



IBM Software Group | Tivoli Software

# Federated Identity Management

## Federated Single Sign-On and Web Services Security



Managed Beta Program



Jon Harry  
*Jon P Harry/UK/IBM*



© IBM Corporation

IBM Software Group | Tivoli Software | **betaWorks** 

# Identity Federation

© IBM Corporation

**ON DEMAND BUSINESS**

2

IBM Software Group | Tivoli Software | **betaWorks** 

## Problem: Ineffective Identity Management




**Partners**  
**Suppliers**  
**Business Clients**  
**Distributors, Brokers**  
**Outsourced Providers**

1. Today, companies have no way to “trust” identities belonging to their partners, suppliers, contracts and their outsourcers.
2. Lack of trust means companies end-up creating online identities (and passwords) for all users
3. This approach is very costly, inefficient & creates user frustration with multiple accounts and registrations for each Web Site.

© IBM Corporation

**ON DEMAND BUSINESS**

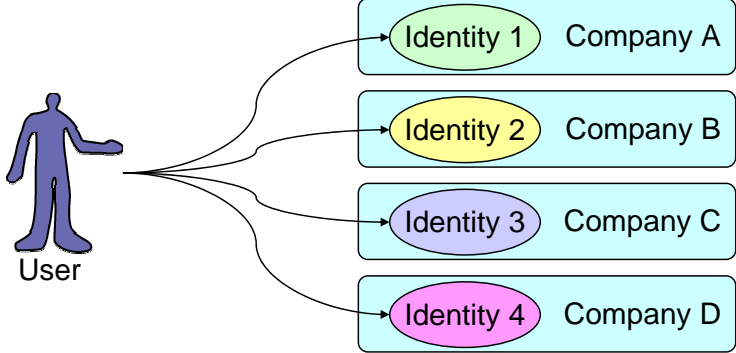
3

IBM Software Group | Tivoli Software | **betaWorks** 

## The multiple identity problem...

◆ **A typical user has a number of distinct identities**


- Each one is associated with duplicate identity information
  - Personal information and authentication information




The diagram illustrates a user (represented by a blue silhouette) connected to four distinct identities. Each identity is represented by a colored oval (green, yellow, purple, and pink) inside a light blue rounded rectangle, with an arrow pointing from the user to each identity. The identities are labeled as Identity 1 (Company A), Identity 2 (Company B), Identity 3 (Company C), and Identity 4 (Company D).

**This is frustrating for the user and EXPENSIVE for the companies**

© IBM Corporation

4 


IBM Software Group | Tivoli Software | **betaWorks** 

## What is Identity Federation?

- ◆ The act or process of linking otherwise distinct identities managed by independent parties.
  - e.g. Link multiple virtual identities of a single real user

The diagram illustrates the concept of identity federation. On the left, a blue silhouette of a person is labeled 'User'. A thick pink vertical bar represents the user's federated identity. Four horizontal boxes are stacked on this bar, each representing a different service provider. The top box is light blue and labeled 'Identity' and 'Company A', with the word 'Identity Provider' to its right. The three boxes below are light grey and each labeled 'Linked Account' and 'Company B', 'Company C', and 'Company D' respectively, with the words 'Service Providers' to their right. Arrows point from the 'User' to each of the four boxes. A double-headed vertical arrow is positioned to the right of the three 'Linked Account' boxes, indicating interaction between the service providers.

© IBM Corporation

5 

## What is a Federation?

### ◆ From a business point of view:

- Federation is the set of business agreements, technology agreements and policies that enable companies to optimally pursue business automation goals that best align with their business model, IT policy, security, privacy and governance goals and requirements

### ◆ From a technology point of view:

- Federation requires (and becomes) the trust infrastructure over which business federations are implemented
- Federation technology enables companies to securely link (join or extend) their IT infrastructures with those of their partners rather than create and manage redundant identity & security infrastructure

