



Tivoli Federated Identity Manager

Sven-Erik Vestergaard
Certified IT Specialist
Security architect
SWG Nordic
svest@dk.ibm.com

IBM Software Day Vilnius 2009



Agenda

- IBM strategy on IAA
- What is a federation from a business perspective
- How does it work
- Web services severity identity propagation
- Customer cases

Identity and Access Assurance

Tivoli Capabilities

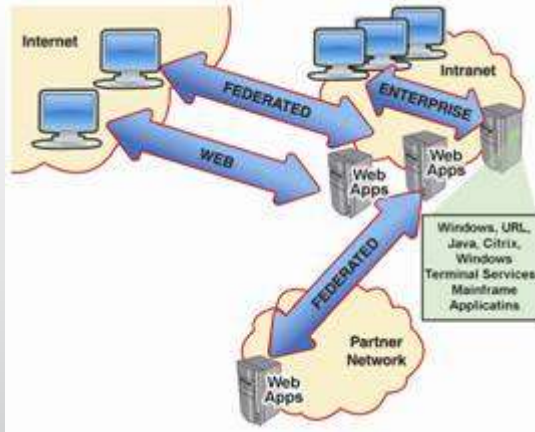
- User provisioning & role management
- Unified single-sign-on
- Privileged user activity audit & reporting
- Directory and integration services
- Log Management
- Self-service password reset
- Identity Assurance / Strong authentication management

Benefits:

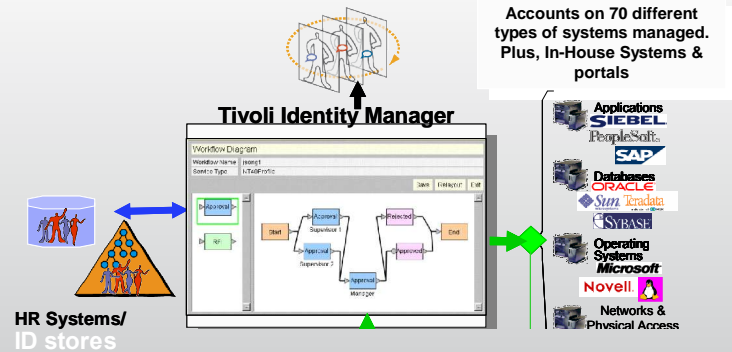
- Reduce help desk operating expenses
- Comply with regulations
- Improve user productivity
- Reduce risk from privileged insiders
- Respond quickly to business initiatives (e.g. new applications, M&A, restructuring)

Getting started with Identity and Access Assurance

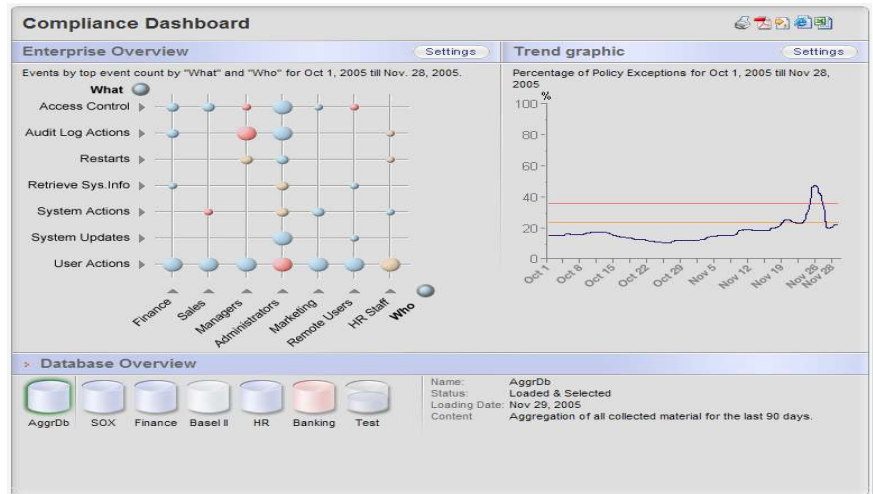
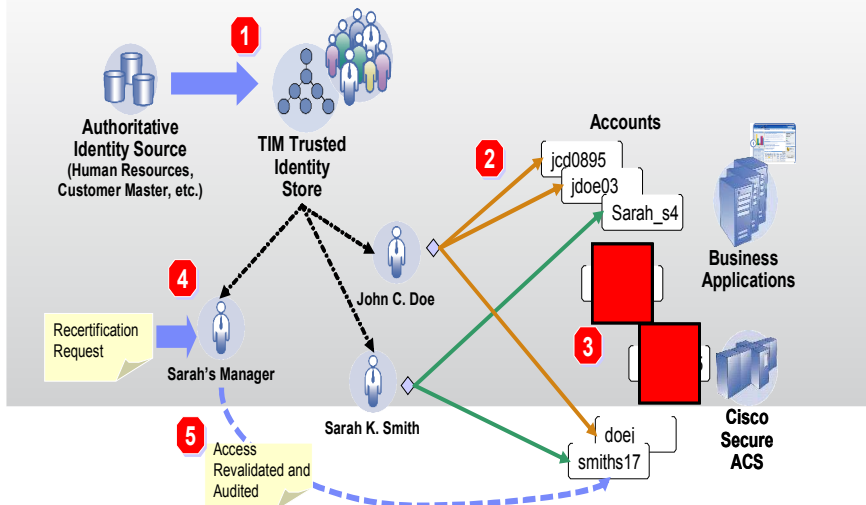
Single Sign On
& Password Management



