

Federated Identity Management

Infosecurity 2011

Marc Vanmaele
CEO SecurIT



- **SecurIT Overview**
- **Federation fundamentals**
 - The Federated Identity Concept
 - Standards
 - Practical Implementation
- **Use Cases**
 - SAML 2.0 Federation, Challenges, Do's and Dont
 - Microsoft SharePoint integration for External Users
 - Kerberos Junctions for Internal Users



- **SecurIT Overview**
- **Federation fundamentals**
 - The Federated Identity Concept
 - Standards
 - Practical Implementation
- **Use Cases**
 - SAML 2.0 Federation, Challenges, Do's and Dont
 - Microsoft SharePoint integration for External Users
 - Kerberos Junctions for Internal Users

SecurIT Overview

- Created in 1999 and privately held
- Offices in Gent (Belgium) and Amsterdam (Netherlands)
- Focus on Identity & Access Management solutions
 - +50 consultants on IAM
 - +50 successful Projects at Large Enterprise Customers
- Software products: TrustBuilder®, D-Man™, RoleManager™



Tbuilder
TRUST

Dman
e-business & security monitoring

ROLE
manager

- Worldwide Partner Network (Europe, North & South America, Australia)

encode

UNISYS



aTheos
L'esprit d'Architecte

first@ttribute

MORSE

AZERTIA



SENETAS
trusted to secure critical information

Some SecurIT Customers



Rabobank



- SecurIT Overview
- **Federation fundamentals**
 - The Federated Identity Concept
 - Standards
 - Practical Implementation
- **Use Cases**
 - SAML 2.0 Federation, Challenges, Do's and Dont
 - Microsoft SharePoint integration for External Users
 - Kerberos Junctions for Internal Users

