Federated Identity Management: Design and Architecture of Federation Models – Customer experiences

Glen Gooding
Senior Consulting IT Specialist
IBM Security
Agenda

• SOA Overview
• Applying Identity to a SOA Scenario (using TFIM)
  ▪ Approaching SOA from the People entry point
  ▪ Adding Service Orientation and Reuse
  ▪ Adding Modeling and Flexible Service Connectivity
• Real life customer experiences
• Summary
Business Challenges

Growth and Innovation
- Mergers & Acquisitions
- Business Process Transformation
- Virtual Enterprises / Collaborative Partnerships
- Integration and Insight to better serve customers

Competition
- Low cost Providers
- Software-As-Service

Cost
- Cost and Efficiency of Service Delivery
- Technology Integration
- Outsourcing

Governance and Compliance
- Management of People, Process, Information and Technology
- Standards and Regulations

The Goal: Strategic Flexibility Through SOA

78% of CEOs believe integrating business and technology is fundamental for innovation
Analysts & Customers Agree: SOA Critical to Innovation

The IBM and GenXus SOA-based solution has made our product more innovative, expanded our market and made us more competitive will let us grow our business significantly in the years to come."

"SOA is the heart of the next wave of innovation. The leaders that do this well are able to rapidly change ..."

"SOA is critical for ... executing the on-demand vision and in preparing ... for the incremental changes ... over time. Companies ... make better decisions."

Tivoli Now!
What is SOA anyway…..?

... a service?

A repeatable business task – e.g., check customer credit; open new account

... service orientation?

A way of integrating your business as linked services

... service oriented architecture (SOA)?

An IT architectural style that supports service orientation

... a composite application?

A set of related & integrated services that support a business process built on an SOA
A programming model complete with standards, tools, methods and technologies such as Web services.

An architectural style which requires a service provider, requestor and a service description. It addresses characteristics such as loose coupling, reuse and simple and composite implementations.

Capabilities that a business wants to expose as a set of services to clients and partner organizations.

A set of agreements among service requestors and service providers that specify the quality of service and identify key business and IT metrics.
SOA begins by working within your existing environment

Business Centric and IT focused Entry Points to SOA

Create & Reuse Services

People
Process
Information
Partner Connections
New Services
Existing Applications

Connectivity

Tivoli Now!
Providing the technical underpinnings for Business Centric SOA

**Business Innovation & Optimization Services**
Facilitates better decision-making with real-time business information

**Interaction Services**
Enables collaboration between people, process & information

**Process Services**
Orchestrates and automates business processes

**Information Services**
Manages diverse data and content in a unified manner

**Partner Services**
Connects with trading partners

**Business App Services**
Builds on a robust, scaleable, and secure services environment

**Access Services**
Facilitates interactions with existing information and application assets

**Infrastructure Services**
Optimizes throughput, availability and performance

**ESB**
Facilitates communication between services

**Integrated environment**
For design and creation of solution assets

**Monitor, manage and secure services, applications & resources**

**Tivoli Now!**
Providing the technical underpinnings for Business Centric SOA

SOA is Identity Driven!!

Tivoli Now!
The Challenge: Bringing People, Process, and Information Together for True SOA Value
The objective of TFIM is to provide Security and Identity related services for a SOA environment

**Current Focus Areas:**

- Single Sign-On (SSO)
  - Browser-based Federated SSO
  - Identity Mediation for Web Services
    - Identity mapping between domains
    - Identity exchange format mapping between domains
    - Interface to authorization services

- Identity Mediation Policy Management
  - WS-Trust based Security Token Service (STS)
    - Integrated management of user identity and identity exchange format requirements for service requestors and service providers.
Scenario Development – Base Scenario

- Objective:
  - Progressively develop a scenario that illustrates the application of Tivoli Security middleware in solving identity related aspects of SOA-based integration.

- Base Scenario
  - A financial services company is comprised of a collection of mostly independent business units, some of which were added via acquisitions.
  - The company is looking at the following initiatives:
    - Outsourcing of selected business processes to outside firms
    - Improve flexibility and agility of its IT operations to match the rapidly evolving needs of the business and its markets.
    - Improve the user experience for its customers and partners by providing a single user interface that combines the services offered by the company.
  - The scenario could readily be applied to a wide range of vertical industry segments.
  - Most of the incremental components added to the scenario could be done in isolation.
    - There is no requirement to follow the same functionality evolution used in the scenario.
      - For example, the Federated SSO, Reuse and Connectivity related features could equally be applied to a non-portal environment.
People Entry Point

1. Introduce a portal to provide a single user interface to customers and partners.
2. Allow large customers and partners to leverage the authentication done by their own organizations to access the company’s portal.
3. Allow internal business units and outsource providers to provide remote portlets for inclusion in the company’s portal.
Reuse
4. In order to satisfy governance requirements, move to an integration architecture where mainframe systems are accessed using individual user ids.
5. Increase the range of services available in the portal by adopting a service orientation for existing applications and connecting services together to create new user-driven business transactions.