User Provisioning / Role Management



Access Attestation



Agenda

- What is a federation from a business perspective

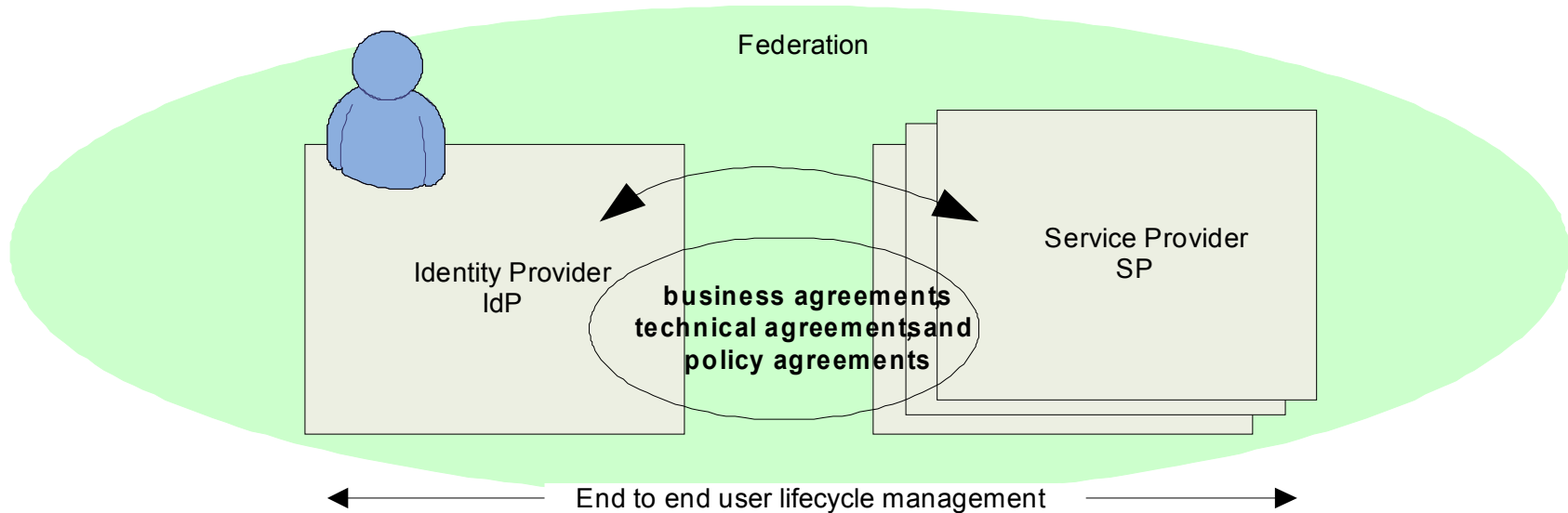
Key Business Models Driving Federation

- Mergers and Acquisitions
 - Success of a merger is often related to how quickly disparate systems can be integrated to meet the needs of the business.
- Collaboration between autonomous Business Units
 - Many companies maintain separate autonomous business units for political, competitive, and regulatory reasons but still require cross-unit access for management and customers.
- Collaborative development with Partners
 - Some organizations are working more with partners on new strategic developments, thereby increasing the need for federated access to partner systems.
- Employee access to Outsourced Services
 - Costs of building and maintaining point-to-point solutions for access to outsourced solutions can dilute benefits of outsourcing.

Key Business Models Driving Federation (cont)

- Service Provider Automation
 - Service providers can incur significant costs in managing user accounts across their customer base – federated technologies can dramatically reduce these costs.
- Government collaboration
 - Government security based initiatives to gain access to law enforcement and a wide range of other personal data in a secure, efficient manner.
- Improved Corporate Governance
 - Key issue with audit/compliance is management of external access to systems.

Federated Identity Management



- Objectives
 - Lower Identity Management costs
 - Improve user experience
 - Provide end-to-end security and trust foundation for inter-organization application integration
- Leverages concept of a portable identity
 - Identity is “asserted” from a trusted third-party
 - Passport
 - Credit / ATM Card
 - Drivers License

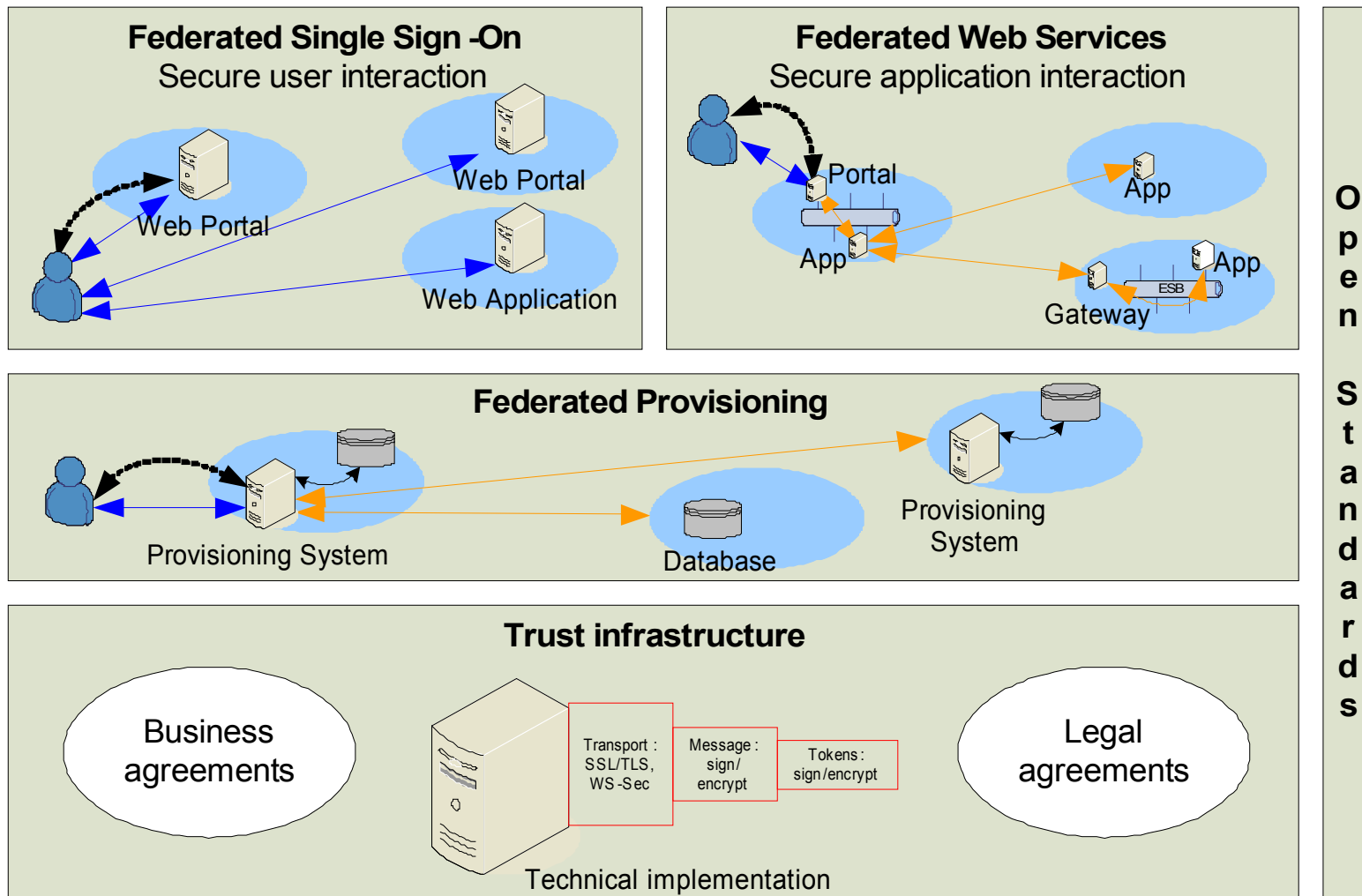
What does IBM Tivoli Federated Identity Manager (TFIM) bring to table?

