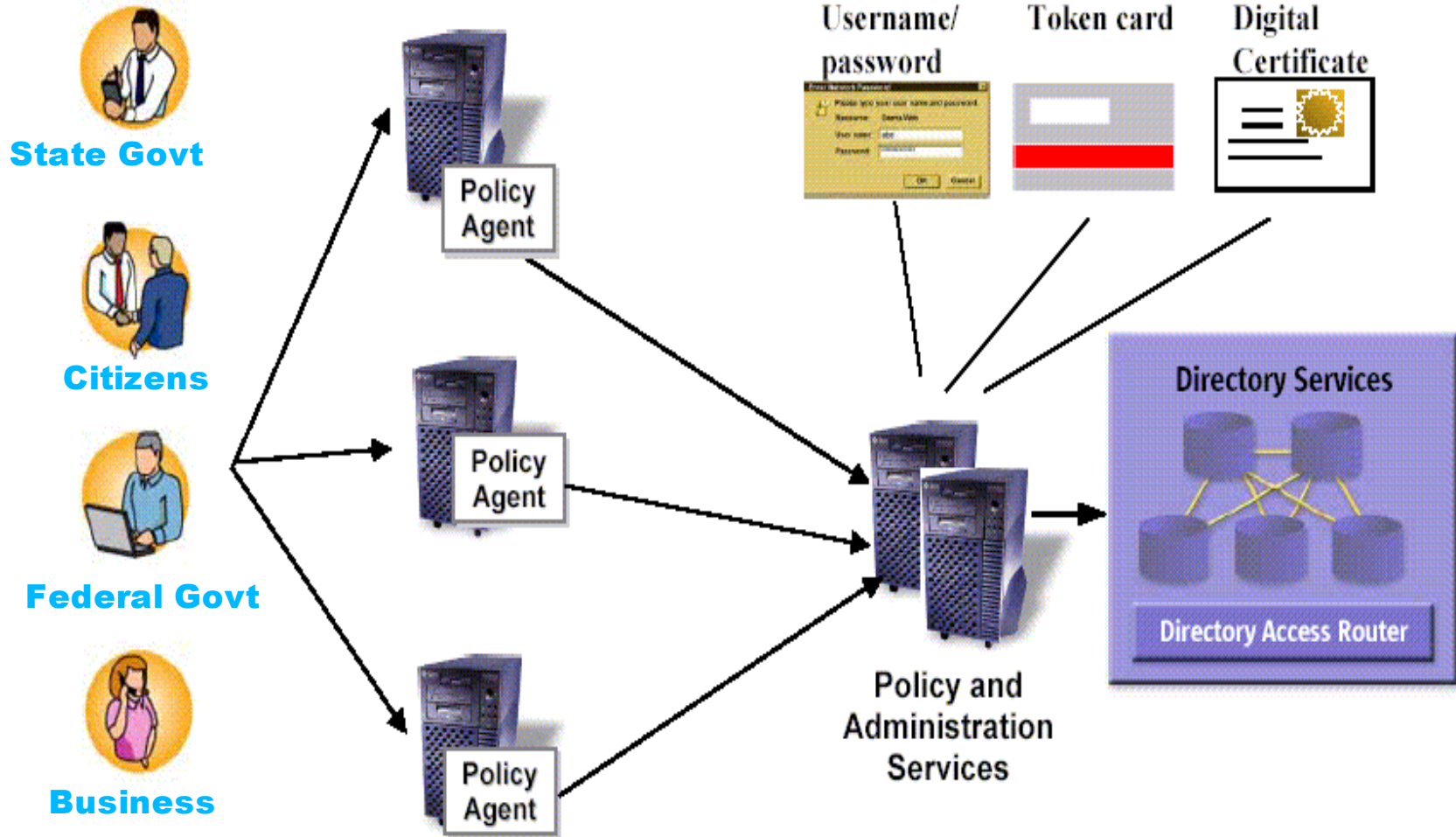


Solution: Identity Management

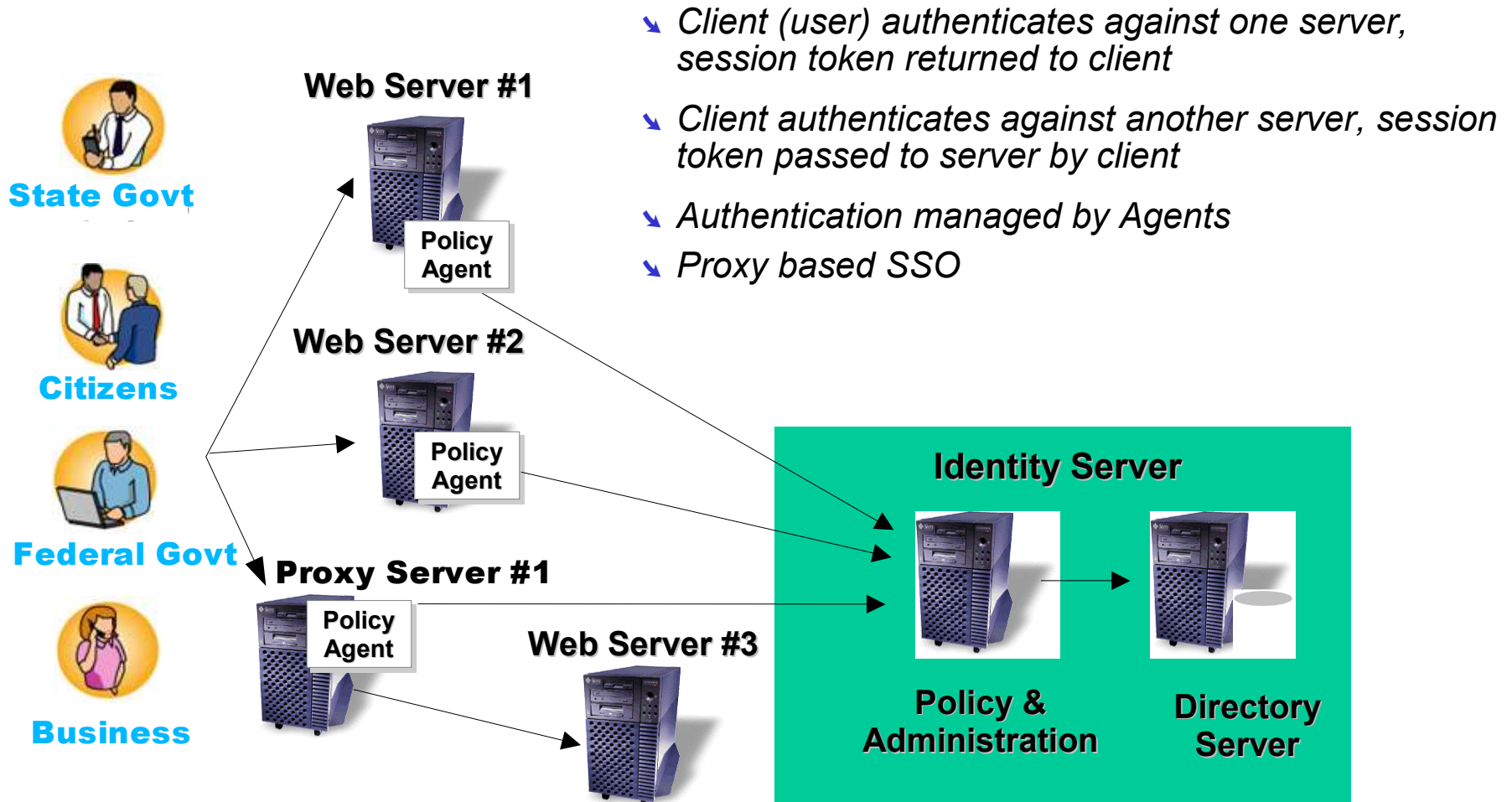
- Complete identity lifecycle management
- Consistent security policies across the network
- Centralized access management
- Self-Service
- Delegated user administration
- Federation