- **Federated Identity**

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

- **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 and Cloud Services

- **Benefits**

- Identity management costs lower
- User experience improved

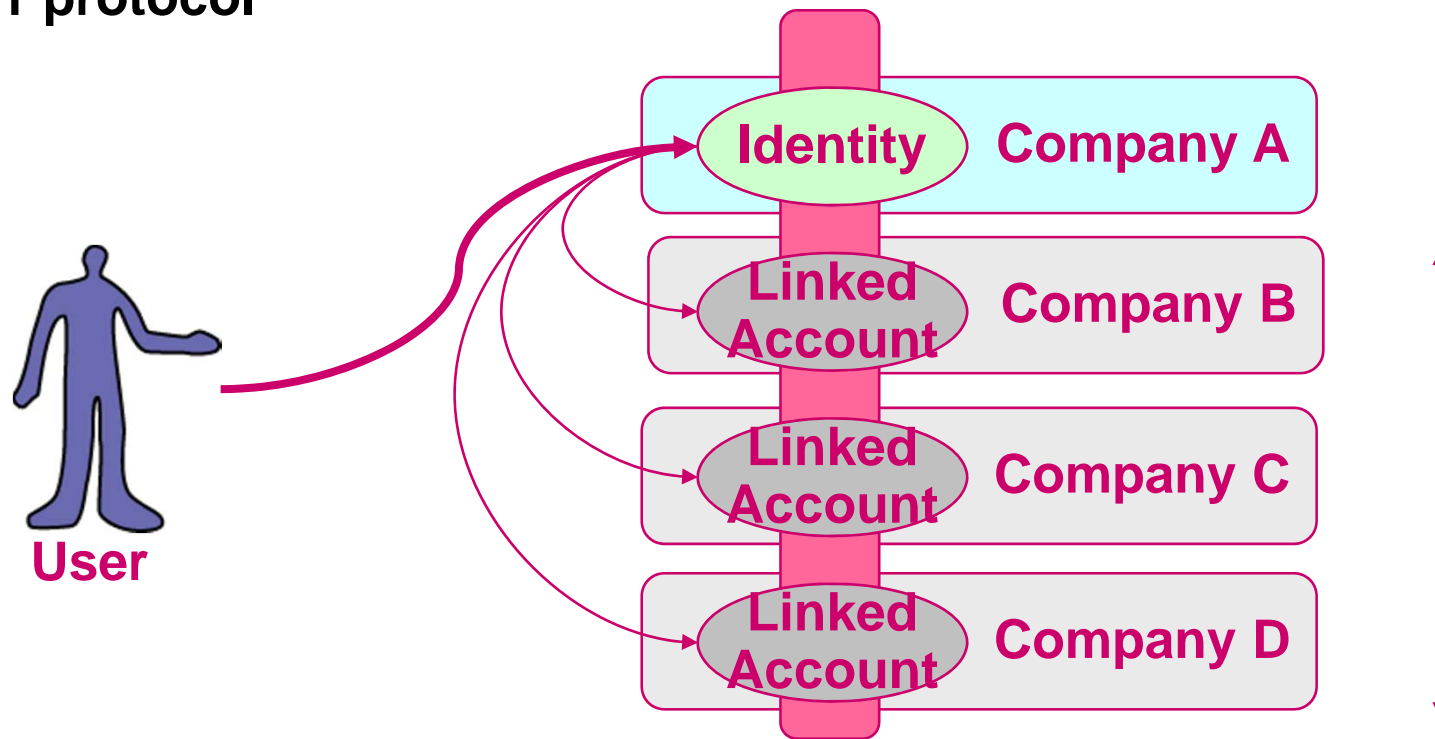
- **Challenge**

- Avoid needless complexity
- Practical experience is important



A Federation

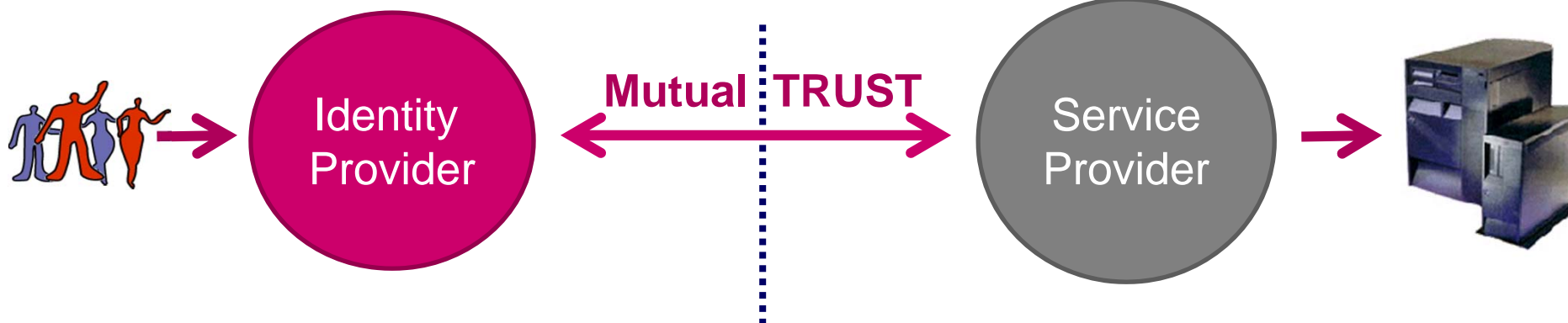
- **1 Identity Provider**
 - Authenticate the user
- **x Service Providers**
- **1 protocol**



Identity Provider vs Service Provider

“Vouching” party in transaction

“Validation” party in transaction



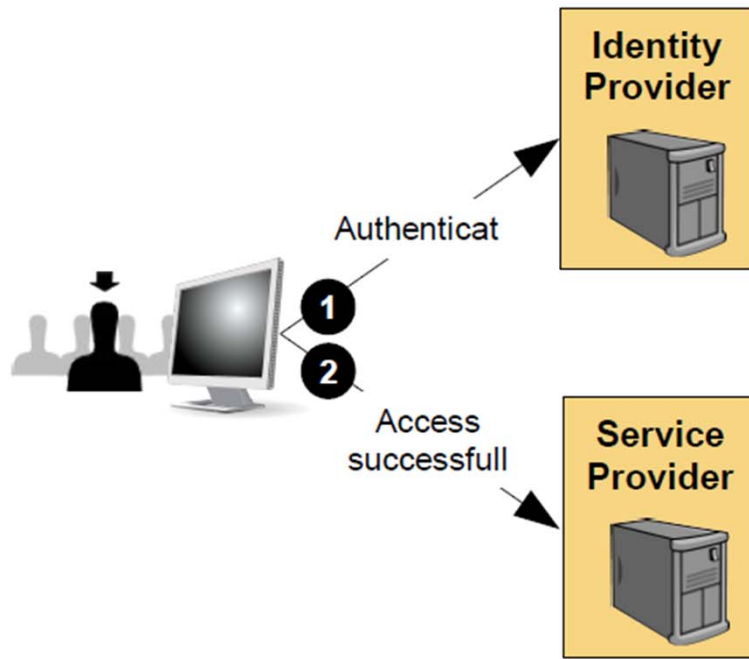
1. Issues Network / Login credentials
2. Handles User Administration/ ID Mgmt
3. Authenticates User
4. “Vouches” for the user’s identity