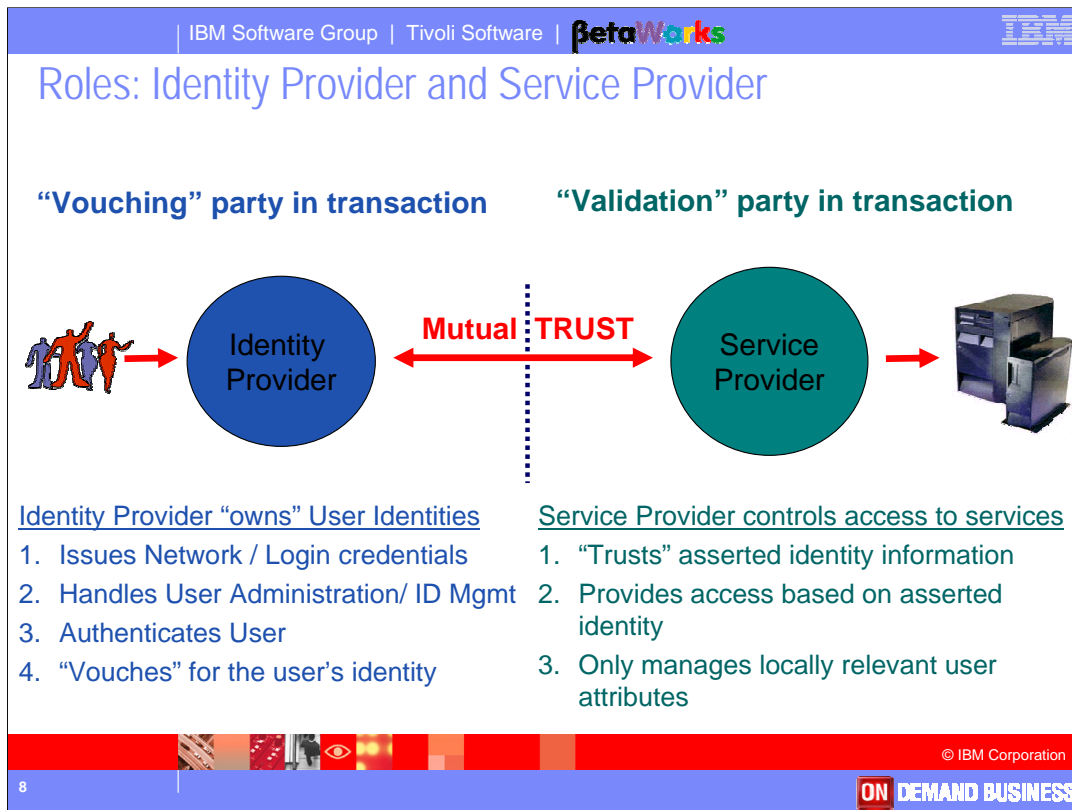
## What is Federated Identity Management?

### ◆ Federated Identity Management

- Identity lifecycle management
  - Provisioning of users and linking of user identities
- Identity mapping across partners
  - Single-sign-on
  - User information exchange
- Secure application interaction
  - Using web services technology

### ◆ Federation requires a trust infrastructure

- Enables the on-line equivalent of real-world business relationships



Within a federation, organizations play one or both of two roles.

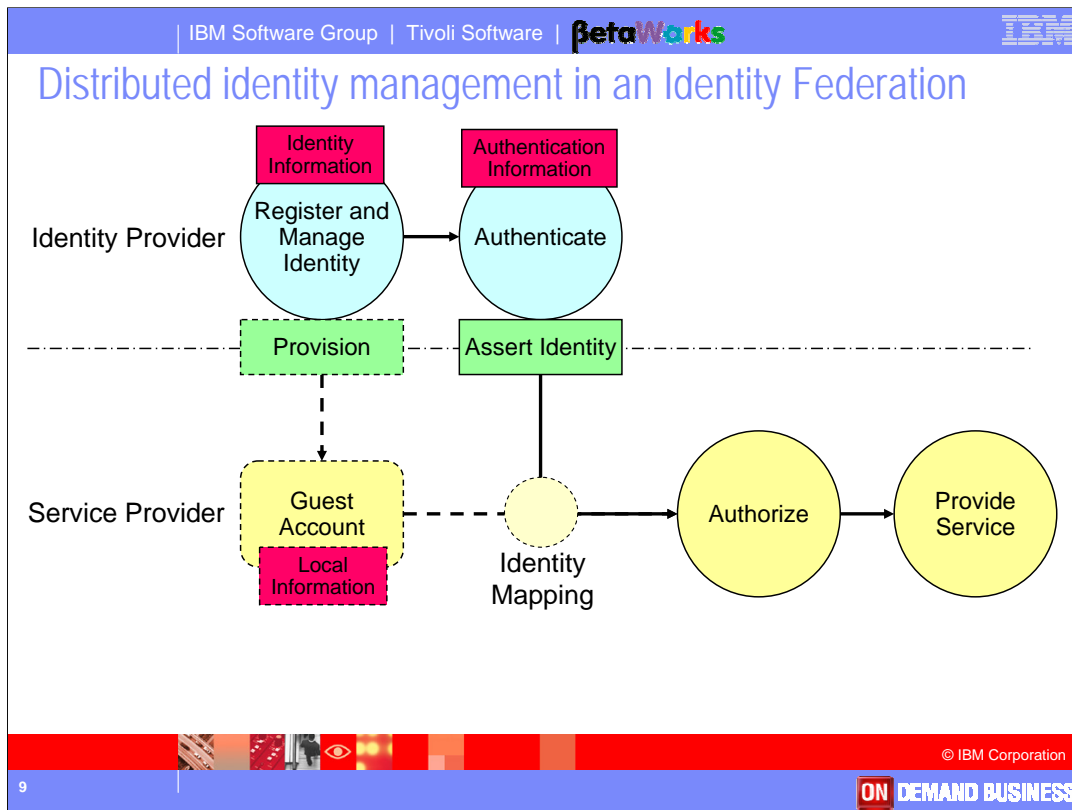
### Identity Provider:

The identity provider (IdP) is the authoritative site responsible for authenticating an end user and asserting an identity for that user in a trusted fashion to trusted partners. The identity provider is responsible for account creation, provisioning, password management, and general account management and also acts as a collection point or client to trusted identity providers.

### Service Provider:

Those partners who offer services but do not act as identity providers are known as service providers. The service provider (SP) relies on the IdP to assert information about a user, leaving the SP to manage only those user attributes that are relevant to the SP.





