More SharePoint Security. Less Effort.

Using Claims Based Authorization to Strengthen SharePoint Data Governance

Antonio Maio
Senior Product Manager, SharePoint Solutions

TITUS

Agenda

- Introduction
- Data Governance, Sharing vs Protecting, Considerations
- Authentication vs Authorization
- What are Claims?
- Architecture and Trusted Identity Providers
  - Common Configuration Considerations
- Common Customer Requirements
- Demonstration
- Question/Answer

WWW.TITUS.COM | © TITUS. ALL RIGHTS RESERVED |

The Netherlands – This Week

- 5 Days
- Drove over 1000 km
- Visited 7 cities
- 5 Different Hotels
- Beautiful Country!

WWW.TITUS.COM | © TITUS. ALL RIGHTS RESERVED |

Book Giveaway

- Professional SharePoint 2010 Development
- Compliments of TITUS

- Draw at end of session
- Fill out the cards and give them back before the end (or give business card)

WWW.TITUS.COM | © TITUS. ALL RIGHTS RESERVED |

TITUS Overview

- Data Security & Classification Market Leader
- Over 300 Enterprise Customers
- Over 2 Million Users Deployed

- SharePoint Security
- Email and Document Marking
- Data Loss Prevention

Check out our SharePoint blog:
http://www.titus.com/blog

Gartner | 2011
COOL VENDOR

WWW.TITUS.COM | © TITUS. ALL RIGHTS RESERVED |

Data Governance

- Recognizing that data is an Asset to Protect
- Applying Controls and Processes to your Data
- Risk Management, Data Quality, Security Policies, Compliance, Auditing, etc…
- Authorization
  - Enforce policies to control access to sensitive content
  - Ensure data can be trusted

WWW.TITUS.COM | © TITUS. ALL RIGHTS RESERVED |

Protecting vs Sharing Information

- Dealing with multitude of information
  - From Many Sources – Internal, External, System Gen, Historical, etc…
  - Content Growing at Incredible Rate
- Military/Government – Success requires sharing data
  - Enterprises Sharing Data also critical – departmental, with partners
- Protecting sensitive information also very important

- Ensure right people are accessing the right information
- Sensitive data sitting beside non-sensitive data

WWW.TITUS.COM | © TITUS. ALL RIGHTS RESERVED |

Information Sharing Considerations

- Automation is Critical
  - Ensures access control policies are consistently applied
- User Identity or Trusted Claims
  - Who am I, What's my clearance level, etc…
- Leverage Document Metadata
  - What's the classification on this document
- Environmental Data
  - Time of day, Geo-location, Connection type, Device
- All Methods of Accessing/Viewing Content
  - Web view, Search, Explorer, Roll-ups, custom web parts
- Visual Security Labels
  - Ensure everyone knows what content is sensitive

WWW.TITUS.COM | © TITUS. ALL RIGHTS RESERVED |

Authentication

- What is Authentication?
  - Determining if someone is who they say they are
  - Typically done today through username/password

- How do Claims go beyond this?
  - Verify other information about a user – a claim
  - More complex authentication processes – Ex. 2 factor
  - Single Sign-On across systems in different domains

WWW.TITUS.COM | © TITUS. ALL RIGHTS RESERVED |

Claims Authentication in SharePoint 2010

- New Authentication Option in SharePoint 2010
  - Some configuration involved
- Previous Authentication Methods (MOSS)
  - Windows Authentication (Windows login, NTLM, Kerberos)
  - Forms Based Authentication (through a web page)
- SharePoint 2010 Authentication Options
  - Classic Mode Authentication (Windows Authentication)
  - Claims Based Authentication
  - Forms Based Authentication – must be configured with claims

WWW.TITUS.COM | © TITUS. ALL RIGHTS RESERVED |

Authorization

- What is Authorization?
  - Determining what users are allowed to access and do
  - Typically done through policies using information about the user, content, etc…
- Using Claims…
  - Authorization can be specific to the user
  - Authorization can be dynamic – ex. changes in a user's security clearance
  - Authorization can include environmental attributes (current time, GEO location, connection type, etc.)
  - Alternative to security groups – Groups do not scale