Connectivity
6. Further improve the capability of the company to rapidly respond to market pressures by moving to a business process management based architecture that utilizes Business Process Modeling and an Enterprise Service Bus.
Value
Improve people productivity by aggregating views that deliver information and interaction in the context of a business process

Hanover transacts business 75% faster with deployed SOA portlets

Start with
Build a view of a key business process by integrating information in front of people to improve decision making

Next steps
Manage performance more tightly with alert-driven dashboards tied to processes
As a first step towards SOA, the company introduces a portal to provide a single user interface to customers and partners.

- This portal will provide “integration at the glass” and single authentication for the company’s applications.
- Dealing with user identity is obviously a critical success factor for this type of integration.
- Authentication requirements in the scenario:
  - Multi-factor and reverse authentication for external customers and partners
  - Integrated desktop SSO for internal users
## Scenario – Product Mapping for the People Entry Point

### Authentication / Single Sign-On
- Strong/Reverse Authentication Framework: √
- SSO from browser to web applications: √
- SSO to web applications from portlets: √
- Credential storage and access for use in SSO: √, √
- Desktop SSO to browser (via SPNEGO): √

### Authorization
- URL-level Authorization: √
- Authorization of Portal resources: √, √
- Ability to restrict access based on strength of authentication: √

### Secure Architecture
- Secure bastion in the DMZ: √

### Audit
- Audit Logging & Reporting: √

**Legend:**
- √ Fully supported
- √ Supported, but not preferred option in most cases
Scenario – Architecture for the People Entry Point

**Internal Users**
- Desktop SSO
- SSO

**External Users**
- Strong Authentication
- TAM WebSEAL

**TAM WebSEAL**
- Audit Reports
- WAS
- Portal Svr
- Portlet
- SSO via userid:pwd

**WAS**
- SSO
- TAI++

**LDAP**
- TAM GSO Lockbox

**Web Application**
- SSO
- Strong Authentication Partner (eg PassMark)

**CARS Audit Svc**
Scenario – Adding Federated SSO Access

To help reduce account management costs for external users and to improve the user experience for those users, the company introduces functionality to allow large corporate customers and partners to leverage the authentication done by their own organizations to access the company’s portal.

- For large customers, all users will have an individual user identity in the company portal.
  - Note that the identity used to authenticate to the external system need not be the same as that for the company portal.
- For large partners, a role based scheme will be used where individual partner user identities are mapped to role based identities for access to the company’s portal.
  - This role mapping will be based on additional data about the user provided by the partner organization.
- In both cases, the user’s individual email address (as specified by their organization) will be written to audit logs to identify the user performing the operation.

In order to be able to respond to the needs of the business and allow technical linkage to be made with a wide variety of partners, whose infrastructures comprise products from a diverse set of vendors, this Federated Single Sign-On interaction will be standards based and support all major industry standards.

An extension to this use case that can be contained within the same architecture is to allow users of the company portal to access related external systems provided by partners and outsource providers without needing to reauthenticate.
### Scenario – Product Mapping for Adding Federated SSO

<table>
<thead>
<tr>
<th>Feature</th>
<th>TAM</th>
<th>TFIM</th>
<th>WP</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Authentication / Single Sign-On</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Federated SSO into Company web applications</td>
<td>✓</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Federated SSO to external web applications</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Support for 1-1 and role based identity mappings</td>
<td>✓</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td><strong>Authorization</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ability to restrict access based on strength of authentication</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td><strong>Audit</strong></td>
<td></td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Audit Logging &amp; Reporting</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
</tbody>
</table>

**Legend:**
- ✓ Fully supported
- ✓ Supported, but not preferred option in most cases

**Supported Federated SSO Protocols:**
- SAML 1.0 / 1.1 / 2.0
- Liberty ID-FF 1.1 / 1.2
- WS-Federation
Scenario – Architecture for Adding Federated SSO