This slide shows how responsibility for a user's identity lifecycle and session lifecycle are split between Identity Providers and Service Providers in a federation.

The four responsibilities are "Manage Identity", "Authenticate", "Authorize" and "Provide Service".

Without a federation each partner would be responsible for all four parts. With a federation, each is only responsible for two.

If there are many partners in the federation the benefit is multiplied.

Note that Provisioning of guest accounts is optional. If the Service Provider doesn't need to maintain information about each user then an individual guest account for each user may not be required.

## FIM: Why is this important?

### ◆ Lower Identity Management costs


- Only Identity Providers have to manage authentication information
- Service Providers only manage information relevant to their service

### ◆ Enables “Service Oriented Architecture”

- Services can be offered (securely) to all end users of the federation
  - Good for both Identity Providers and Service Providers
- Simplify user experience with Single Sign On


### ◆ Automation of Provisioning between companies


- Provisioning of user identities, entitlements and business services
- Current manual method is costly and time consuming

IBM Software Group | Tivoli Software | **betaWorks** 

## Benefits of Identity Federation

- ◆ **Users**
  - Only one place to update Personal Information
  - Only one authentication required
  
- ◆ **Identity Providers**
  - Maintain a close relationship with the user
  - Offer 3rd party services seamlessly
  
- ◆ **Service Providers**
  - Reduced/removed need for local identity management
    - SP only has to manage locally relevant information about users
  - Easier access to all users in the federation

 © IBM Corporation

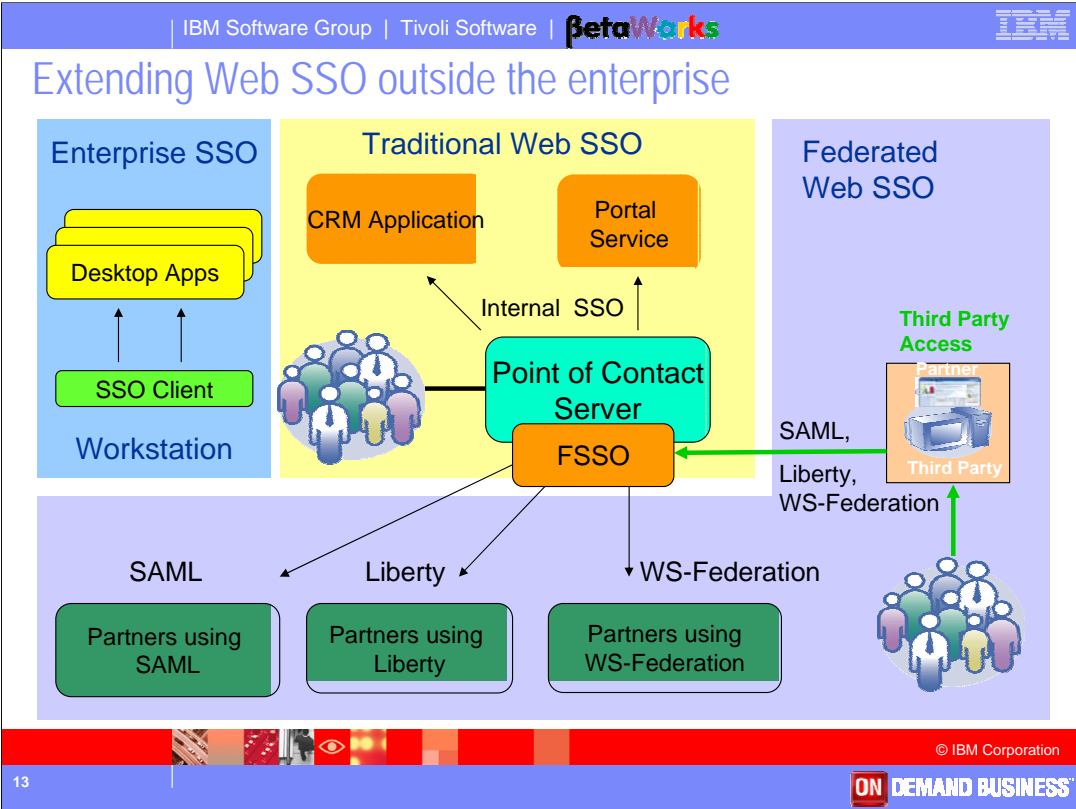
11 


IBM Software Group | Tivoli Software | **betaWorks** 

## Federated Single Sign-On

© IBM Corporation


12 




IBM Software Group | Tivoli Software | **betaWorks** 

## "Federation" SSO Efforts

- ◆ **SAML**
  - Provides a standard format for asserting identity information
  - Also defines a number of SSO protocols (SAML 1.0, 1.1, 2.0)
  
- ◆ **WS-Federation**
  - Part of the overall "Web Services Security Roadmap"
  - Describes how to manage trust across trust domains
  - Defines protocols to simplify single-sign-on and session management in Passive and Active client environments
  
- ◆ **Liberty Alliance**
  - Defines a set of specifications for identity federation
  - Define SSO protocol and protocols for management of aliases
  - Liberty ID-FF 1.1 & 1.2 are based on SAML 1.x

 © IBM Corporation

14 

IBM Software Group | Tivoli Software | **betaWorks** 

# Web Services Security

© IBM Corporation

15 



Web Services are widely perceived to be the next evolutionary step in the use of the Internet. Web Services will enable the creation of a new breed of end-user applications that are not restricted to today's model of a "web application" that must use HTML talking to a web server.