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

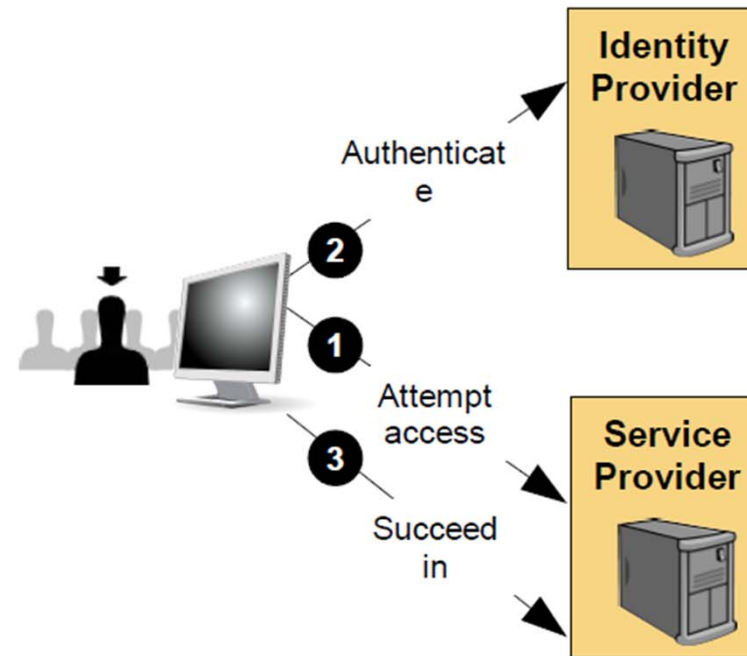
Federation Example



Push versus Pull

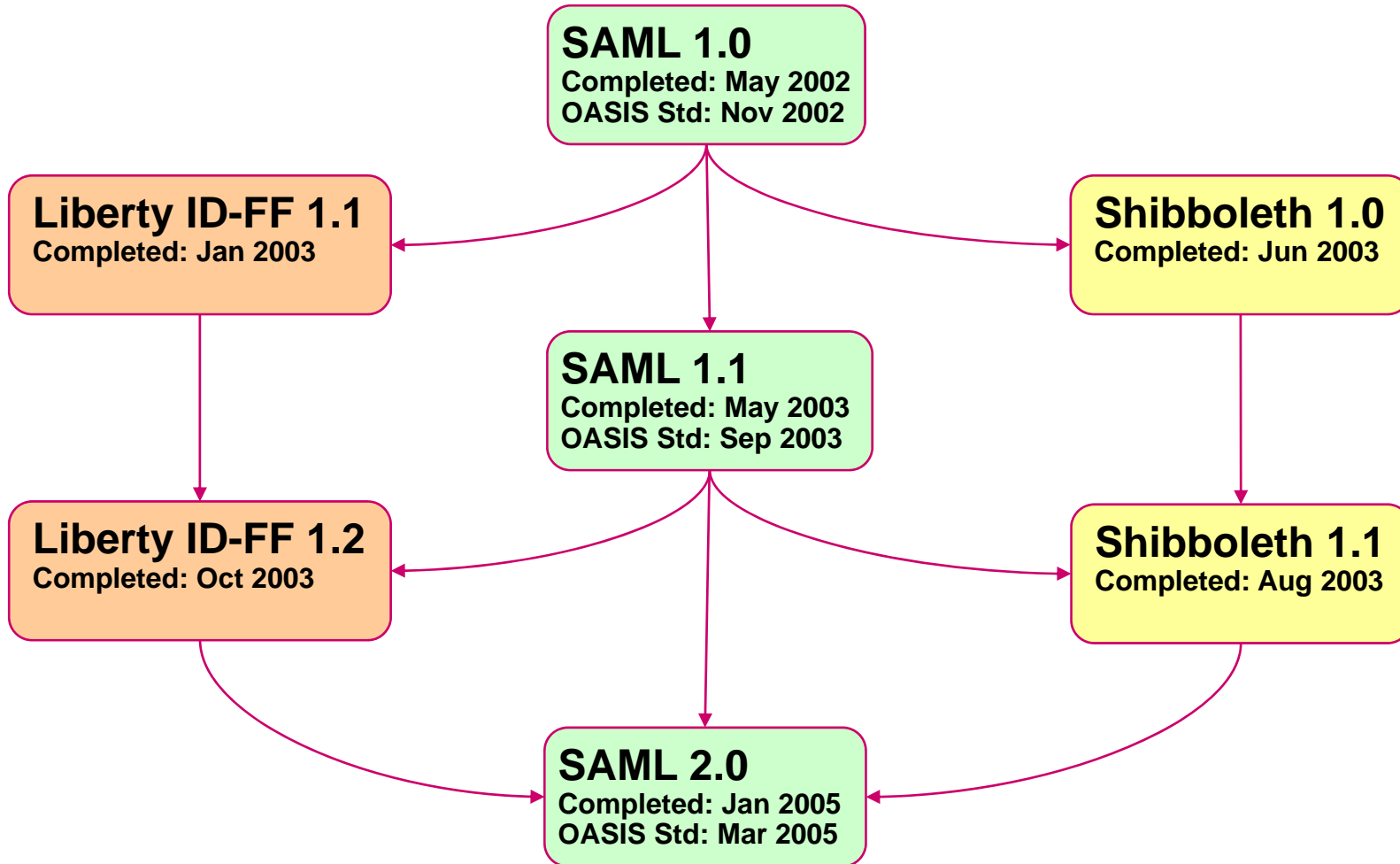


IdP-initiated



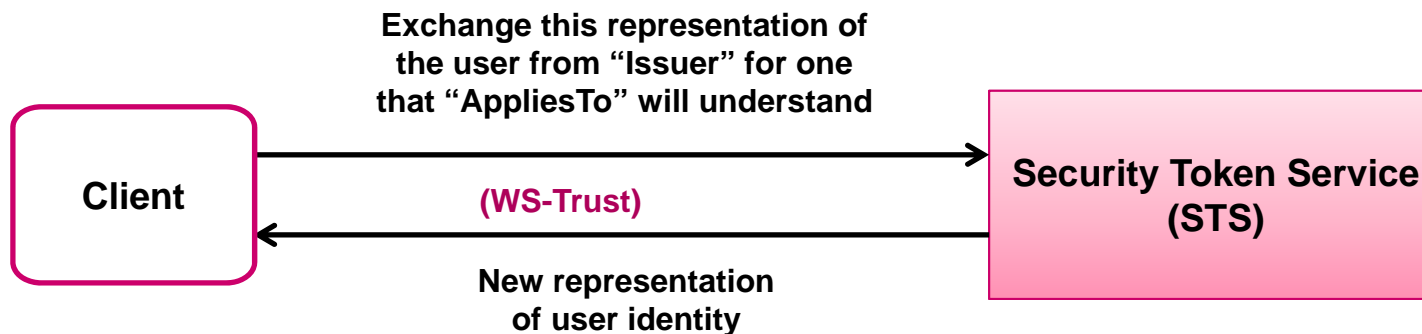
SP-initiated

Evolution of Federated SSO Standards

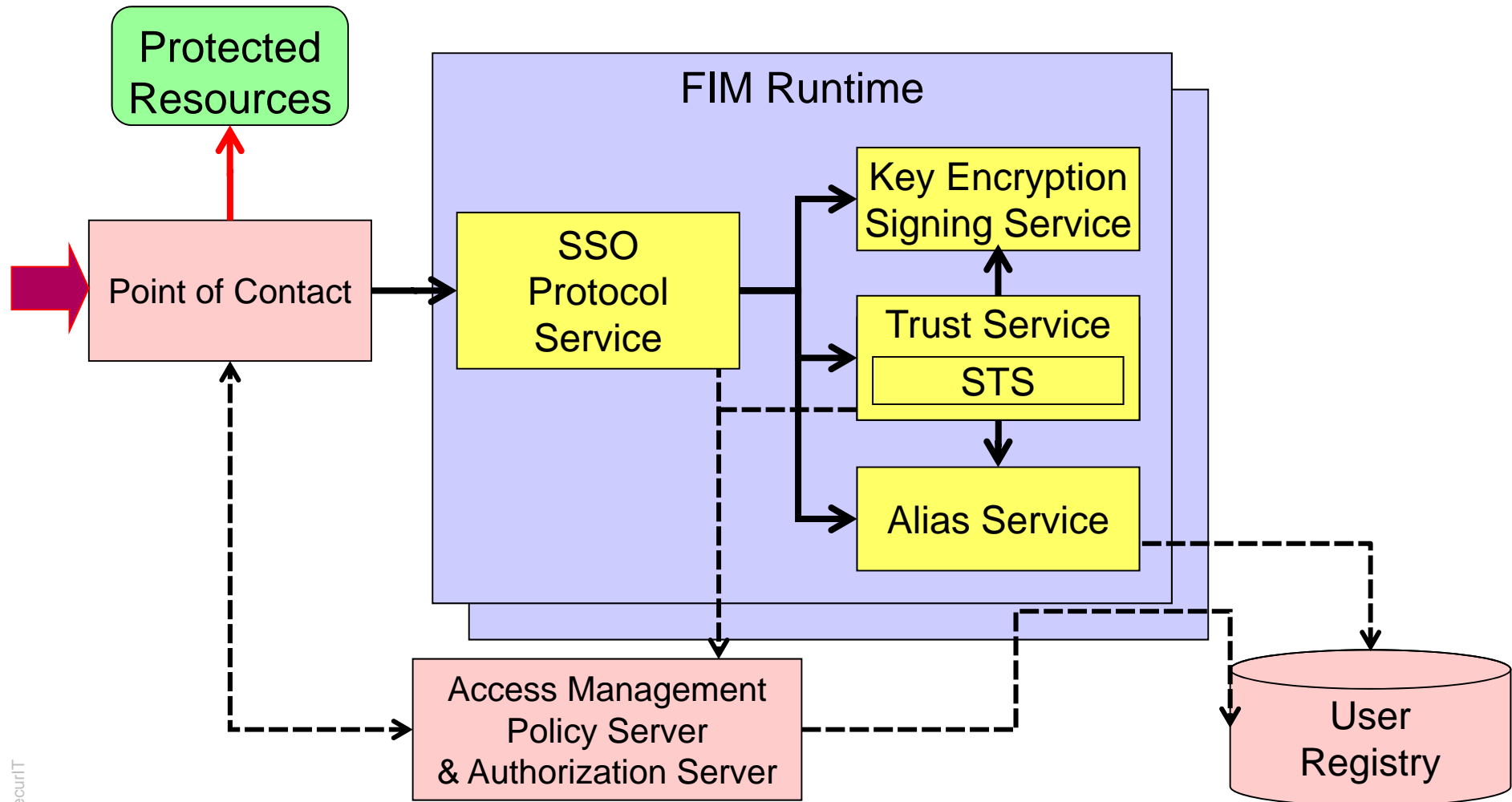


- **Based on a Security Token Service**

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



FIM Components for Federated SSO





- **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...



- **SecurIT Overview**
- **Federation fundamentals**
 - The Federated Identity Concept
 - Standards
 - Practical Implementation
- **Use Cases**
 - SAML 2.0 Federation, Challenges, Do's and Dont
 - Microsoft SharePoint integration for External Users
 - Kerberos Junctions for Internal Users



- **Customer Case**

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

- **SharePoint Integration**

- Federation
- Kerberos Junctions



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





- **Challenges**

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



- **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.