- Ability to handle identity/attribute transformation as part of token handling
- Ability to exchange token types as part of validation of request at edge
 - Enables advanced “intermediary” type functionality
- Ability to do authorization decisions at abstract WSDL level
 - Independent of WSDL binding
- Integrates with TAM Authorization
 - Access allowed? (Yes/No)
 - Protected Object Policies (e.g. Time of Day)
 - Authorization Rules (authorization policies based on client attributes)
- Audit
- All of this in a standards-based manner!

Agenda

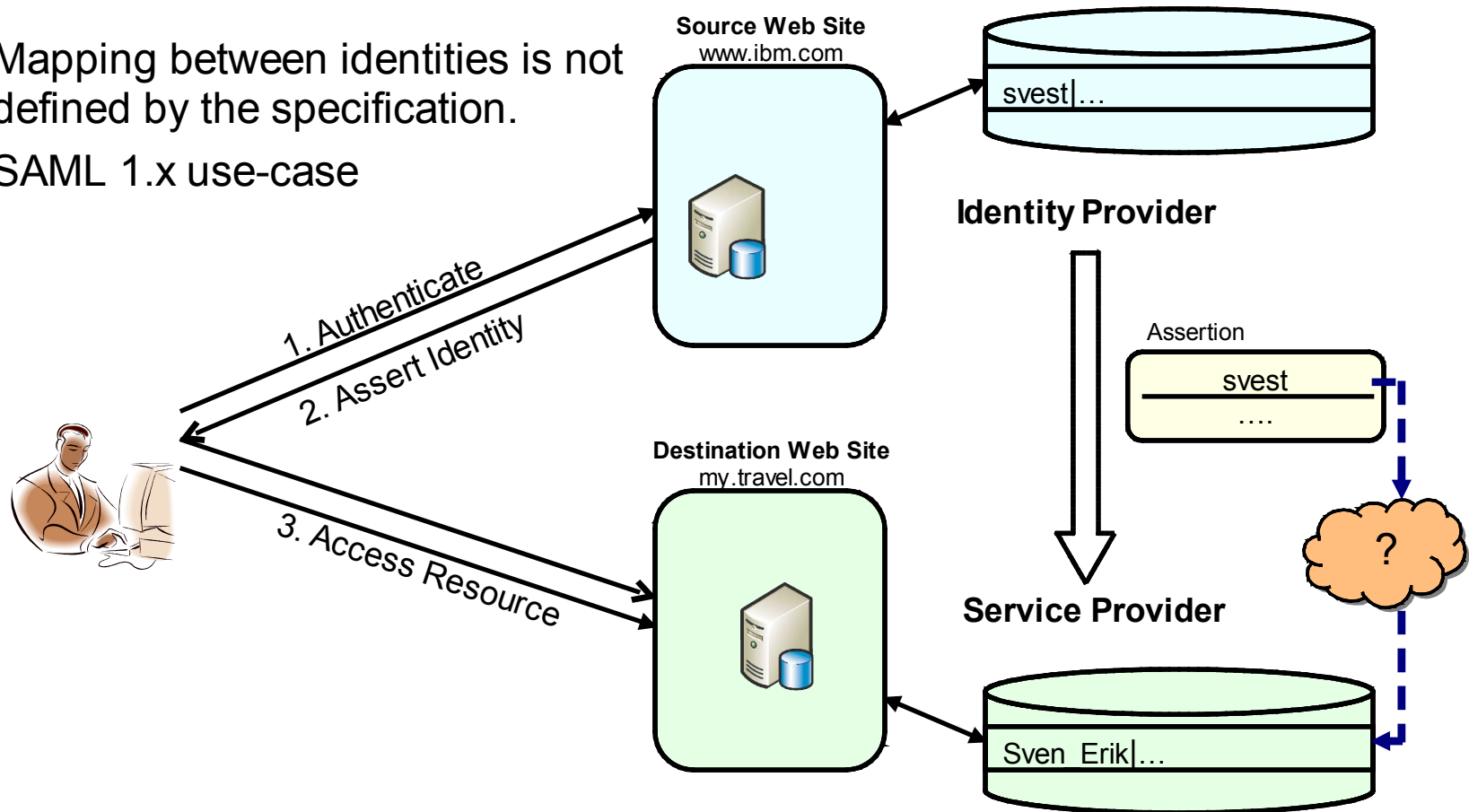
- How does it work

TFIM Architecture Overview



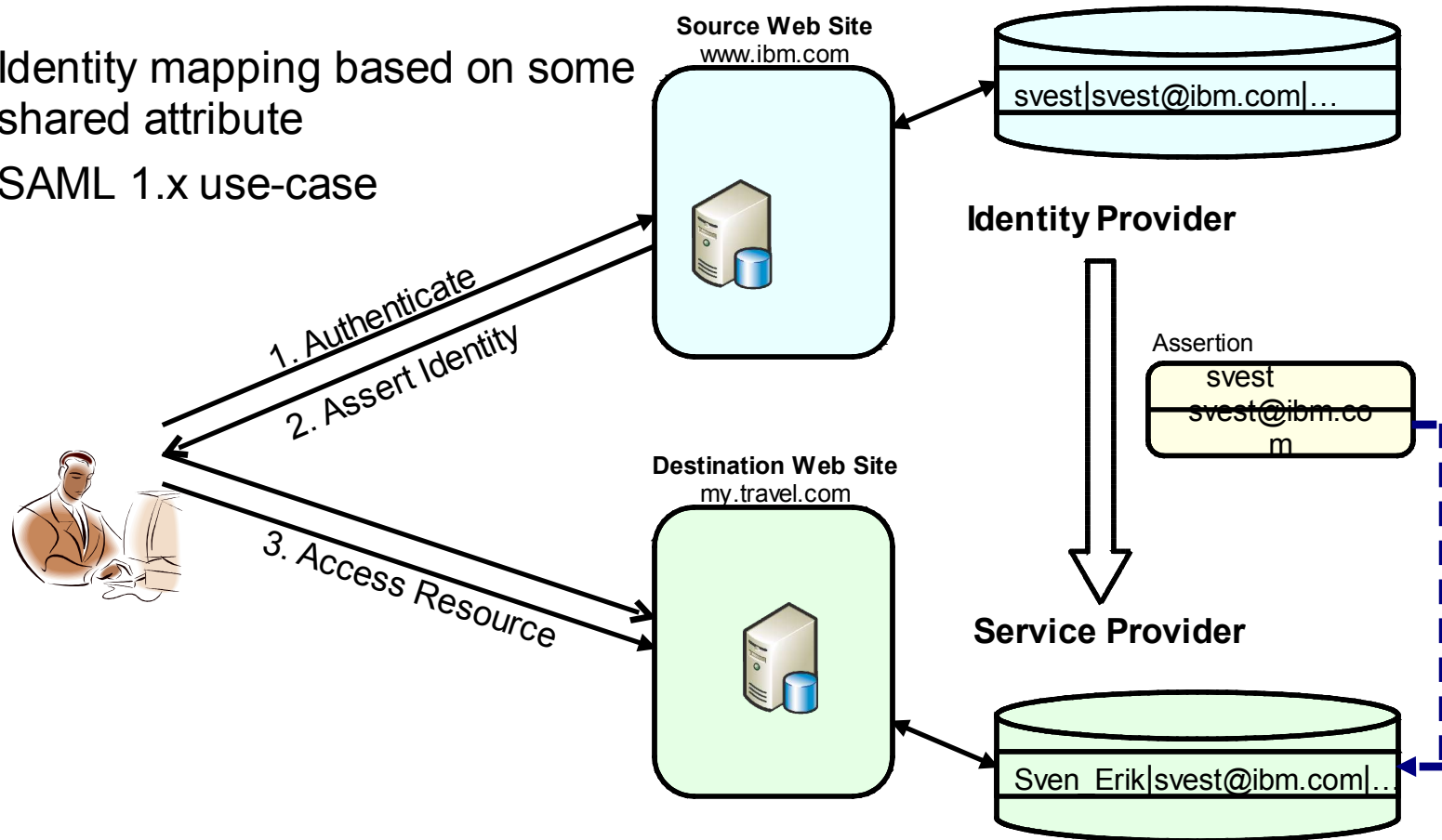
Identity Federation – SSO with OOB Acct Linking (cont)