Instead users will use "active clients" that exchange XML messages with multiple applications in parallel to create a significantly enhanced user experience.

The Federated Single Sign-on capability of FIM offers great advantages in the area of identity management – allowing the separation of service offerings from user management. This will create an enhanced user experience at reduce cost for today's standard web-based applications.

The potential for the next generation of web service based applications can only be realized, however, if web services are secure. Further, the security infrastructure used by these applications must be flexible and effectively managed.

For this reason FIM's Web Services Security Management is an essential enabler of the new "active client" applications that build upon the trust relations of a federation - allowing trust-worthy application-to-application interaction across federated identity and service providers.

These applications will integrate many distributed services to create a higher-value, more effective user experience than is possible with today's HTML/HTTP technology.



IBM Software Group | Tivoli Software | **betaWorks** 

## SOAP Security Only a Building Block

- ◆ **SOAP Security defines SOAP elements for:**
  - Security Tokens → message authentication
  - Signature → message integrity
  - Encryption → message privacy
  
- ◆ **These fulfill the requirement for “message-based security” for SOAP, but....**
  - WS-Security does not meet the need for Web Service Security *Management*
  
- ◆ **WS Security Management requires a holistic approach to**
  - Management of Partners
  - Management of Applications
  - Management of Trust Relationships

© IBM Corporation

17 

The SOAP specification does not address security requirements for SOAP messages. From SOAP 1.1:

### 8.0 Security Considerations

Not described in this document are methods for integrity and privacy protection. Such issues will be addressed more fully in a future version(s) of this document

It is possible to use the security capabilities of the transport protocol that carries the SOAP message, but this approach has the drawback that multiple-hop transport paths may introduce ambiguity of origin and unacceptable “gaps” in the security. More importantly, the application-to-application nature of web services require *message-level* facilities for management that cannot be achieved using only transport protocol facilities.

The OASIS standard, “Web Services Security – SOAP Message Security” describes how to use SOAP Header elements that encrypt and sign the SOAP Body and include “security tokens”. These elements allow a SOAP message to be “self securing”. That is, the SOAP message can be transported in any manner and the message origin, integrity and privacy are not affected because these are properties of the message itself.

These capabilities of SOAP Security are vital, but do not in themselves provide any security *management*. For example, it is important to know that the received message has not been changed and that the message came from entity-X. But what rights does the client have in the local environment?.

Also, the identity in the SOAP Security token may have a different representation in the local environment – requiring an identity mapping capability.. Is the client identity *authorized* to access the target web service? Are local or remote attributes of the client identity required to make an authorization decision?

WS-Security does, however, provide the elements that can be used as building blocks in the overall management solution.

IBM Software Group | Tivoli Software | **betaWorks** 

## Web Services Security Management : Requirements

- ◆ **Web services security *management* must provide:**
  - Token Management
  - Identity & Attribute Management
  - Authorization Management
- ◆ **Management is required on both**
  - the client (requestor) side, and
  - the web service (provider) side
- ◆ **Solutions must also provide**
  - Interoperability with multiple service endpoints (J2EE, .Net, ...)
  - Interoperability with multiple gateways/firewalls
  - Audit Management

© IBM Corporation

18 

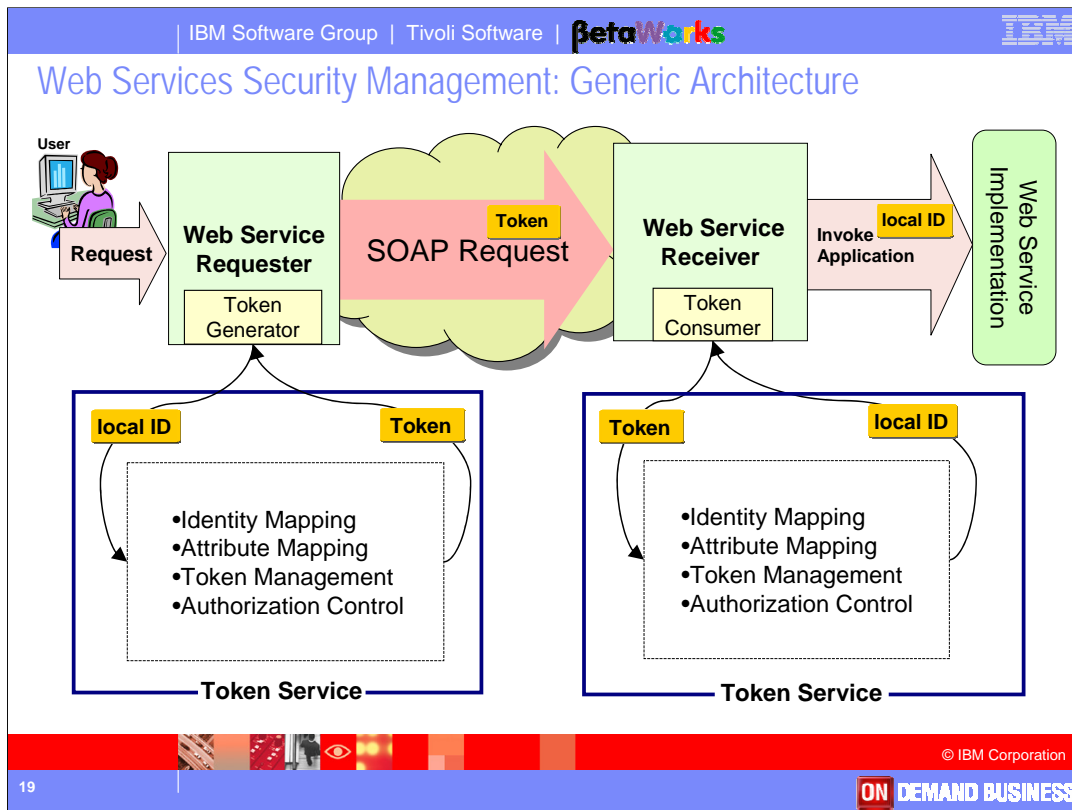
WS-Security:SOAP Message Security is an extendable framework that allows for many types of *security tokens* that identify the origin of the message. As SOAP security evolves new Security Tokens will be created. It is important that the management infrastructure be able to easily accommodate new types of security tokens without requiring changes to applications.