- **Clearly define requirements and scope**

- Flow of login process
- Session management
 - Consider using Session Management Server
- Single Sign-On / Single Sign-Out 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 PEP server instances, firewall ports, keystores etc.



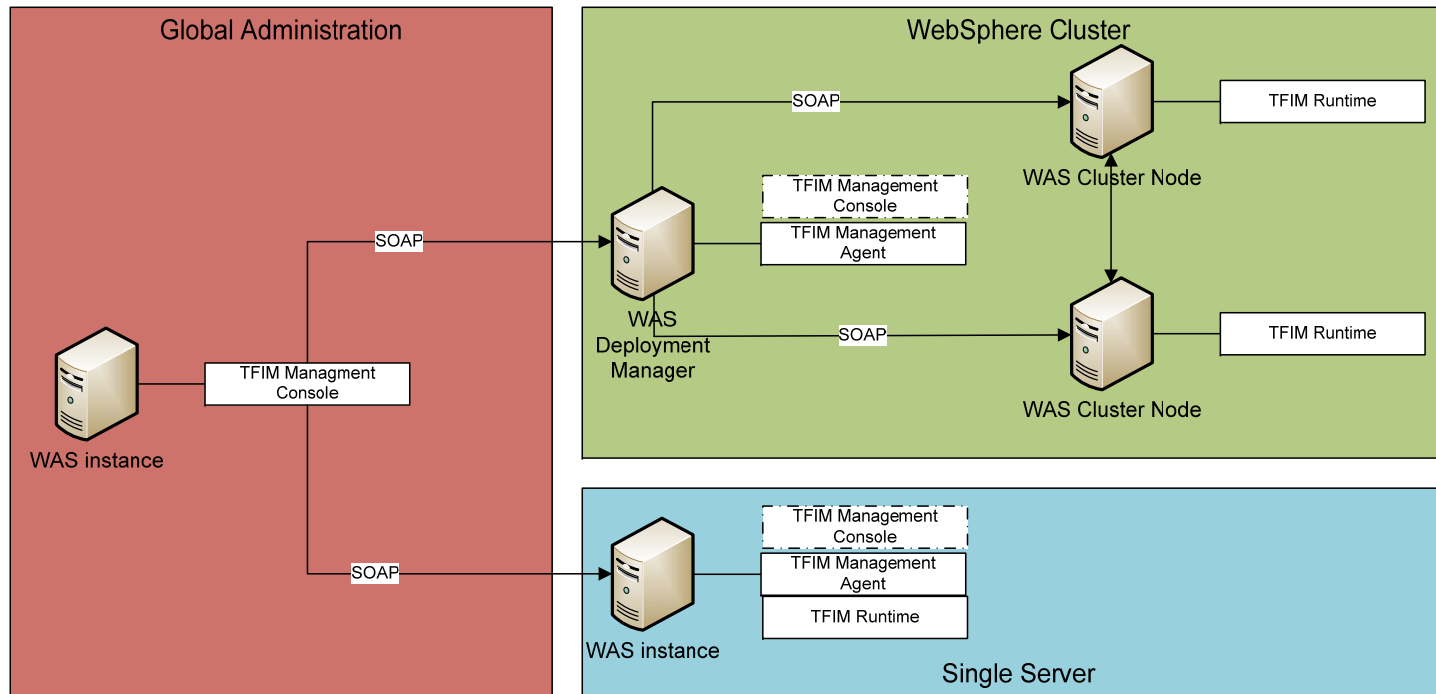
• Naming conventions

- 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



Availability

- an IdP function quickly becomes business critical.
- Installation in a cluster is often a necessity
- PEP and User Repository are critical components, so need to be replicated
- When using some Session Management Server, cluster it as well



- **User mapping**

- **Do**

- Use xsl mapping files, or
 - Use ITDI (Metadirectory Tool)