- Mapping between identities is not defined by the specification.
- SAML 1.x use-case

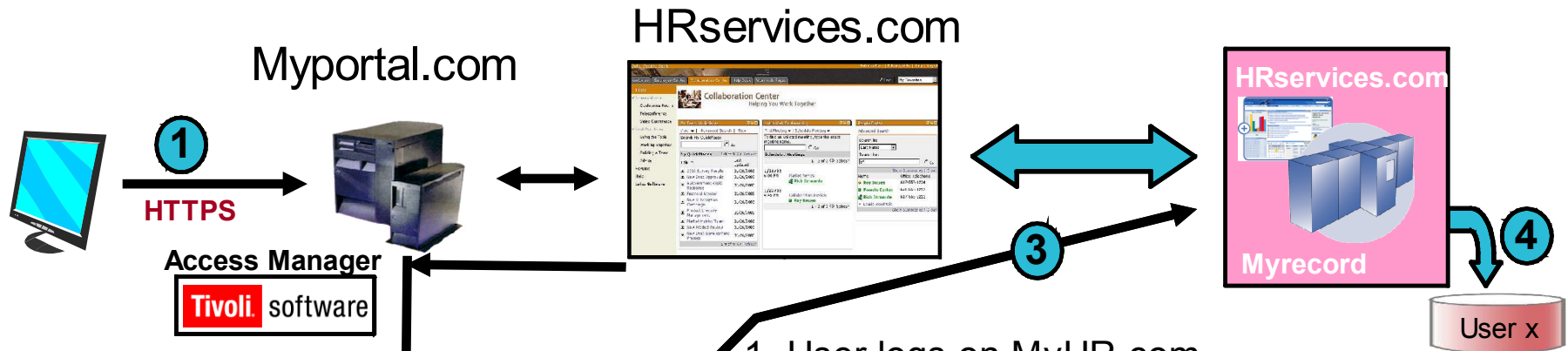


Identity Federation – Attribute Federation

- Identity mapping based on some shared attribute
- SAML 1.x use-case



A Quick, Practical Example — Partner Case



1. User logs on MyHR.com
 - TAMEb authenticates user, creates session
 - TAMEb controls user access & session mgmt.

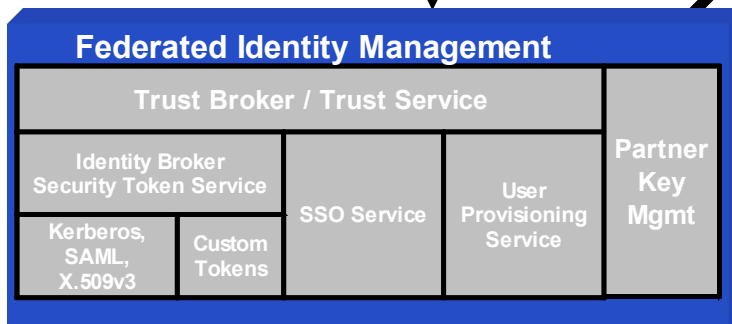
2. User clicks on third-party link Options.com
 - Link configured for Liberty, WS-Fed, or SAML