Browser

Outsource Provider

HTTP(S)

TAM WebSEAL

Web Application

HTTP(S)

TFIM Federated SSO Service

WAS

Portal Svr

HTTP(S)

Federated SSO Service

Web Application

SAML

WS-Federation

Liberty ID-FF

Audit Reports

CARS Audit Svc
Scenario – Adding Remote Portlets to the Company Portal

- To help make access to outsourced and partner applications transparent to users of the company portal, other providers will provide remote portlets for inclusion in the company’s portal.
  - Depending on the nature of the application, either individual user identities or role based identities will be passed to the remote portlet provider.
- To help maintain a loose coupling between the applications in the (mostly independent) internal business units and the company portal, the ability to provide remote portlets will be extended to internal systems.
  - Note that given the relatively independent nature of the business units, a particular user may have different identities in applications from different business units.
- In order to satisfy regulatory requirements, any mapping between individual identities and/or role based mappings must be logged in audit trails.
- In line with common industry practices, user identity will be exchanged with internal business units, partners and outsource providers via SAML assertions in WS-Security headers of the web services messages containing the remote portlet (WSRP) requests.
### Scenario – Product Mapping for Adding Remote Portlets

<table>
<thead>
<tr>
<th><strong>Authentication / Single Sign-On</strong></th>
<th>TAM</th>
<th>TFIM</th>
<th>DP</th>
<th>WP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Support for WS-Security headers in WSRP messages</td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Support for adding SAML assertions to WS-Security headers</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Support for 1-1 and role based identity mappings</td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Authorization</strong></th>
<th>TAM</th>
<th>TFIM</th>
<th>DP</th>
<th>WP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access control for web service endpoints</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Secure Architecture</strong></th>
<th>TAM</th>
<th>TFIM</th>
<th>DP</th>
<th>WP</th>
</tr>
</thead>
<tbody>
<tr>
<td>XML Firewall in DMZ</td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Audit</strong></th>
<th>TAM</th>
<th>TFIM</th>
<th>DP</th>
<th>WP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Audit Logging &amp; Reporting</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
</tbody>
</table>

**Legend:** ✓ Fully supported   ✓ Supported, but not preferred option in most cases
Scenario – Architecture for Adding Remote Portlets

Outsource Provider or Partner

Audit Reports

Tivoli Now!
SOA Entry Point to Creating & Reusing Services:

Create Flexible, Service-based Business Applications

Value
- Cut cost, reduce cycle times and expand access to core applications through reuse
- It is 5X less expensive to re-use existing applications than to write new applications*

Start with
- Identify high-value existing IT assets and service-enable them for reuse
- Create new services for today's business needs and future reuse
- Registry/repository to facilitate centralized access and control of reusable services

“With reuse, solving the next business problem can be done more quickly and efficiently.”

- Amy Wohl

* Software Productivity Research (SPR)
In order to increase the range of services available in the company portal, the company wants to add the ability to directly invoke several operations that are currently implemented as CICS transactions on their mainframe.

- Corporate security policies forbid the storage of mainframe passwords in an unencrypted or reversibly encrypted form, so authentication to the mainframe will be achieved via RACF passtickets.

- In line with new regulatory requirements, access to the mainframe will be done using individual user identities; the integration practice used in the past where application userids and passwords were used for mainframe authentication is no longer a viable option.

- In order to satisfy regulatory requirements, any mapping between individual identities and/or role based mappings must be logged in audit trails.
## Scenario – Product Mapping for Adding Mainframe Reuse

<table>
<thead>
<tr>
<th>Service Level Single Sign-On</th>
<th>TAM</th>
<th>TFIM</th>
<th>WP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Generation of RACF passtickets</td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Support for 1-1 and role based identity mappings</td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Support for using passtickets with web services</td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Support for using passtickets with JCA</td>
<td></td>
<td>(coming soon)</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Authorization</th>
<th>TAM</th>
<th>TFIM</th>
<th>WP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Course grained authorization for access to CICS</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Audit</th>
<th>TAM</th>
<th>TFIM</th>
<th>WP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Audit Logging &amp; Reporting</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
</tbody>
</table>

**Legend:**
- ✓ Fully supported
- ✓ Supported, but not preferred option in most cases

---

**Tivoli Now!**
Scenario – Architecture for Adding Mainframe Reuse

TFIM
- Authorization, identity mapping, audit logging, passticket generation
- May run on distributed or z/OS platforms
- Protocol between WAS & TFIM is defined by the WS-Trust specification

LDAP Server
- May run on distributed or z/OS platforms
In order to increase the range of services available in the company portal, the company starts to adopt a service orientation for existing applications and will eventually connect these services together to create new user-driven business transactions.