WWW.TITUS.COM | © TITUS. ALL RIGHTS RESERVED |

Enabling Authorization in SharePoint 2010

- Infrastructure and Configuration Required
  - Storing, managing, retrieving, transforming, trusting claims
  - Configuration – we'll see some of that
- Planning Required
  - Determining policies, claims, getting stakeholders to agree
- Development Required or 3rd Party Apps
  - Native SharePoint 2010 functionality to do this is manual
  - WS-Trust and WS-Federation to retrieve and validate claims
  - Design apps to verify specific required claims only – remember privacy

WWW.TITUS.COM | © TITUS. ALL RIGHTS RESERVED |

What is a Claim?

- User attributes
- Metadata about a user
- AD attributes/LDAP attributes

- Claims are trusted assertions I make about myself
  - Identity attributes retrieved from a trusted identity provider
  - Packaged and signed in a standards-based way (ex. SAML)
  - Allow me to take my identity across network boundaries in a trusted and secure way

WWW.TITUS.COM | © TITUS. ALL RIGHTS RESERVED |

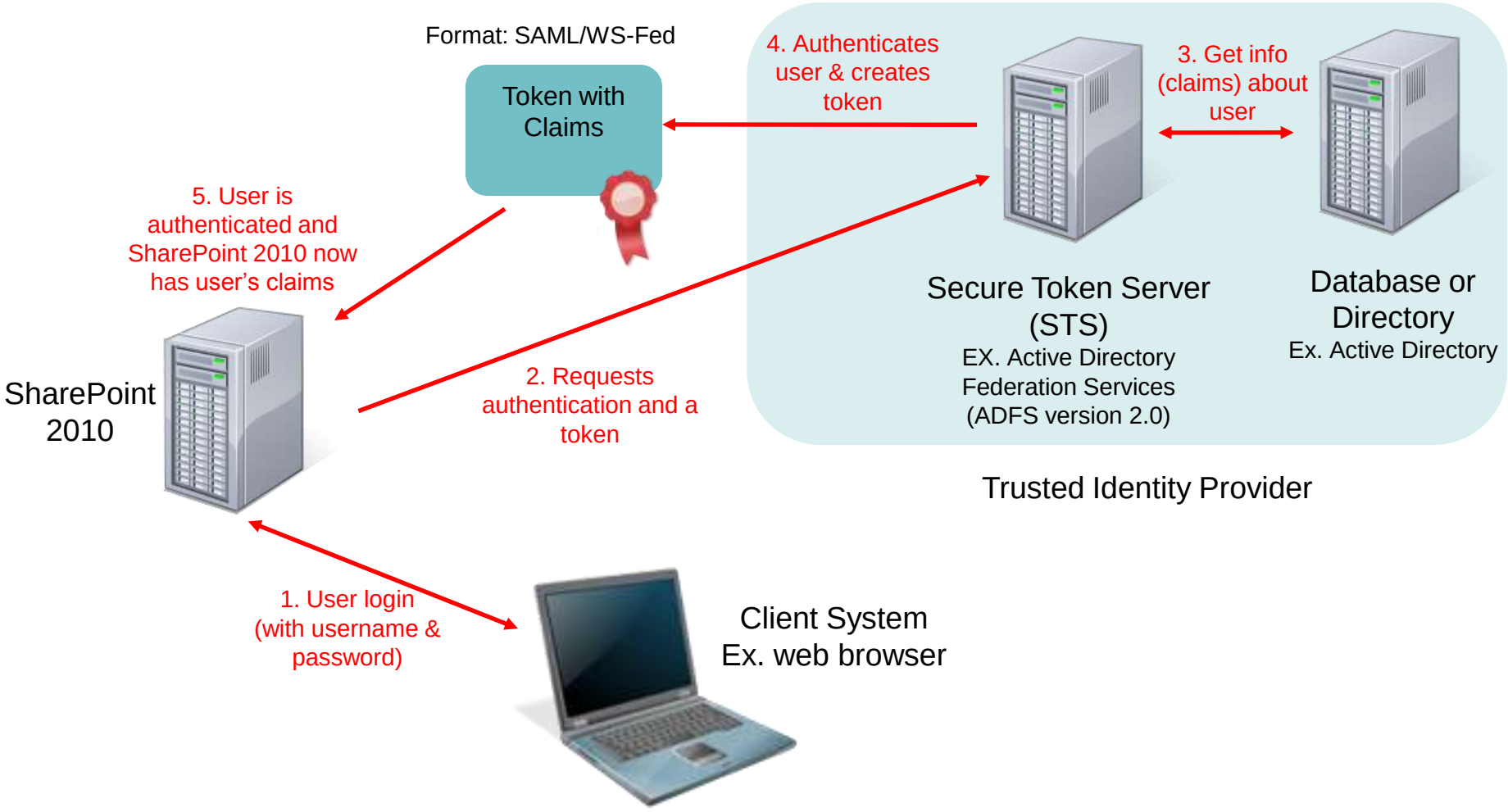
Claims About Me

Name	Antonio Maio
Email	antonio.maio@titus.com
Department	Product Management
Security Clearance	Secret (Canada)
Military Rank	<none>
Employment Status	FTE
Over 18 Years Old	Yes
Valid Driver's License	Yes
Country of Birth	Canada
Citizenship	Canadian, Italian

How can you trust these claims I'm making?