TAM consults FIM

3. FIM initiates SSO with 3rd party site
 - FIM creates SSO Token user session

4. Options.com maps token to local identity

*** User has transparent SSO to third-party ***



SSO

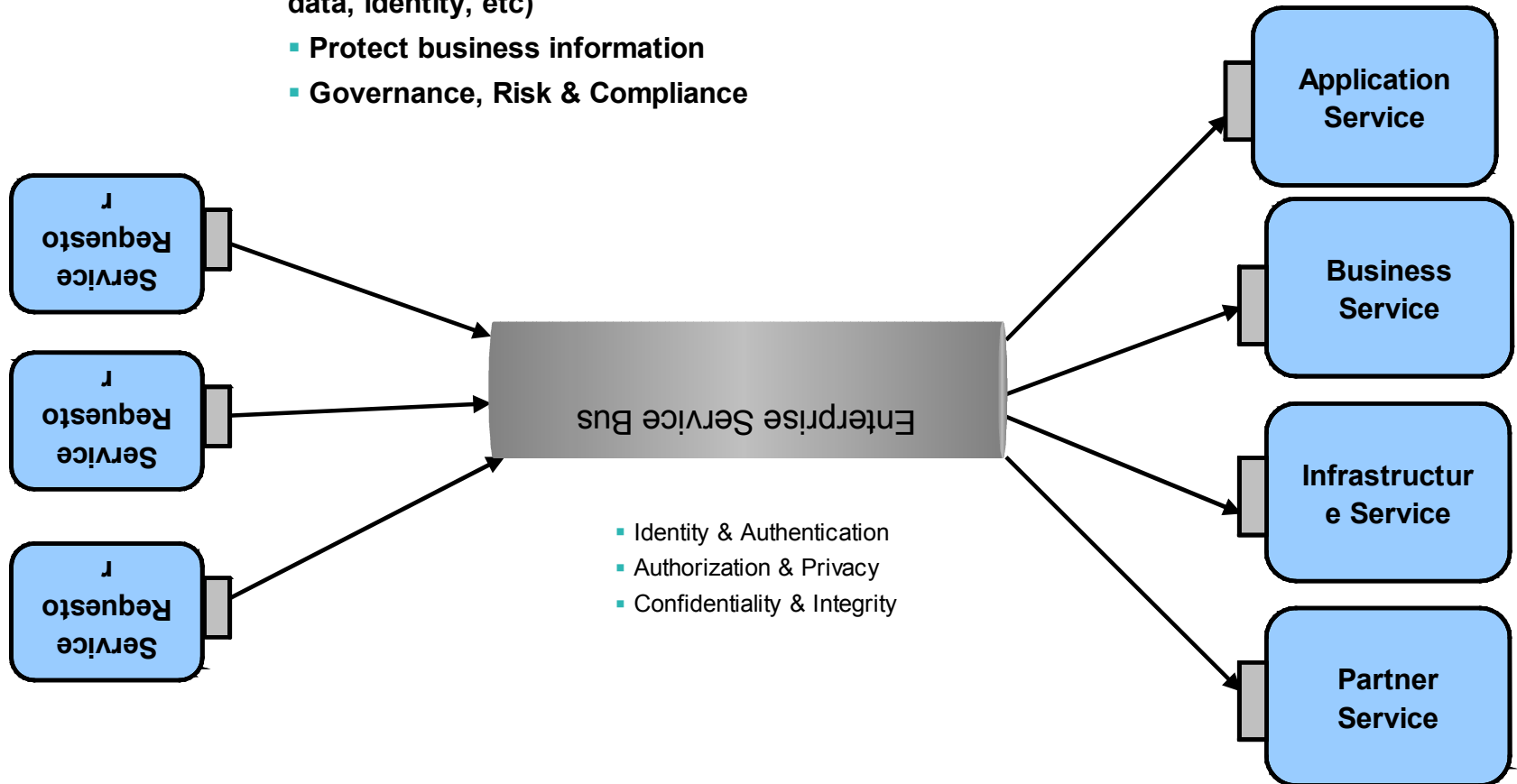
- SAML
- Liberty
- WS-Federation

Agenda

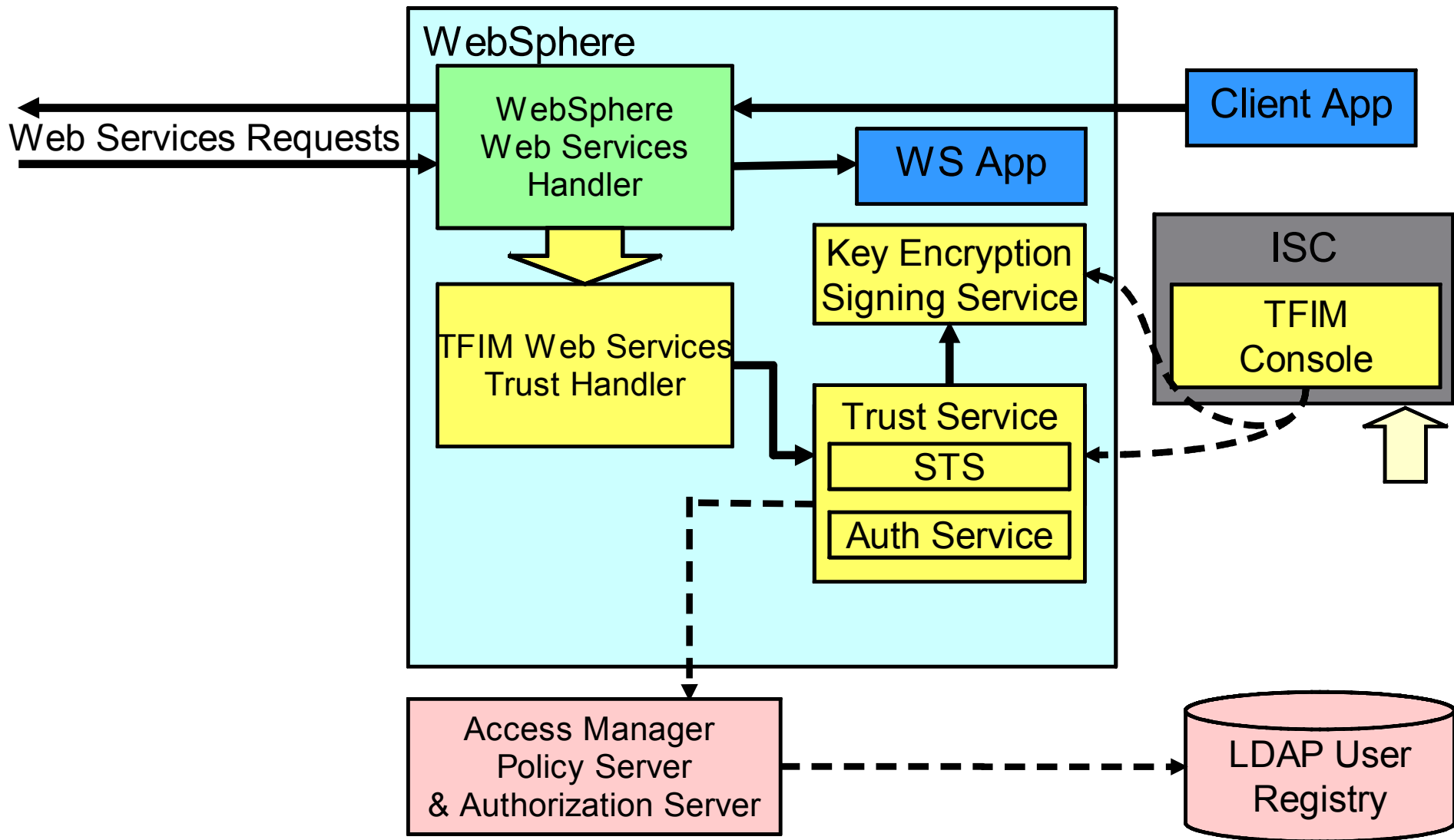
- Web services severity identity propagation

