

Federated Identity Management Use Case

Marc Vanmaele
CEO SecurIT



Agenda

- **Federation fundamentals**
- **Use Cases**
 - SAML 2.0 Federation
 - Microsoft SharePoint integration for External Users
 - Kerberos Junctions for Internal Users

Federated Single-Sign On

- **Federated Identity**

- Goal: Share user information among trusted partners in a transaction.
- Foundation of trust between partners

- **Benefits**

- Identity management costs lower
- User experience improved

- **Business model for FIM**

- Mergers and acquisitions
- Collaboration between autonomous cross-business units
- Customer acquisition strategy via partnerships
- Employee access to outsourced provider services
- Portal-based integration of software-as-services

© 2009 SecurIT

3

SecurIT

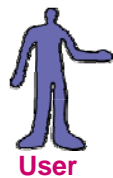
A Federation

- **1 Identity Provider**

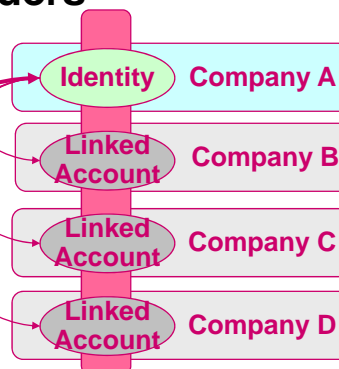
- Authenticate the user

- **x Service Providers**

- **1 protocol**



User



© 2009 SecurIT

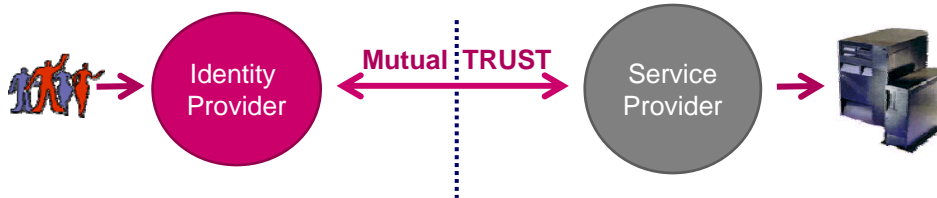
4

SecurIT

Identity Provider vs Service Provider

“Vouching” party in transaction

“Validation” party in transaction



1. Issues Network / Login credentials
2. Handles User Administration/ ID Mgmt
3. Authenticates User
4. “Vouches” for the user’s identity

1. Service Provider controls access to services
2. Third-party user has access to services for the duration of the federation
3. Only manages user attributes relevant to SP

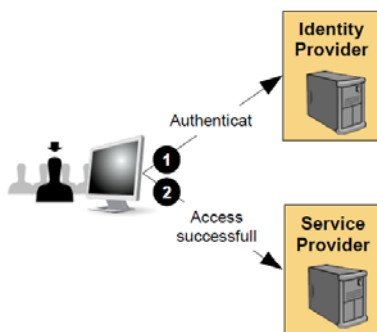
© 2009 SecurIT

5

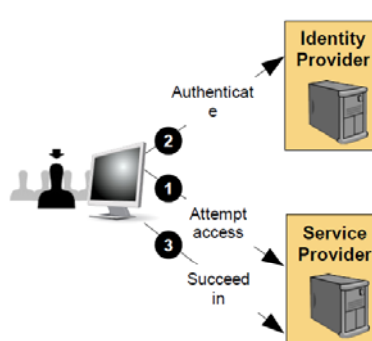
SecurIT

Federation Example

SAML 2.0: Push vs Pull



IDP-initiated



SP-initiated

© 2009 SecurIT

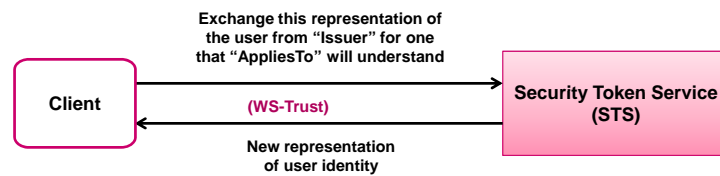
6

SecurIT

Security Token Service (STS)