- **Don't**

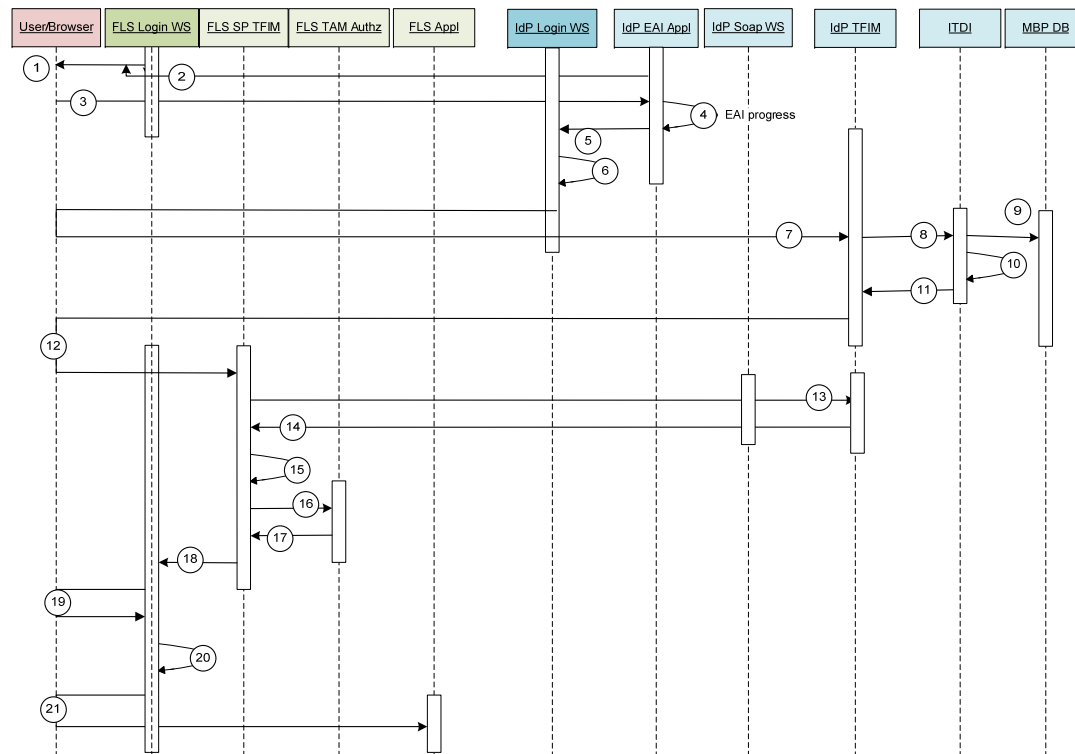
- **Avoid persistent mapping**

- Persistent storing of mapping data in LDAP or DB is difficult to manage
 - No standard interfaces are available to remove these mappings
 - Cleaning up once a user is de-federated/removed becomes difficult



Pitfalls

- **Think about what can go wrong in the authentication process**
 - Login process can be complex with different steps at different components
 - Make sure errors in the login process are clearly understood and mapped to understandable messages for users (text) as well as support (errorcode)





- **It takes two to federate**

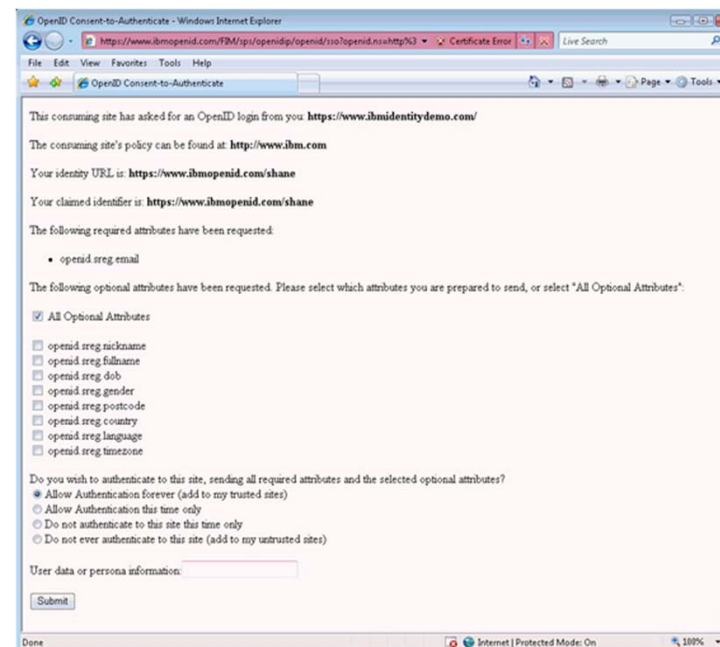
- Terminology differences
 - Much of the terminology is well established.
 - Some terms (“artifact resolution service”, etc) may be part of a standard, but don’t assume the person at the other end knows what you mean.
- Organizational differences
 - You may have no idea who you’re working with at the 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