Identity Management Vision

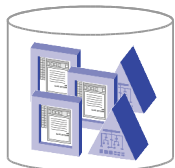


Web Single Sign On



Identity Synchronization: System-to-System Updates

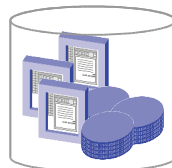
- **Data silos independently owned and manually administered**
- **Manual updates, if occurring, are error-prone**
- **Inconsistent identity information across the enterprise**
- **Inefficient business operations**



Exchange and
Active Directory



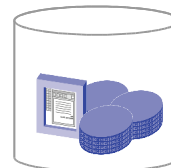
Extranet
Directory



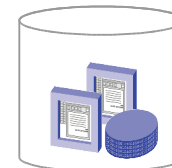
CRM



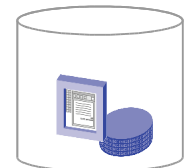
Human
Resources
System



ERP



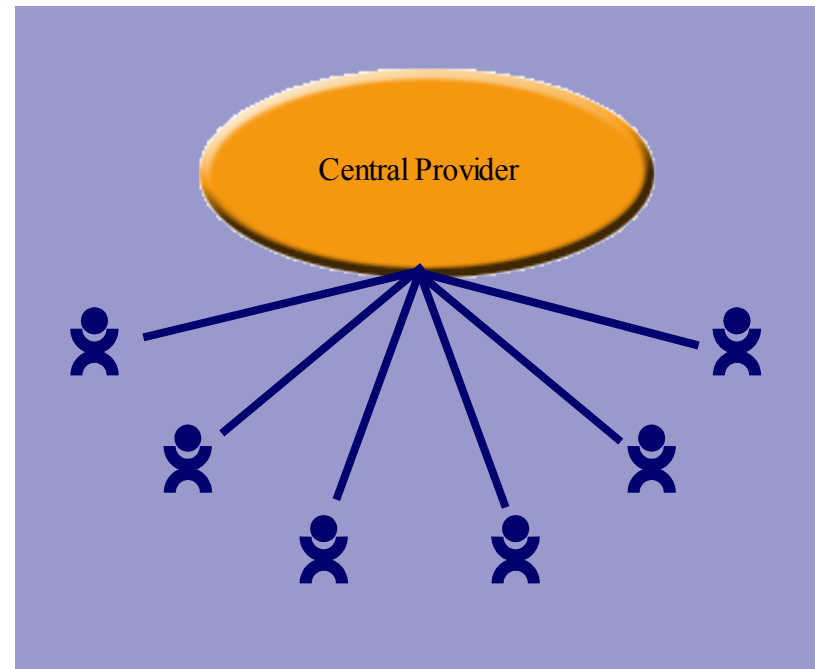
Custom
Application



Payroll Systems

Non-Federated Identity

- Identity and Profiles in a central repository
- Centralized control
- Single point of failure
- Links only similar systems



What is Passport?

- **A Microsoft led initiative to provide centralized network identity, authentication, and authorization**
 - Provides tiered infrastructure (master-replica)
 - Provides loose federation among sub-masters
- **Integration with Active Directory and SQL Server based infrastructures**
 - Required to access MS services (webmail, dev sites)
 - Single Sign-on
 - Integration with payment services (eWallet)
- **Membership mostly Microsoft sites and related properties (MSN, Hotmail) and select large e-tailers (Amazon, eBay)**
- **Not being emphasized as heavily over last 18 months**