Use Case – Services Integration

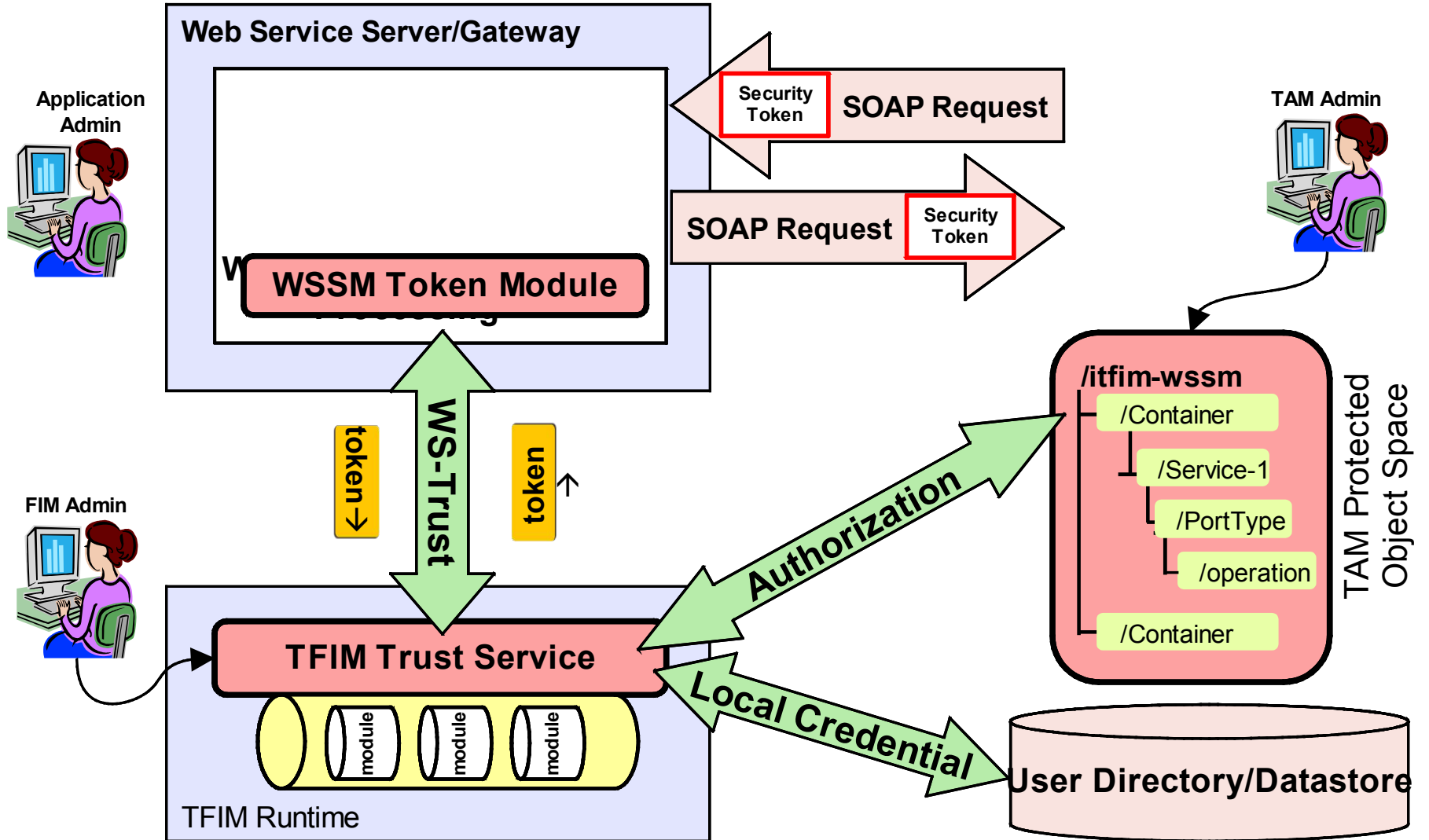
- Propagate identity: Cross domain/realm identity mapping and token transformation
- Reflect business relationships: Trust Management (for data, identity, etc)
- Protect business information
- Governance, Risk & Compliance



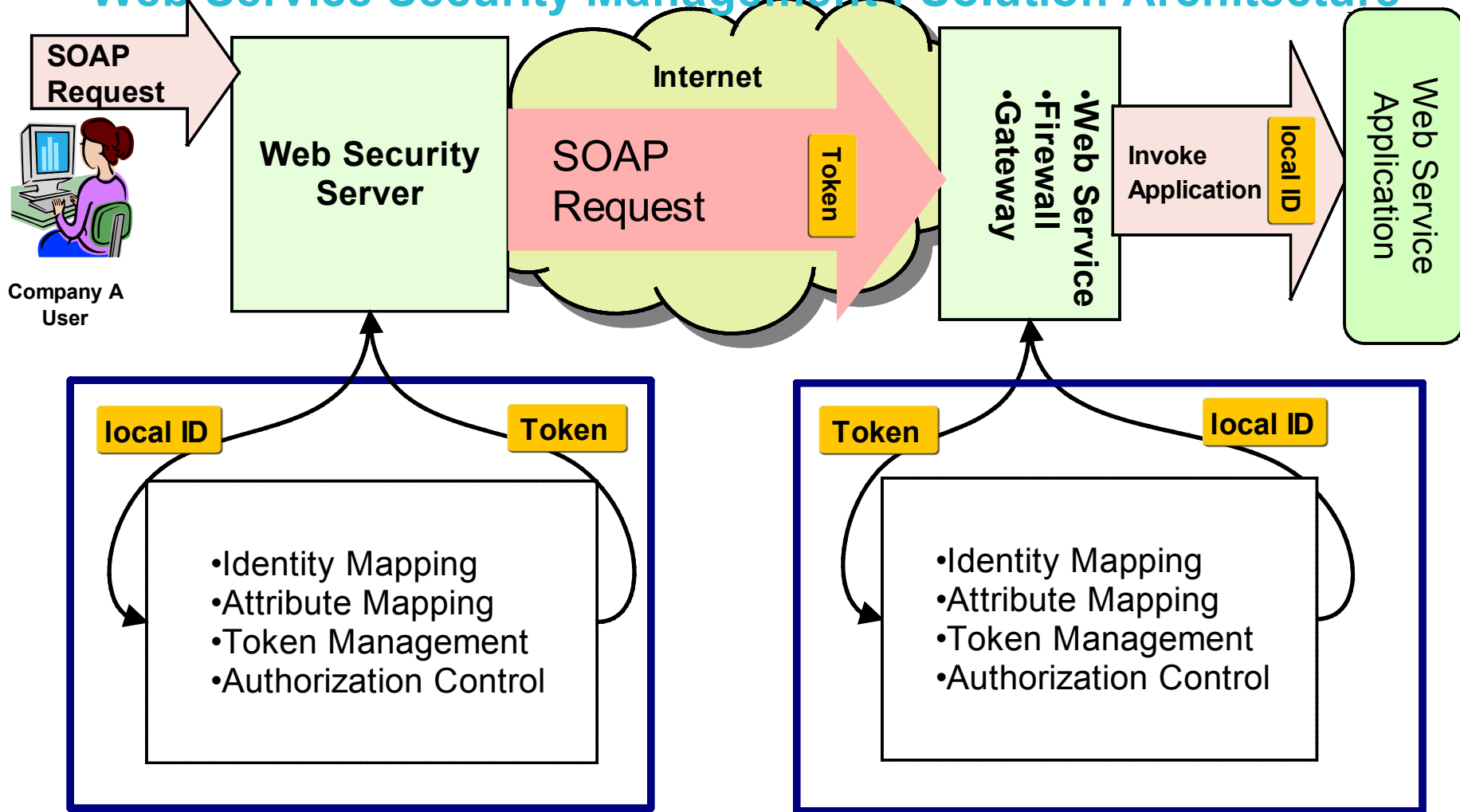
TFIM Components for Web Services Security Management