WWW.TITUS.COM | © TITUS. ALL RIGHTS RESERVED |

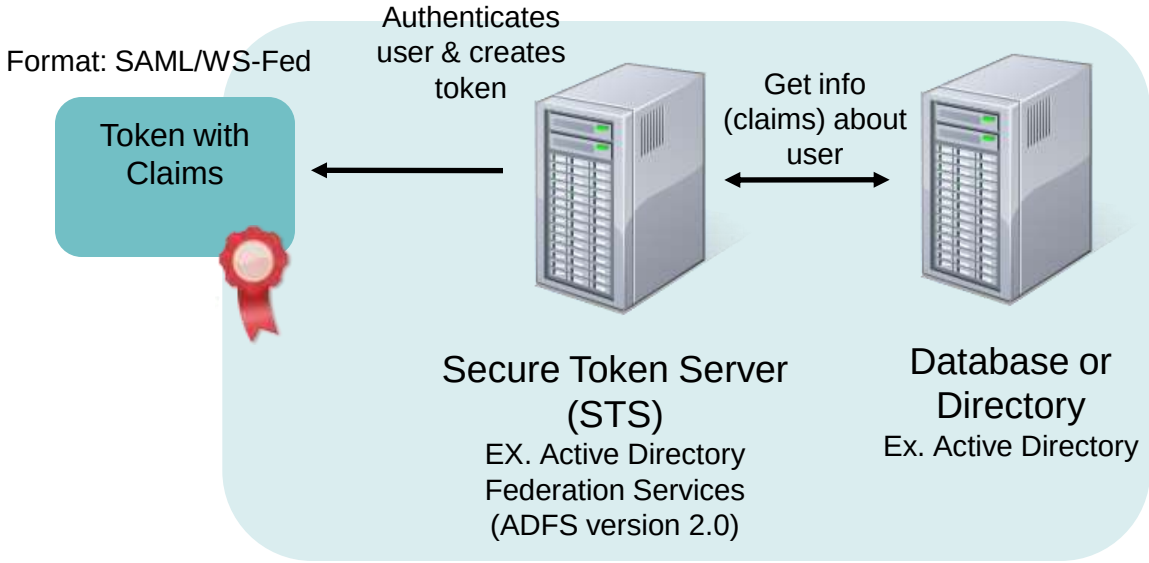
Architecture for Authentication



WWW.TITUS.COM | © TITUS. ALL RIGHTS RESERVED |

Trusted Identity Providers

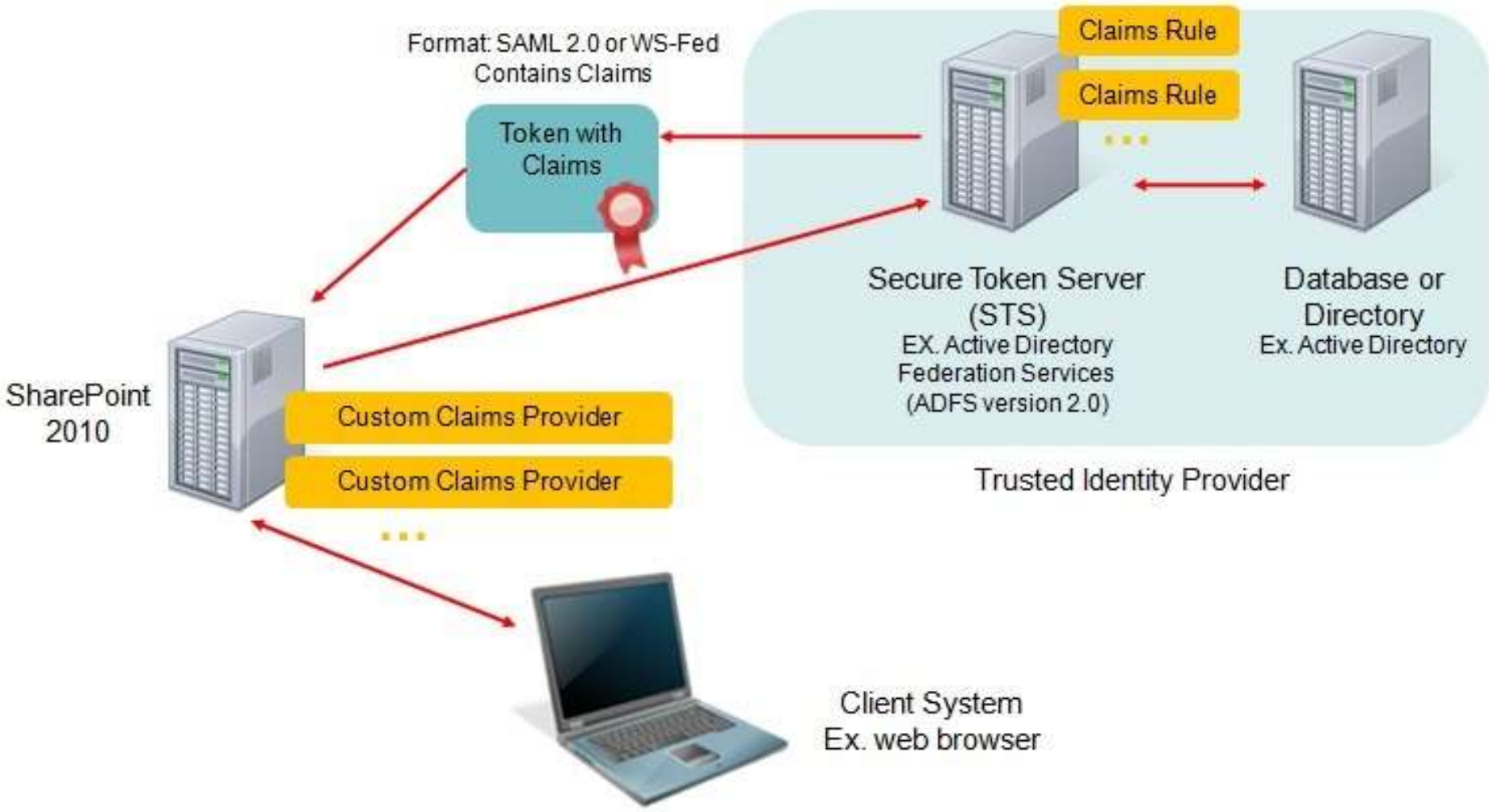
- Standards-based Trusted Identity Provider
  - SAML (SharePoint 2010 supports SAML 1.1 tokens and SAML 2.0 protocol)
  - WS-Federation
- Consider Custom Claim Providers



Trusted Identity Provider

WWW.TITUS.COM | © TITUS. ALL RIGHTS RESERVED |

Architecture for Authorization



WWW.TITUS.COM | © TITUS. ALL RIGHTS RESERVED |

Customer Requirements

- How do customers want to make use of Claims?