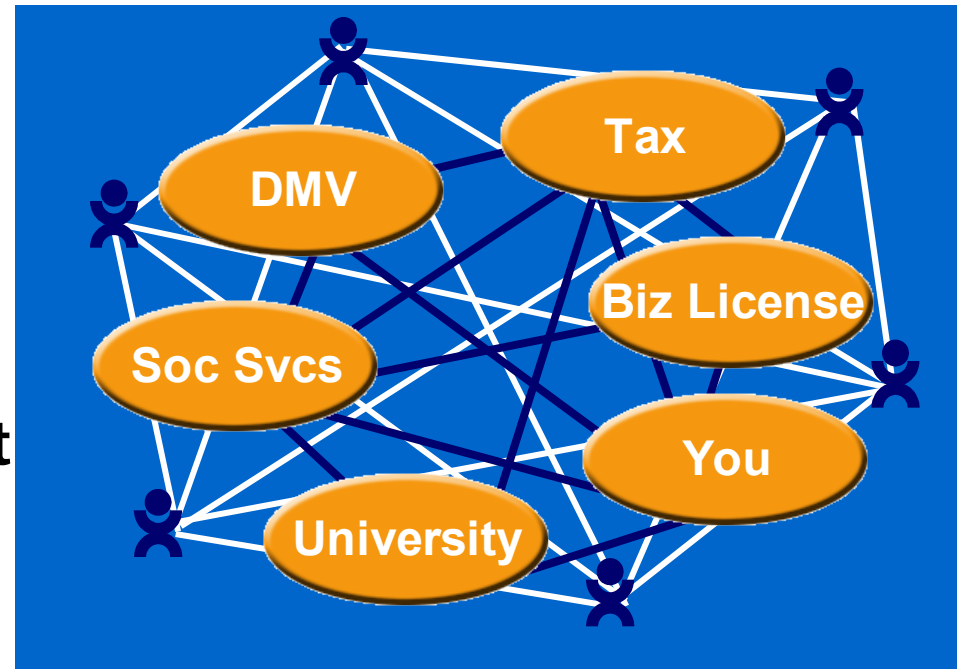
What is a “Federated” Identity?

You manage your own directories...

...a standard allows directories to link together upon authorised request

Federation avoids a single point of failure or control.

Build on what you already have



What is Liberty?

- **An industry alliance to drive open, neutral, federated standards for network identity, authentication, and authorization**
- **Extends SAML to provide framework for:**
 - **Opt-in linking of user accounts**
 - **Single Sign-on**
 - **Global Log Out**
 - **User anonymity**
- **Membership spans industries**
 - **Government, Financial, Banking, Travel, Airlines, Telecom, ISPs, Wireless/Mobile operators, Device Manufacturers, Technology vendors**
- **Over 2 billion identities represented**