TFIM WSSM – Generic Design Overview



Web Service Security Management : Solution Architecture



IBM Tivoli Federated Identity Manager

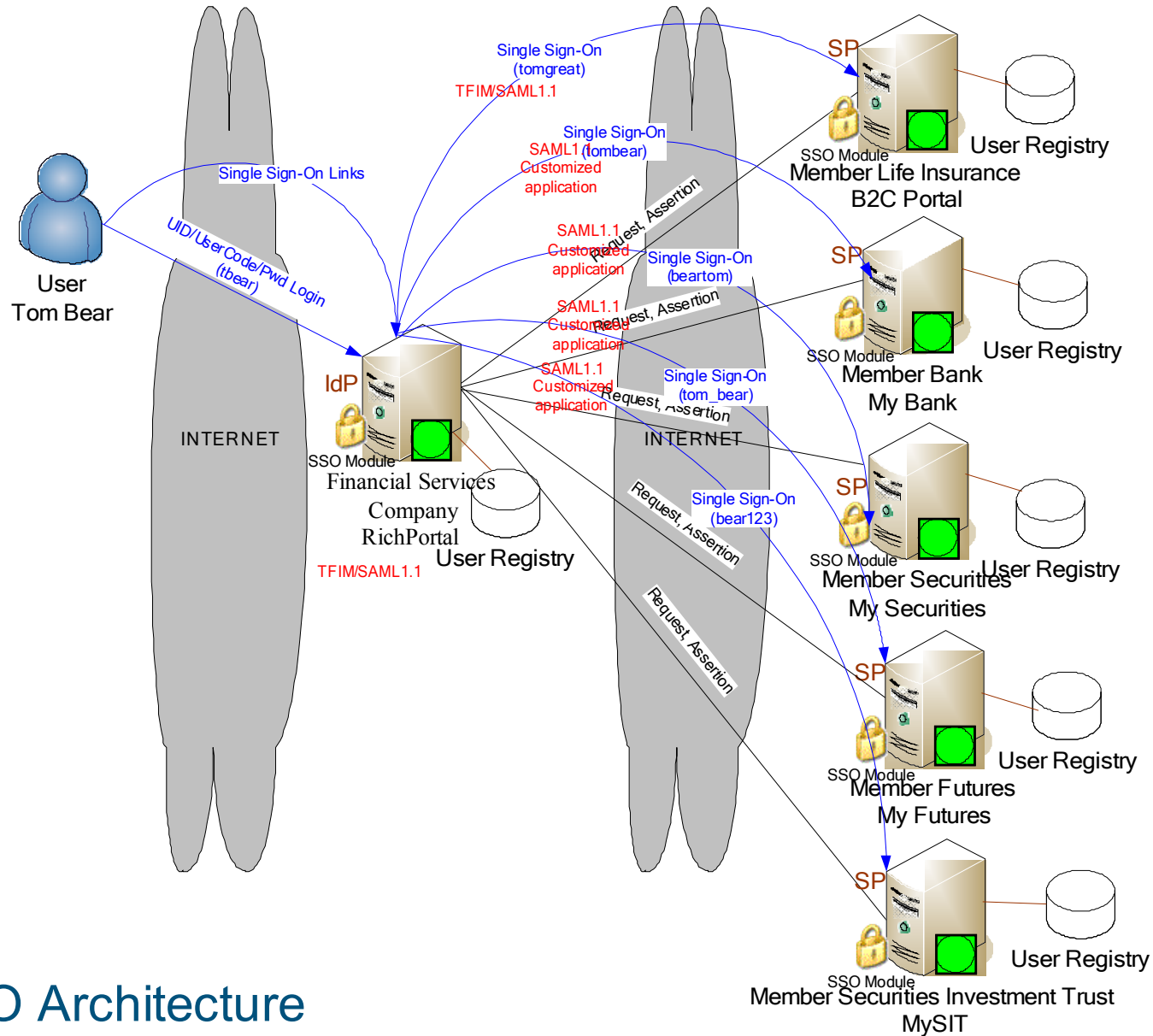
- Federated Single Sign-On
 - Integration with IBM Tivoli Access Manager
 - Supported Protocols:
 - SAML 1.0 / 1.1 / 2.0
 - WS-Federation
 - Liberty 1.1 / 1.2

- Federated Web Services
 - WS-Trust based integration with Enterprise Service Buses, XML Gateways
 - Integration with WebSphere Application Server
 - SOAP, JCA and JDBC integration
 - SAML modules to allow WAS to generate/consume SAML assertions in WS-Security headers of SOAP message
 - Evolving into Identity Propagation in SOA

- Federated Provisioning
 - Provides linking of local provisioning systems
 - Supported Protocol:
 - WS-Provisioning