- **Based on a Security Token Service**

- As defined by WS-Trust (OASIS Standard)
- WS-Trust defines Identity Mediation Service

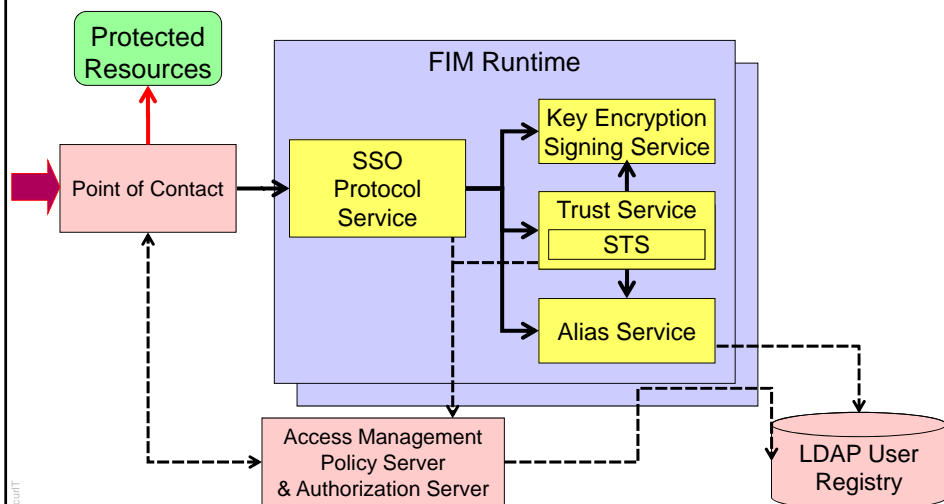


© 2009 SecurIT

7

SecurIT

FIM Components for Federated SSO



© 2009 SecurIT

8

SecurIT

FIM example

- **Example: IBM Tivoli Federated Identity Management (TFIM)**

- Point-Of-Contacts
 - WebSphere, WebSEAL, IIS, Custom POC
- Support of standards based web single sign-on protocols
 - SAML 1.1, SAML 2.0, OpenID, WS-Federation, IdentityCard...

© 2009 SecurIT

9

SecurIT

Use Cases

- **Customer Case**

- SAML 2.0 federation
- Challenges
- Do's and Don'ts



- **SharePoint Integration**

- Federation
- Kerberos Junctions



© 2009 SecurIT

10

SecurIT

Customer Case: SAML 2.0 federation

- **Purpose : Marketing driven**
 - Send direct marketing information to a customer
 - Tracking people's interests
 - Ultimate goal: 1 portal with all service providers
- **# of users**
 - 1,2 Million users on Identity Provider
- **Entities involved :**
 - Telecom company as Identity Provider
 - Several 'brands' as Service provider
 - Fixed Lines
 - Internet Provider
 - Mobile Communication Services
 - External services
 - Video on demand

© 2009 SecurIT

11

SecurIT

Challenges

- **Challenges**
 - Integrating in the current application environment with a minimum (none) of changes to the current applications.
 - Setting up the complex TFIM environment into the current infrastructure.
 - Mapping Identities from the Identity Provider to the Service Provider based on attributes from multiple (existing) repositories (ITDI)

© 2009 SecurIT

12

SecurIT

Do's

- **Start inside – inside**

- IdP and SP partners from common organization.
 - Easier to control the variables.
 - Mapping principal identities usually much easier.
 - Reduce/eliminate legal issues.
 - Experience allows development of organizational competency and standards which can later be translated to working with external partners.

Do's

- **Clearly define requirements and scope**

- Flow of login process
- Session management
 - Consider using Session Management Server
- Single Log on/Single logout requirements

- **Clearly define security requirements**

- Encryption/signing of data
 - All/partial
 - Might add complexity in the setup
- Protocol bindings
 - Artifact might be more secure, but demands more WebSEAL server instances, firewall ports, keystores etc.