For the local management system to make relevant decisions about web service access, the user of the web service must be represented by a local credential. Only a local credential will contain the locally defined values for users, groups, security attributes that are relevant to the local security policy. It may not be possible (or efficient), of course, for every possible web service client to have a local identity. An “identity mapping” capability is required to allow for such clients to obtain a local credential that is meaningful to the local access policy.

An enterprise may deploy web services onto a number of vendor platforms. Two of the most important today are J2EE and .NET. The management infrastructure must provide a solution for BOTH of these web service platforms.


Many applications will require attributes about the user. Some of these attributes will be provided as part of the request (remote attributes) and others will be part of the local identity (local attributes). The token exchange mechanism should allow for the mapping of remote attributes and the addition of locally defined attributes and the resultant security token must be available to the target web service application.

There are, of course, other security requirements not covered by this list, and individual customers/architectures will have ones unique to them. For example, Key Management is required is required for the keys that encrypt and sign the SOAP messages. The FIM Administration Console provides key import and export capabilities, but the PKI system that creates the keys & certificates is another subject.




This diagram shows a user at company A, accessing a resource at company B via a web service request.

1. User at Company-A invokes a web service using her local ID.
2. Web services functionality at Company-A side may do identity/attribute mapping as part of creating a security token to be added to the Request
3. The Request is sent across the Internet to Company B. A number of different technologies can be used to provide message privacy & integrity – SSL, SOAP-Security, VPN tunnel, etc.)
4. The initial point of contact at Company B could be an XML/WS Firewall or Gateway or similar. The general requirement for this node is to “normalize” and authorize inbound requests such that they can be processed in the local environment. Its functionality may include:
  - Mapping of identity claimed in incoming token to a locally valid id
  - Mapping of attributes claimed in incoming token to local valid attributes such as groups/roles
  - Exchange of presented token for a local valid token format
  - Invocation of back end app as a web service or as a local app (eg J2EE)

IBM Software Group | Tivoli Software | **betaWorks** 

# Secure Token Service

© IBM Corporation

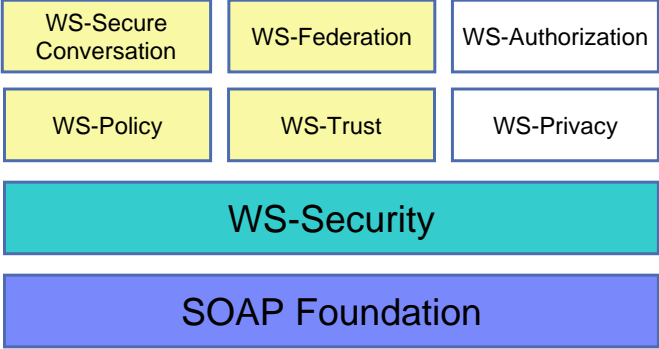
20 

## WS-Trust : Overview

- ◆ **WS-Trust defines mechanism for:**
  - “...security token exchange to enable the issuance and dissemination of credentials within different trust domains”
  
- ◆ **Defines the **Security Token Service** which can:**
  - Validate security tokens
  - Exchange security tokens
    - exchange one type of token for another type
  
- ◆ **Defines how to broker trust relationships**
  - Some trust relationship must exist before the fact

IBM Software Group | Tivoli Software | **betaWorks** 

## Web Services Security Roadmap



WS-Secure Conversation	WS-Federation	WS-Authorization
WS-Policy	WS-Trust	WS-Privacy