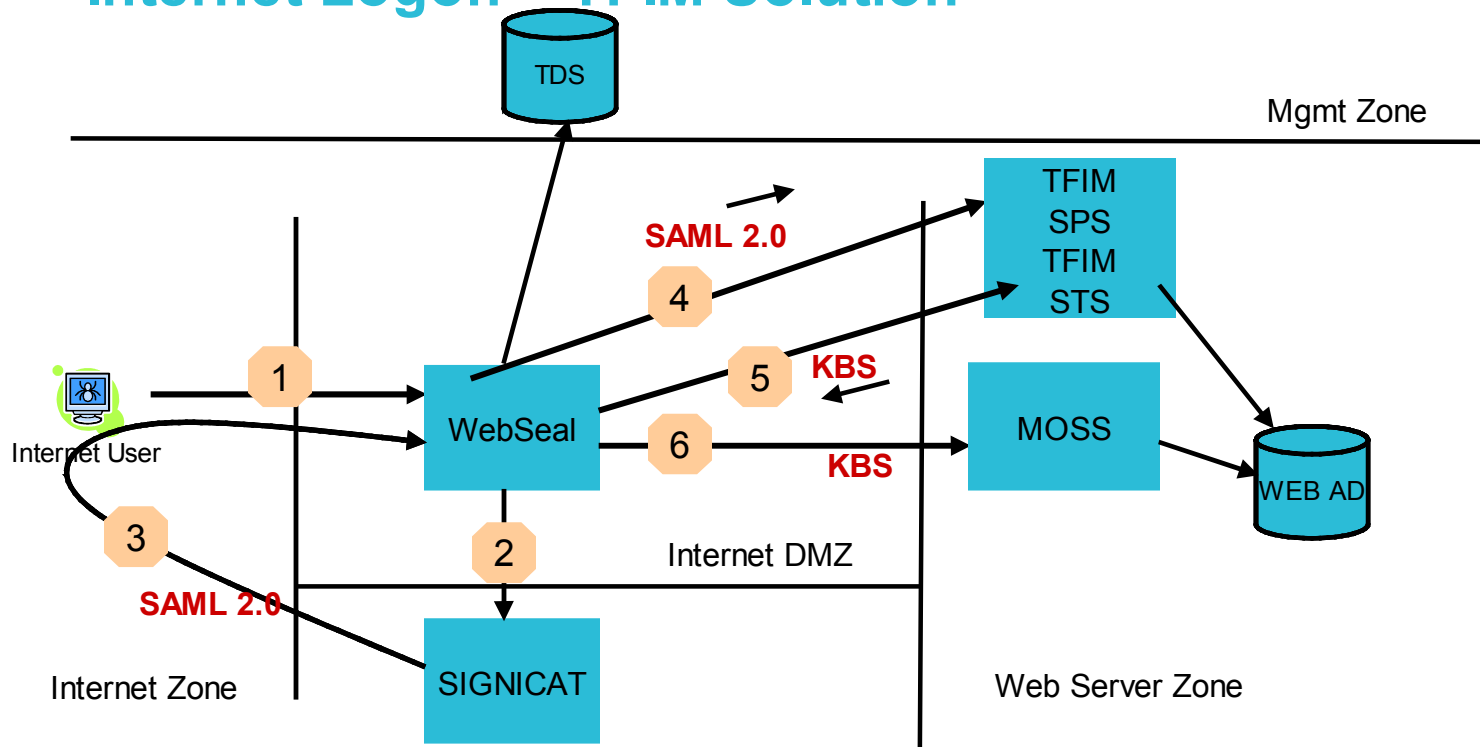
Agenda

- Customer cases



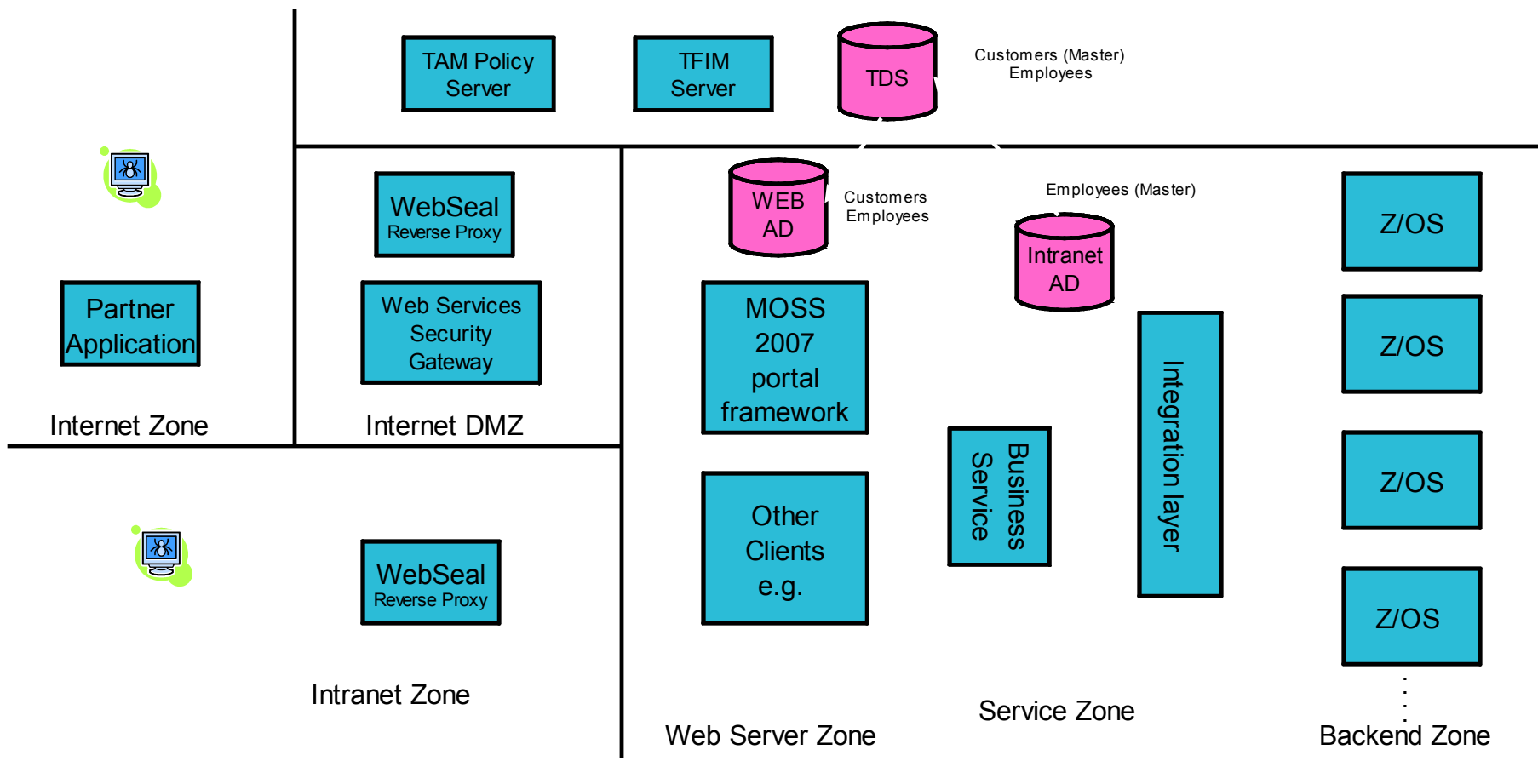
SSO Architecture

Internet Logon – TFIM Solution



1. User accesses protected page – no session defined
2. Reroute to Signincaat
3. Signicat authenticates user and sends SAML 2.0 encrypted assertion through browser picked up by WebSeal
4. Single Protocol Service - TFIM called to create HTTP HDR based on SAML 2.0 assertions
5. Single Token Service – WS-Trust used to create KBS token
6. Request sent to Moss with correct KBS token

SOA Security Overview



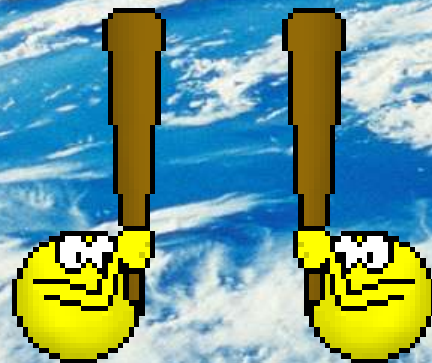
Does This Also Help with Compliance?

You bet.

One of the hardest compliance issues to solve is:

“Prove to me that your external users still need access to the current system, including all their current privileges.”

Questions ?





IBM

Trust Service Composed of Module Chains