Legal requirements

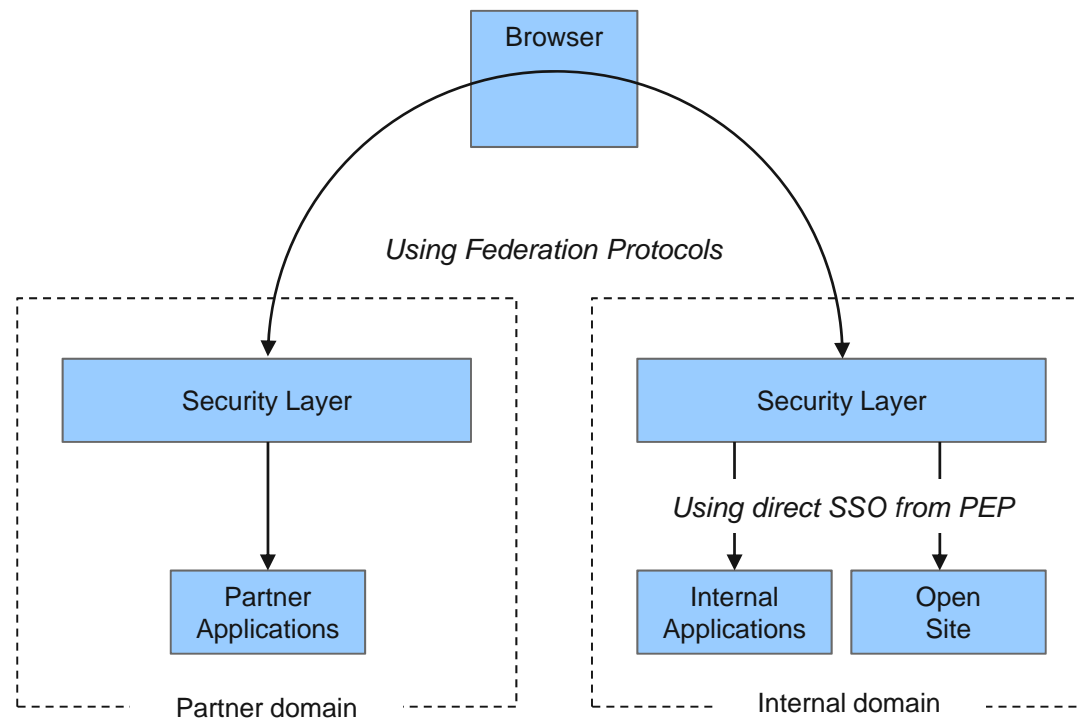
- **Legal**

- 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.



Federation – for external and internal (?)

- Federation pattern, preferred for external hosted applications
- Classic Web Access Management preferred for internal applications
- Hybrid approach for an integrated solution