**WS-Security**

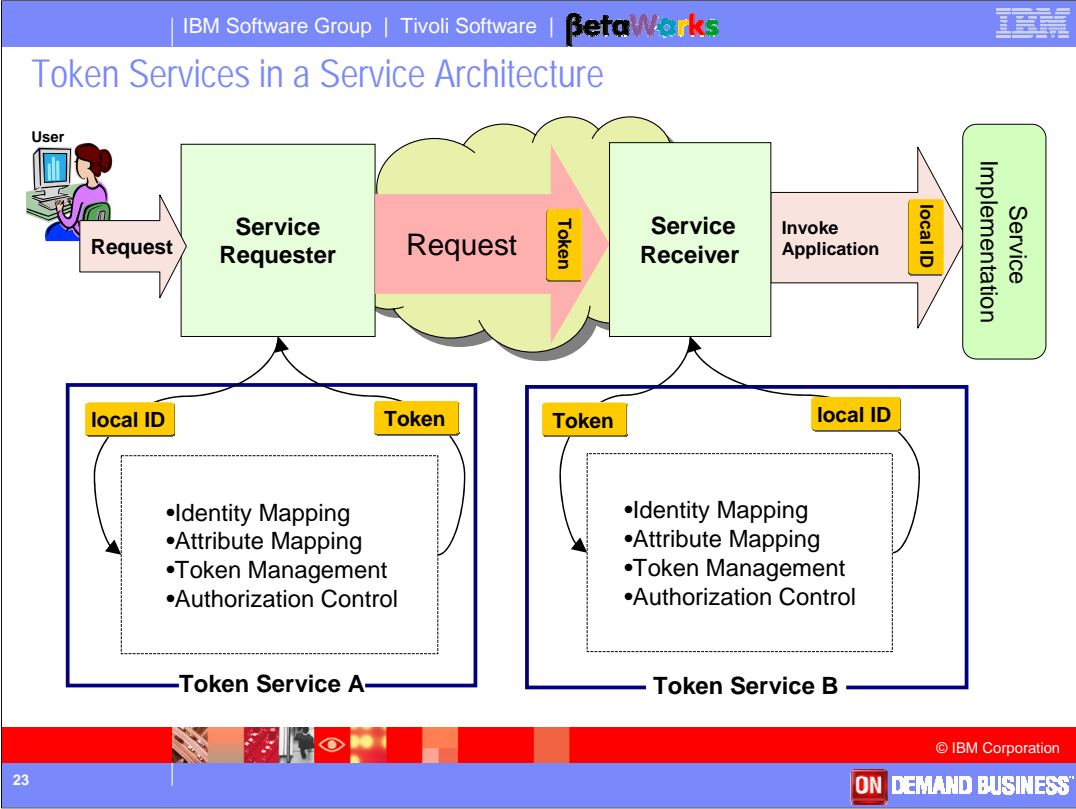
**SOAP Foundation**

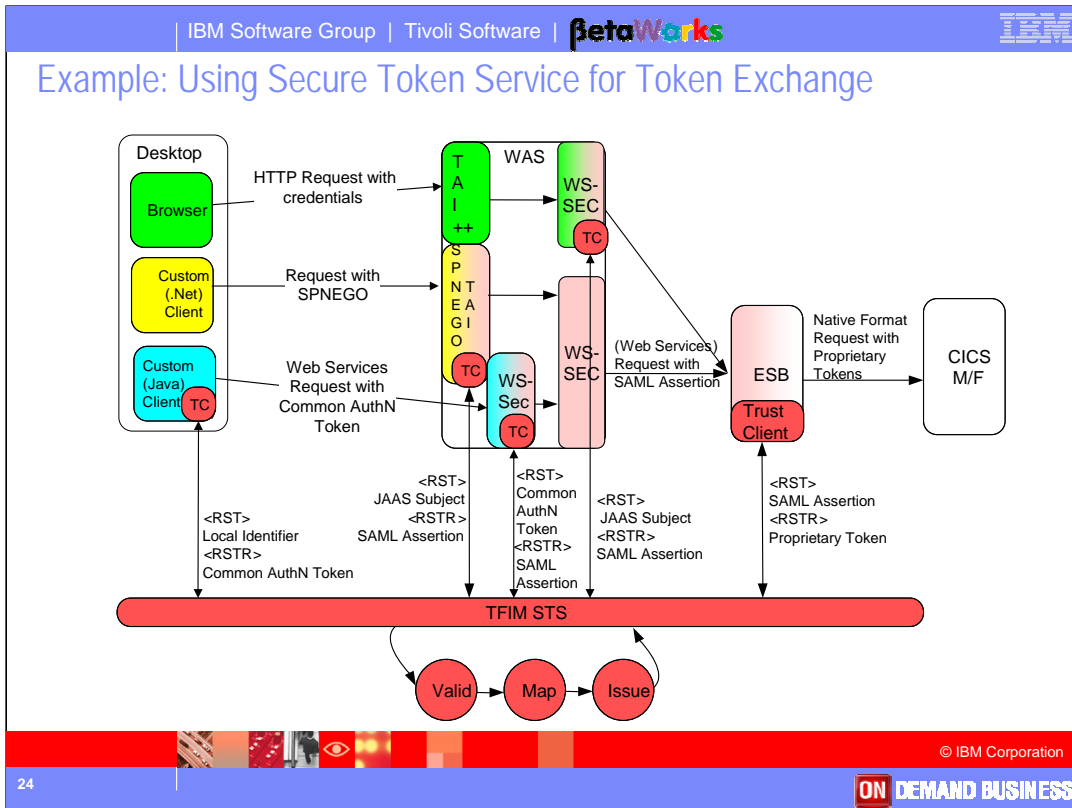
Web services zone page:  
<http://www.ibm.com/developerworks/webservices/>