The Liberty Alliance

Membership spans industries and continents

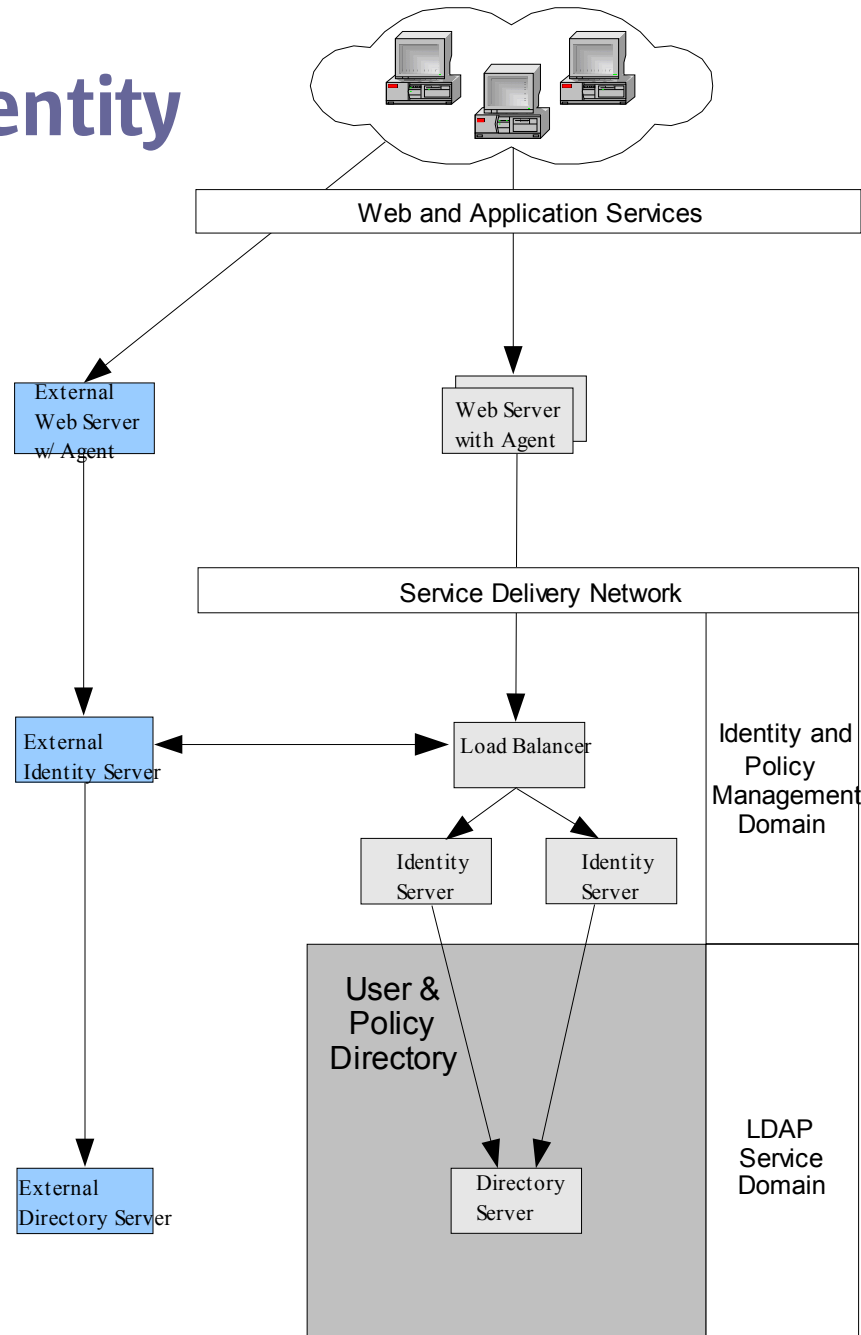
- Government, Financial, Banking, Travel, Airlines, Telecom Carriers, ISPs, Wireless/Mobile operators, Device manufacturers, Technology vendors
- 174 members
- Over 2 billion identities represented



Federated Identity

- SAML v1.1 specifications
 - Interoperability with other applications
 - Exchange of security assertions
- Liberty Alliance v2.0 specifications
 - Identity Federation(ID-FF)
 - Identity Web Services Framework(ID-WSF) for Identity Services like Discovery Service
 - Identity Service Instance Specifications(ID-SIS), Personal Profile Service, Employee Profile Service

Federated Identity



Sun's Commitment to Standards

Industry Standard	Sun Leadership
Liberty Alliance (Federation and Identity Services)	Management board member; first vendor to earn 'Liberty Alliance interoperable' logo for Access Manager
OASIS Security Assertion Markup Language (SAML)	Co-founder, former chair, and current secretary of Security Services technical committee; leader in defining SAML; first to deliver in Access Manager
OASIS Service Provisioning Markup Language (SPML)	Chair of OASIS Provisioning Services Technical Committee; major contributor to the SPML specification; first to release open source SPML toolkit
OASIS eXtensible Access Control Markup Language (XACML)	Secretary of the OASIS XACML technical committee; first to release open source version of XACML 1.0.
Web Services Interoperability Organization (WS-I)	Board member and vice-chair of the Basic Security Profile Working Group of WS-I
Lightweight Directory Access Protocol (LDAP)	Co-author of the LDAP V3 technical specification and first vendor to ship reference LDAP implementation

Questions ?



Goodwin Ting
goodwin.ting@sun.com