- In the first instance, the company wants to access several services available in SAP via web services from the company portal.
  - The user identities used in their SAP implementation do not match the identities used in the corporate portal.
- The company has also written web service wrappers several custom applications they had previously developed.
  - These applications run on either WebSphere Application Server or Microsoft .Net application servers.
## Scenario – Product Mapping for Adding Service Orientation

<table>
<thead>
<tr>
<th>Service Level Single Sign-On</th>
<th>TAM</th>
<th>TFIM</th>
<th>WP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Support for using SAML assertions with WebSphere Application Server</td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Support for using .Net Kerberos Tickets with WebSphere Application Server</td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Support for 1-1 and role based identity mappings</td>
<td></td>
<td>✓</td>
<td></td>
</tr>
</tbody>
</table>

## Authorization

<table>
<thead>
<tr>
<th>Course grained authorization for service access</th>
<th>TAM</th>
<th>TFIM</th>
<th>WP</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
</tbody>
</table>

## Audit

<table>
<thead>
<tr>
<th>Audit Logging &amp; Reporting</th>
<th>TAM</th>
<th>TFIM</th>
<th>WP</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
</tbody>
</table>

**Legend:** ✓ Fully supported, ✓ Supported, but not preferred option in most cases
**Underlying Connectivity to Support Business-centric SOA**

**Value**
- Deliver services through new business channels with any-to-any connectivity for a secure, consistent user experience
- Savings of 2X-4X over custom-built integration or FTP*

**Start with**
- Messaging backbone leveraging messaging and web services protocols as the foundation for SOA connectivity
- Enable mediated exchange between services, by leveraging an ESB
- Specialized devices to provide scalable web services connectivity in an alternate form factor

*Software Strategies
“Enterprise Integration Challenge” 2005
To further improve their capability to rapidly respond to market pressures the company decides to adopt a focus on business process management and fully embraces a Service Oriented Architecture to help attain their goals.

- The company adopts a full SOA lifecycle approach and as a first step adds Business Process Modeling and Enterprise Service Bus technologies to their architecture.
Today Tivoli Security’s support for an ESB centric architecture is focused on providing token and identity mediation services for Datapower SOA Appliances acting in an ESB onload/offload role.

<table>
<thead>
<tr>
<th>Service Level Single Sign-On</th>
<th>TAM</th>
<th>TFIM</th>
<th>DP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identity/Token mediation services for Datapower SOA appliances</td>
<td></td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>Identity/Token mediation services for WebSphere Application Server</td>
<td></td>
<td>√</td>
<td></td>
</tr>
<tr>
<td>Support for 1-1 and role based identity mappings</td>
<td></td>
<td>√</td>
<td></td>
</tr>
<tr>
<td>Authorization</td>
<td></td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>Course grained authorization for service access</td>
<td></td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>Audit</td>
<td></td>
<td>√</td>
<td>√</td>
</tr>
</tbody>
</table>

**Legend:**
- ✓ Fully supported
- ✓ Supported, but not preferred option in most cases

*Stay tuned for future announcements in this space.*
SOA is based on reusing existing IT investments by dividing the various business applications into discrete business functions and combining them in various ways to implement the organization’s business processes.

- Managing user identities and transforming their representations as they are passed between the services comprising a business process is key to the success of SOA.

→ SOA is Identity Driven!

- Tivoli Security products provide a set of Identity Management and browser/service “Single Sign-On” capabilities for enabling SOA.

Many customers will evolve their systems towards a Service Oriented Architecture.

- Federated Single Sign-On for browser based applications is a popular early step towards the goals of SOA.
Real world implementations of IBM/Tivoli FIM

- T Rowe Price
- Credit Card Co
- Insurance Co

SAML * WS-Security * WS-Trust * Liberty

Tivoli Now!
Customer Pain

- T Rowe Price (TRP) have hundreds of applications for internal and external users secured today by IBM Tivoli Access Manager
- TRP would like to add services that can be outsourced to external providers
- Adding services can lead to increased costs associated with customers and employees needing extra IDs
- Outsourced services can lead to customers leaving the TRP website (introducing inconvenience)
- Looking for a way to seamlessly introduce outsourced services to existing user base
- Partners may have very specific token exchange requirements
T Rowe Price
- Financial services for consumers
- Populations include customers, financial advisors etc.