Do's

• Naming conventions

- Keystores
 - Determine the need for certificates, keys etc.
 - Define naming conventions for keystores:
 - There are quite a few to keep track of
- Federations, domains
 - Keep names meaningful, short, lowercase and simple
 - Names come back in url's, and are not easily changed afterwards

© 2009 SecurIT

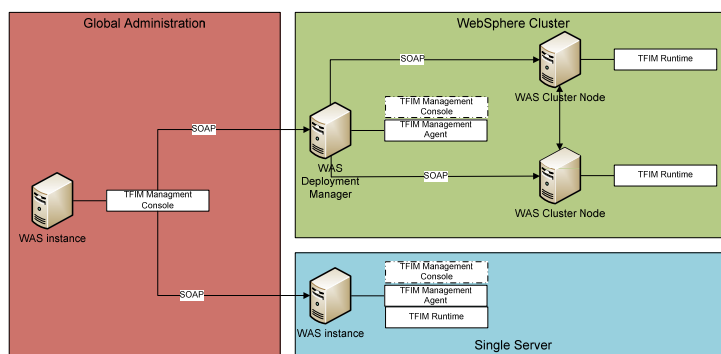
15

SecurIT

Do's

Availability

- an IdP function quickly becomes business critical.
- Installation of TFIM in a WebSphere cluster is a necessity
- WebSEAL and LDAP are critical components, so need to be replicated
- When using Session Management Server, cluster it as well



© 2009 SecurIT

16

SecurIT

Pitfalls – External

- **It takes two to federate**

- Terminology differences
 - Much of the terminology is well established.
 - Some terms (“artifact resolution service”, etc) may be part of a standard, but don’t assume the person at the other end knows what you mean.
- Organizational differences
 - You may have no idea who you’re working with at the other end.
 - Communication with your federation partner is likely to be via email, phone.
- Technology differences
 - You may not even know what product the other end is using.
 - Not all products support the full set of protocol options/capabilities

© 2009 SecurIT

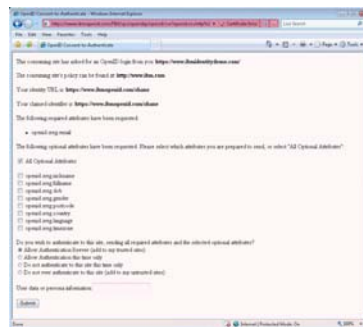
19

SecurIT

Legal requirements

- **Legal**

- Inside-out and outside-in federations will almost always be done in the context of some legal agreement between the parties.
- Agreements may have certain assumptions and restrictions within them.
- Consider if user consent is needed to federate (and if chosen standard supports it (like OpenID, SAML 2.0))
- If a party says “let’s federate”, it is a good idea to ask whether an existing agreement is in place which will allow it.



© 2009 SecurIT

20

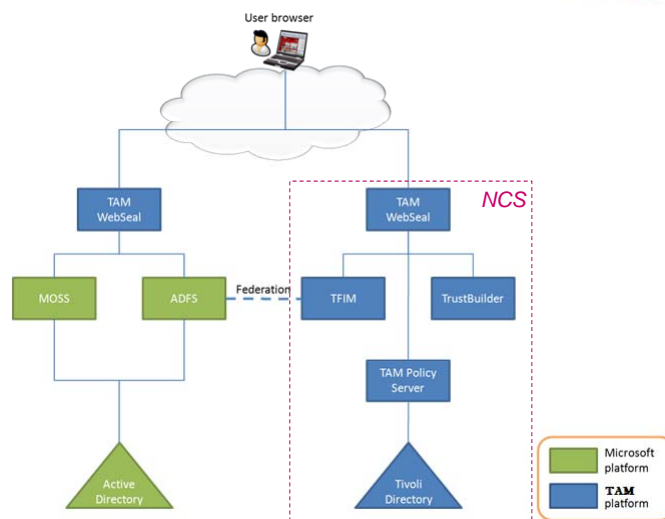
SecurIT

SHAREPOINT INTEGRATION (POC)

2 USE CASES

- **External Users: Federation**
with Microsoft Active Directory Federation Service (ADFS)
- **Internal Users: TAM Kerberos junctions**