© IBM Corporation

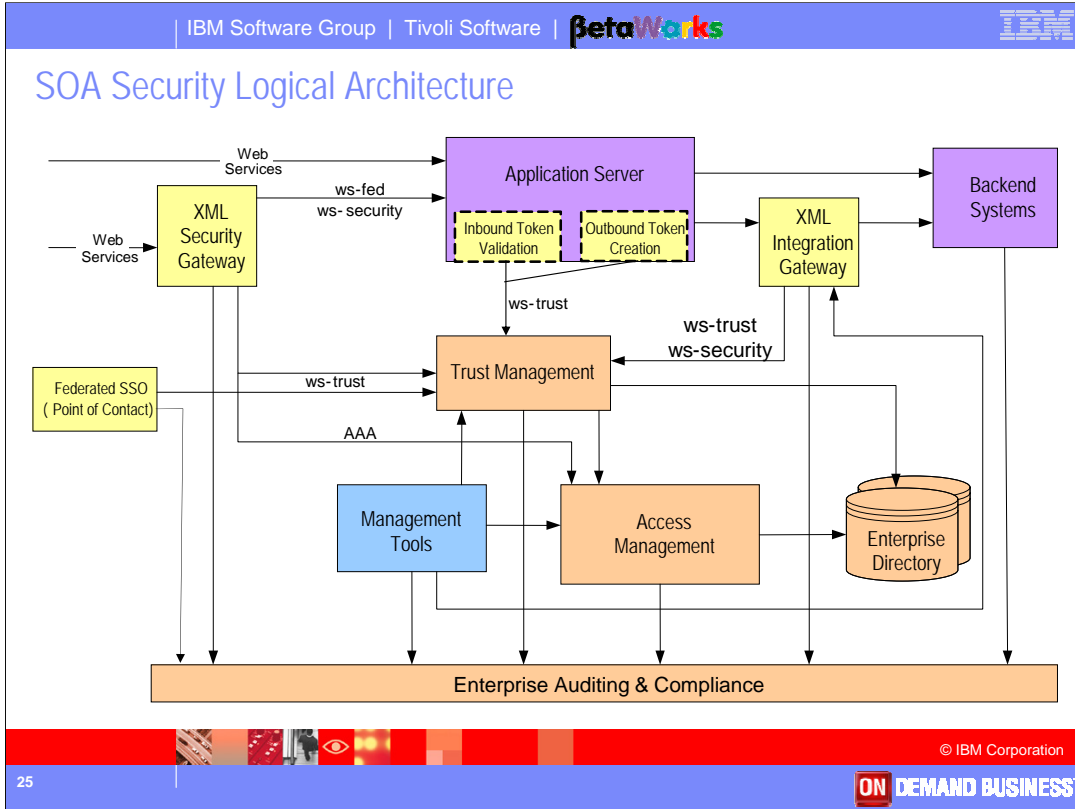
**ON DEMAND BUSINESS**

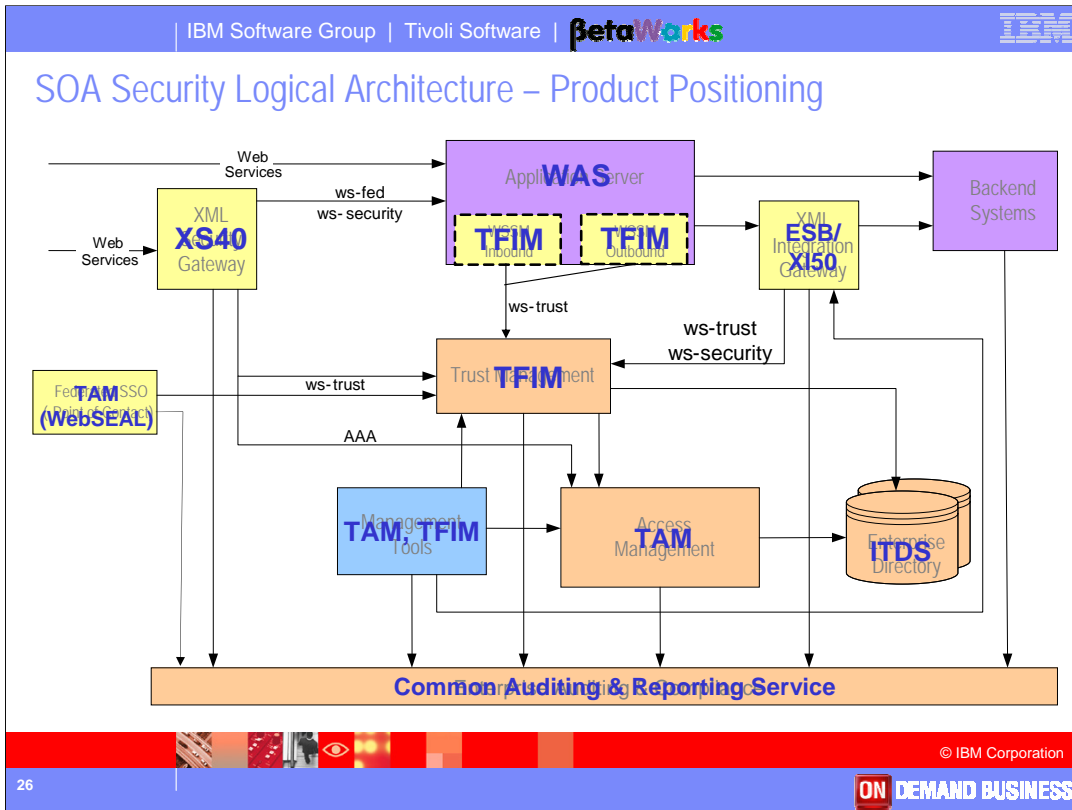
22












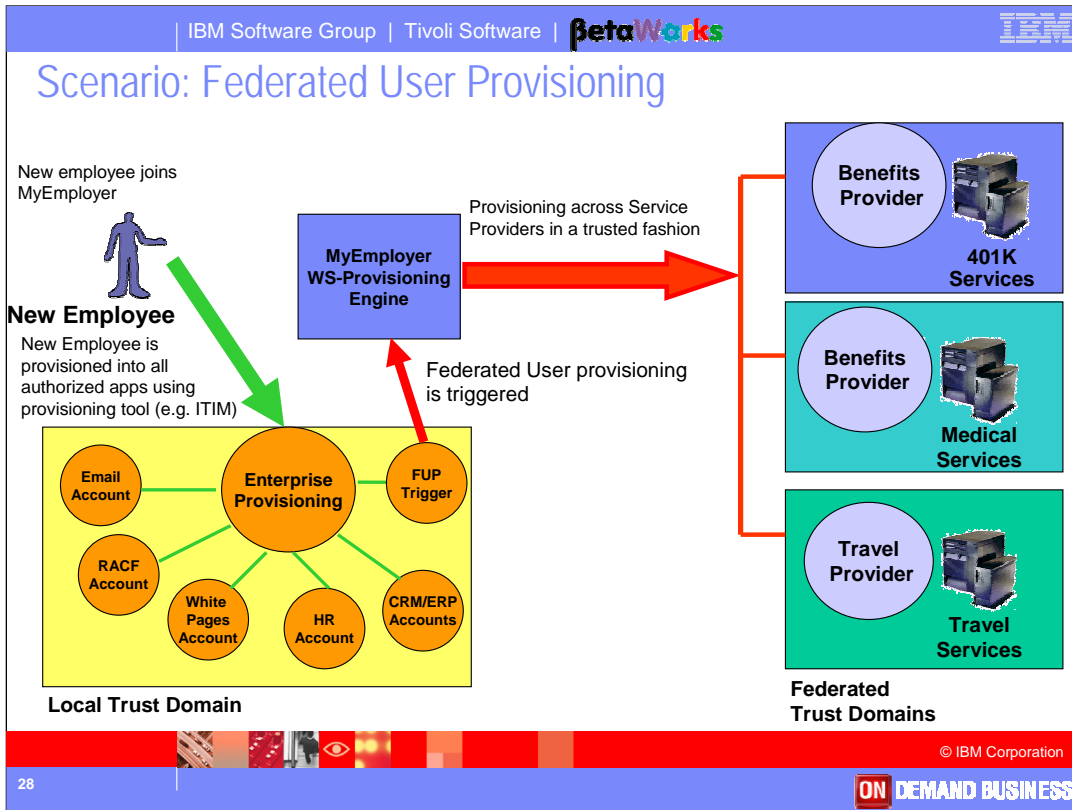
IBM Software Group | Tivoli Software | **betaWorks** 


# Federated Provisioning

© IBM Corporation

**ON DEMAND BUSINESS**


27




IBM Software Group | Tivoli Software | **betaWorks** 

## Federated Provisioning - Value

- ◆ **User Management link from Identity to Service Provider**
  - add/remove authorized users to Service Providers
  - user entitlements can be sent to Service Provider
- ◆ **Allows Service Providers to establish local accounts**
  - middleware, registries, applications
    - required to provide the service
  - local accounts used to maintain service-specific attributes, e.g.
    - user preferences
    - user consent to data handling, disclosure, etc
- ◆ **Could provide remote-to-local account linkage via aliases**
  - eliminates need for account *federation* step during SSO
- ◆ **Allows automated updates for:**
  - user entitlements
  - de-provisioning

 © IBM Corporation

29 

IBM Software Group | Tivoli Software | **betaWorks** 

## IBM Tivoli Federated Identity Manager (TFIM)

- ◆ **Trust Service**
  - Manages trust/identity infrastructure
    - Token Validation and Exchange
    - Identity and Attribute Mapping
    - Key Management
- ◆ **Federated Single Sign-On Service**
  - Provides implementation of Web SSO protocols and profiles
  - Manages protocol configuration and partner definitions
  - Uses Trust Service for required token/identity management
- ◆ **Web Services Security Management (WSSM)**
  - Web Security plug-ins for WebSphere Application Server
  - Allows WebSphere to use the Trust Service for token management
- ◆ **Federated Provisioning**
  - Implementation of WS-Provisioning
  - Enables cross-enterprise provisioning

30  © IBM Corporation **ON DEMAND BUSINESS**