Yodlee.com
- B2B Financial solutions
- BillDirect (on-line billing), Financial Advisor View tools, Internet toolbar
  - Yodlee can provide seamless billing for existing TRP customers as well as tools for TRP’s financial services advisors (comprehensive account viewing etc.)
  - Enhanced capabilities for customers and advisors provide service improvements/efficiencies at minimal cost/disruption
  - T Rowe Maintains session control as the Identity Provider
How to approach the problem

Yodlee have standardized on SAML for interoperability

Yodlee have very specific SAML requirements for interoperability

All Yodlee-required data is encapsulated within one SAML attribute called YodleeAttributes

It will be the responsibility of TRP to generate this data, and it is likely this will be done via a java callout from the XSL mapping rule

- XSL Mapping rule is a part of the FIM Security Token Service (STS)
  - STS provides the flexibility for extending attributes used in the token

TRP will retrieve the required Yodlee attributes from existing corporate databases during the single-signon process

Tivoli Now!
1. User authenticates with WebSEAL and access TRP application
2. User clicks on third-party link (e.g., ‘Pay Bill’) to initiate Single Sign-On
3. TAM instructs FIM to complete the SSO handshake
4. FIM builds SAML token to Yodlee spec using additional user attributes from TRP data sources
5. Yodlee validates the token
6. Yodlee builds session and provides service
7. After service completes, control returns to TRP application
Why did T. Rowe Price choose TFIM?

Vendors are asking for standard SSO solutions (SAML)
Customers are asking for standard SSO solutions
Faster integration time.
  - With junction technology, they can integrate vendor sites in minutes
  - TFIM meets the same standard.
Vendor Support Solution
  - Let the experts handle implementation details.
• Design approach for Consumer Single Sign On (CSSO) as part of a larger CSSO Blueprint
• Attempted to build environment themselves with a SAML toolkit, but had to re-evaluate and made a decision to go with a COTS product
• Member banks will need to conform to CCC standards
  ▪ SAML 1.1
  ▪ Custom attributes need to be defined
• SSL traffic between all moving components of FIM
• Clustered WebSphere Application Server support a requirement
• Key storage of encryption keys to be offloaded to nCipher F2 cards
Manages the initial authentication process

Member Bank * Identity Provider

CCC International Service Provider

User registry

Internet

SAML assertion

User registry

Tower Group Application

* Manages the initial authentication process
IC’s Info Systems are evolving in several ways:
- Applications are becoming more distributed
- IC has more business partners and vendors
- Is conducting more business electronically.

By adopting a Service-Oriented Architecture (SOA) for IS applications
- The complexity of applications will increase in that control will be further distributed across multiple systems/machines.
- IC recognizes that as these systems evolve to meet goals of improved functionality and efficiency, the security model is simultaneously complicated and its vulnerabilities are magnified.

IC’s goal is to have the ability to define and apply security and privacy policies
- Audit system behavior to ensure compliance

IC’s research is to identify best-practice security administration and controls to be compliant with current US laws and regulations.

The technology and product’s selected must integrate smoothly and naturally with existing infrastructure and strategic plans
- Must perform well with near-constant availability.

IC seeks to determine the out-of-the-box (OOTB) capabilities of IBM’s FIM suite
EPI Service Chaining

- Meaningful business application web services will often be built by combining other web services (‘high-level’ web service calling ‘low-level’ web services).
- Key to security in these scenarios is the preservation of identity from one invocation to the next. In this use-case, the BillingInquiry web service will be logically split into sub-services (say, ‘A’ and ‘B’), such that client calls A; A in turn calls B.
- This use-case will verify that end-user identity (and authorization) is preserved across the chain of invocations from one web service to the next.
Use-Case 3: EPI Billing Inquiry Service Chain

1. Client invokes BillingInquiry Web Service A with SAML authentication assertion
2. Gateway validates authentication assertion, forwards to BillingInquiry service A
3. BillingInquiry A service processes request, itself invoking web service B
4. Gateway receives and forwards request to web service B, preserving identity from (1)
5. Web service B processes & returns response to web service A
6. Web service A completes request from (2), returning final response
7. Response returned to client
EPI ‘Mixed-Mode’