Case 1: Federation with ADFS

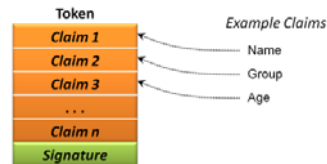


POC: Federation with ADFS/Sharepoint

- **Protocol:** WS-Federation/SAML 2.0
- **IdP:** TFIM with WebSEAL
- **SP:** Active Directory Federation Services (ADFS)

- **User mapping**

- TAM user ID = Identity in SAML token
 - Is used to welcome the user
- LDAP attribute is read during authentication
 - Has value "role1" or "role2"
 - → in TAM extended attribute: tagvalue_roles
 - → TFIM: Translated in SAML attributes
 - <http://test.lab/federation/v1/claim1> → true if role1
 - <http://test.lab/federation/v1/claim2> → true if role2
 - → ADFS: Translated in sharepoint roles and thus authorization



© 2009 SecurIT

23

SecurIT

Authentication/Authorization Process

- **User accesses protected page**
- **User logs in on WebSEAL using his CAP/EMV bankcard**
- **User gets access to the sharepoint junction**
- **ADFS detects that user should be authenticated**
- **ADFS sends Authentication request to the IdP**
- **TFIM creates SAML token**
 - User ID = TAM ID
 - Attribute claims are set to TRUE|FALSE
- **Authentication response including SAML token is sent to ADFS**
- **ADFS consumes token and create internal session for the user with certain role (based on the info in the SAML token)**
- **User gets access to the applications allowed for this role**

© 2009 SecurIT

24

SecurIT

Case 2: TAM – Sharepoint Junctions

• Kerberos Junctions

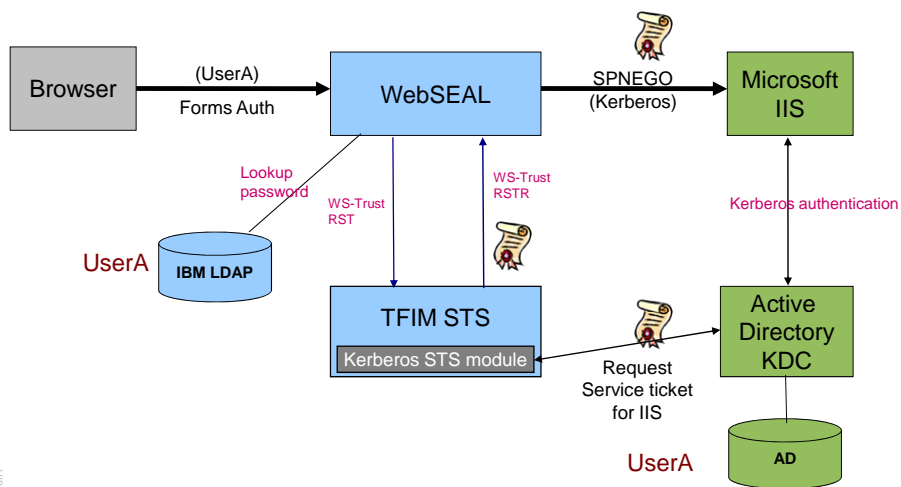
- allows WebSEAL to send a Kerberos ticket (via SPNEGO) to achieve SSO to a junctioned application
- TFIM Security Token Service (STS) to generate the Kerberos tickets
 - **! TAM 6.1.1** – SSO to junctioned backend using STS
 - Kerberos credentials, LTPA tokens, SAML tokens
- Many Microsoft applications require a new ticket for each HTTP request
 - TFIM can generate a 'set' of Kerberos tickets for each request from WebSEAL
- User ID mapping possible in the STS
- Any form of authentication to WebSEAL can be used
- No platform restrictions for TAM servers, only the TFIM server must run in the AD Domain
- Identity that runs IIS application pool must be configured for Kerberos constrained delegation

© 2009 SecurIT

25

SecurIT

Kerberos Junction Detail



© 2009 SecurIT

26

SecurIT

Questions?



Thank
You

© 2009 SecurIT

27

SecurIT