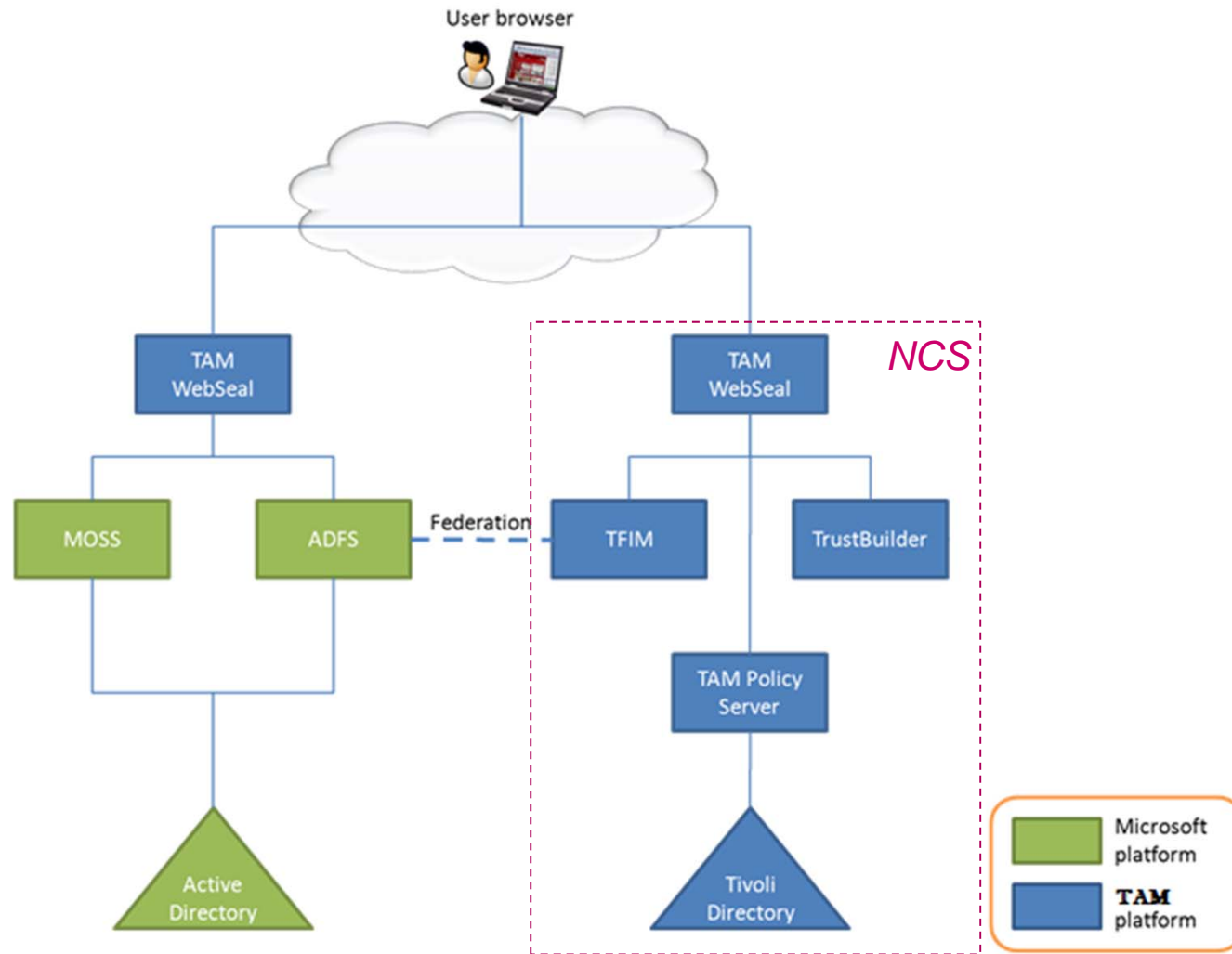


MICROSOFT SHAREPOINT INTEGRATION

2 Examples:

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

Case 1: Federation with ADFS

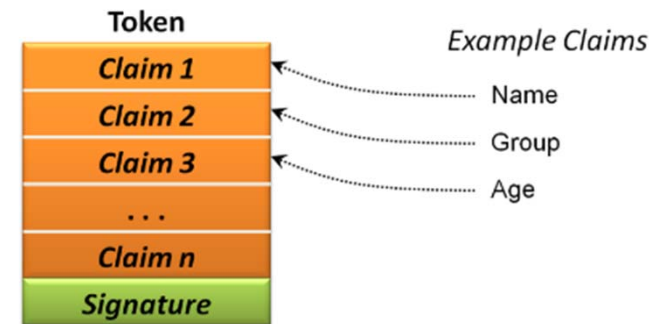




- **Protocol:** **WS-Federation/SAML 2.0**
- **IdP:** **TFIM with WebSEAL**
- **SP:** **Active Directory Federation Services (ADFS)**

- **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

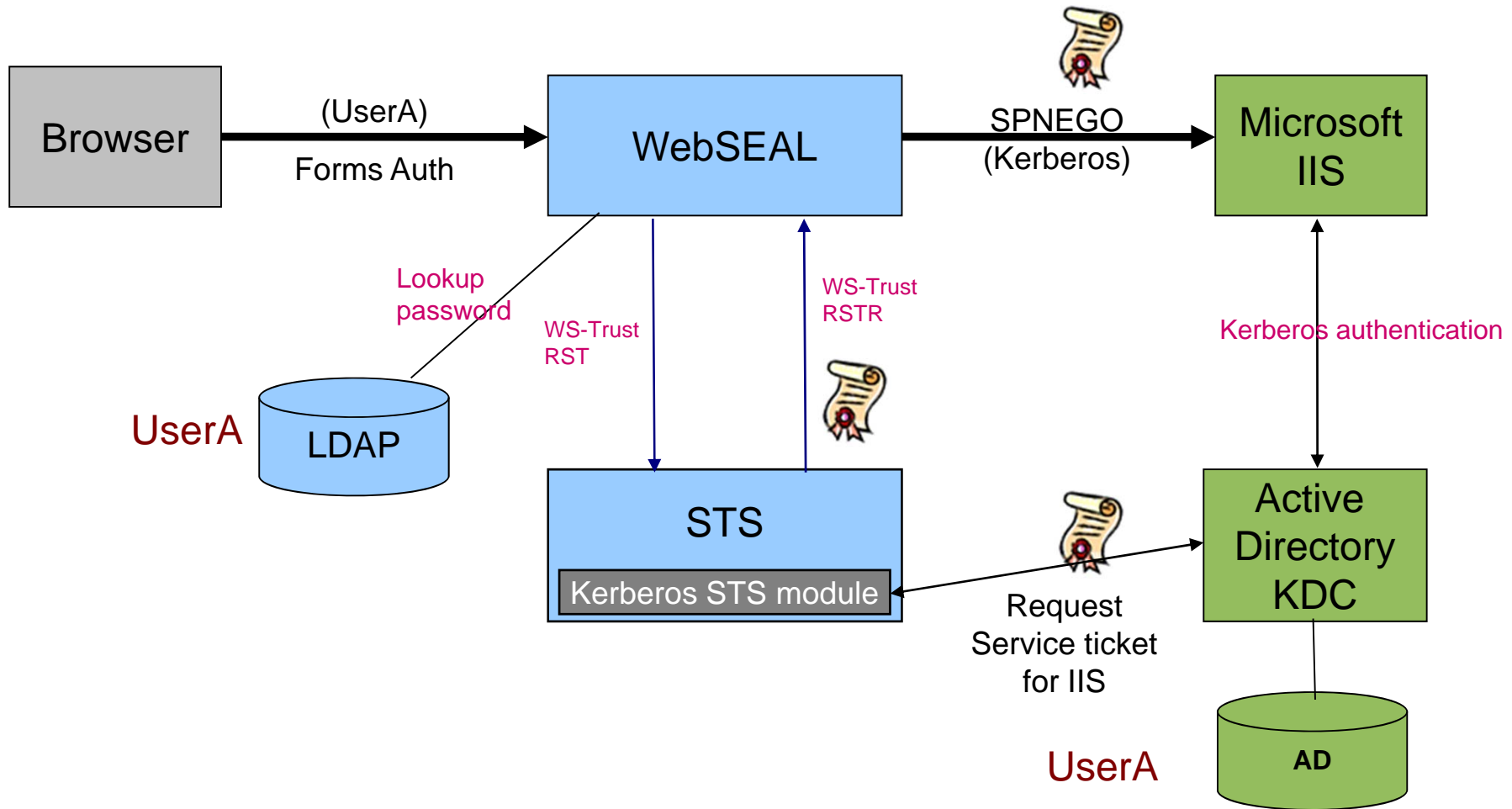


Example 1: Federated Sign-On



- **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**

Kerberos Junction Detail



Conclusions



- **Federated Identity Management provides the Security Layer for the Mashed Business World**
- **Benefit of Standards on the long term**
- **Lower Identity Management costs and enhanced user experience**
- **Be ware of Misuse**

Questions?



Thank
You

marc.vanmaele@securit.biz