- This is likely to be the most challenging of the use-cases, this use-case will use the gateway’s ability to transform messages.
- The web services client will emulate an Agency Management System (AMS). AMS is an automated process that acts on behalf of agents (end-users).
  - AMS, however, invokes FFIC services using XML over HTTP (i.e. not true SOAP messages). Thus, WS-Security SOAP headers will not be sent from the client.
  - Rather, AMS-specific XML will be sent, which contains elements containing userid and password (plaintext).
- The gateway will receive and transform the incoming request into an equivalent SOAP message (mapping the AMS credentials to WS-Security headers – again UsernameToken). The gateway will then proceed with authentication. Similarly, the response SOAP message must be transformed back into an AMS-specific message as it is returned to the client.
- Further still, this scenario involves the “mixed-mode” operation that EPI requires. The client’s initial request is to a web service. That web service’s response is XML with HTML embedded in one of the XML elements. The HTML will contain links to FFIC web applications, and must include an appropriate token (SAML artifact) that can/will be accepted and authenticated by WebSEAL.
Use-Case 4: EPI ‘Mixed-Mode’ (web service & web appl.)

1. Client invokes EPI Web Service A (XML over HTTP)
2. Gateway extracts authn, authenticates and produces SAML browser artifact to correspond to authn assertion
3. Web Service A processes request, returning XML with HTML ‘attachment’...SAML artifact copied into HTML
4. Web service response (XML) returned to client, which then renders the HTML in a browser
5. Using browser w/ HTML from (4), user invokes web application (via WebSEAL gateway)
6. WebSEAL validates SAML artifact, if valid invocation of web application proceeds.
7. Web Application processes request and returns response.
IC - Use Case 4

XML

Get uid:pwd from XML

wst:RST (UT)

uid:pwd

(Success)

wst:RSTR (UT-no pwd)

XSL (Accord XML->SOAP)

SOAP

HTTP GET to SAML SSO endpoint (BA - uid:pwd)

HTTP 302 to SP SAML SSO endpoint (includes SAML artifact)

Modify URLs in HTML document to include SP endpoint (with original URL as TARGET value)

XSL (SOAP->Accord XML)

Accord XML reply

XML reply (with HTML attachment)

Launch Browser with HTML from attachment

HTTP GET to SP SAML SSO endpoint (includes target URL & SAML artifact)

SOAP (saml: artifact)

SOAP (saml: assertion)

Set TAM login context

Redirect to target URL

HTTP GET to target URL in Webify

HTTP 200

HTTP 200

HTTP 200

Browser

Client

WebSEAL/
Ivans

Layer 7
SSG

FIM STS

TAM Authcn /
LDAP

FIM IdP/
WebSEAL

WebSEAL

(FP)

FIM SP

Webify

FIM IdP/
WebSEAL

WebSEAL

(SP)
Thank You
Disclaimers and Trademarks

No part of this document may be reproduced or transmitted in any form without written permission from IBM Corporation.

Product data has been reviewed for accuracy as of the date of initial publication. Product data is subject to change without notice. Any statements regarding IBM's future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only.

THE INFORMATION PROVIDED IN THIS DOCUMENT IS DISTRIBUTED "AS IS" WITHOUT ANY WARRANTY, EITHER EXPRESS OR IMPLIED. IBM EXPRESSLY DISCLAIMS ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT. IBM products are warranted according to the terms and conditions of the agreements (e.g. IBM Customer Agreement, Statement of Limited Warranty, International Program License Agreement, etc.) under which they are provided.

IBM customers are responsible for ensuring their own compliance with legal requirements. It is the customer's sole responsibility to obtain advice of competent legal counsel as to the identification and interpretation of any relevant laws and regulatory requirements that may affect the customer's business and any actions the customer may need to take to comply with such laws.

The following terms are trademarks or registered trademarks of the IBM Corporation in either the United States, other countries or both: DB2, e-business logo, eServer, IBM, IBM eServer, IBM logo, Lotus, Tivoli, WebSphere, Rational, z/OS, zSeries, System z.

Java and all Java-based trademarks are trademarks of Sun Microsystems, Inc. in the United States and/or other countries.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States and/or other countries.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Linux is a trademark of Linus Torvalds in the United States and other countries.

Other company, product, or service names may be trademarks or service marks of others.

ITIL® is a Registered Trade Mark, and a Registered Community Trade Mark of the Office of Government Commerce, and is Registered in the U.S. Patent and Trademark Office.

IT Infrastructure Library® is a Registered Trademark of the Central Computer and Telecommunications Agency which is now part of the Office of Government Commerce.