  Document Metadata + User Claims

  Example:
  Doc Classification + User's Security Clearance

  - Goal: Sensitive content sitting beside non-sensitive content
  - Fine Grained Access Control
  - Automation is critical and keep policies simple to start

WWW.TITUS.COM | © TITUS. ALL RIGHTS RESERVED |

Scenarios #1

- Claim: Employee Status
- Document Metadata: Classification (HBI, MBI, LBI)

If employee.status = FTE and document.classification = HBI
Then permit access to document

If employee.status = Contract and document.classification = HBI
Then deny access to document

WWW.TITUS.COM | © TITUS. ALL RIGHTS RESERVED |

Scenarios #2

- Claim: Group Membership
- Document Metadata: Project

If user belongs to GROUPX and belongs to GROUPY and document.project='eagle'

Then permit access to document

If user belongs to GROUPX and DOES NOT belong to GROUPY and document.project='eagle'

Then deny access to document

WWW.TITUS.COM | © TITUS. ALL RIGHTS RESERVED |

Scenarios #3

- Claim: Client Case Numbers
- Document Metadata: Document Case Number

If document.case=X AND client.casenumbers includes X
Then permit access to document

If document.case=X AND client.casenumbers DOES NOT includes X
Then deny access to document

WWW.TITUS.COM | © TITUS. ALL RIGHTS RESERVED |

Demonstration

WWW.TITUS.COM | © TITUS. ALL RIGHTS RESERVED |

Summary

- Authentication & Authorization - different but both important
  - Can use Claims today for Authentication in SharePoint 2010
- Claims are great tool for Enterprise-Grade Authorization to
  - Strengthen your Data Governance Strategies
  - Can do manually today in SharePoint 2010
  - Consider Automation with 3rd party applications – critical to consistent data governance
- Infrastructure and Planning Required
- Plan policies with business stakeholders – Keep Simple to Start!
- Connect with TITUS to bring Claims Based Authorization in SharePoint 2010 to Your Environment

Antonio Maio – antonio.maio@titus.com

SharePoint blog: www.titus.com/blog

WWW.TITUS.COM | © TITUS. ALL RIGHTS RESERVED |

More SharePoint Security. Less Effort.

Question and Answer – Thank You

Antonio Maio
antonio.maio@titus.com
Senior Product Manager, SharePoint Solutions

Check out our blog: http://www.titus.com/blog
Follow on Twitter: @AntonioMaio2

TITUS

Configuration: Active Directory

- Define which attributes in AD need values returned as claims for users
  - Fill in those values
  - Consider multi-value fields
- Use default schema and existing attributes
  - Ex. organizationalStatus
- Add new attributes to AD Schema if required

WWW.TITUS.COM | © TITUS. ALL RIGHTS RESERVED |

Configuration: ADFS v2

1. Install ADFSv2 as a Federation Server and in IIS create a self-signed certificate
2. Create a New Federation Service – use the wizard
   - Take note of the 'Federation Service Name' – https://sp-server-2010.sp.local
3. Add a Claims Description
   - Selecting claims to be sent back to SharePoint; not mapping to AD attributes yet
   - Take note of claims type URL – http://schemas.sp.local/EmployeeStatus
4. Add a Relying Party Trust
   - Selected WS-Federation Passive Protocol
   - Relying Party URL = 'Federation Service Name' + '/_trust/'
   - Relying Party Trust Identifier = urn:ServerName:application
     urn:sp-server-2010.sp.local:sharepoint2010
5. Create Claims Rules for the Relying Party
   - Mapping AD attributes to Claims – consider the Claims Rule Language
6. View and Export ADFSv2 Token Signing Certificate - c:\adfs20Certificate.cer

WWW.TITUS.COM | © TITUS. ALL RIGHTS RESERVED |

Configuration: Transforming Claims

- ADFSv2 Claims Rule Language
- Example: Send custom claim “EmployeePermission” with value “FullControl” only if user belongs to “SeniorManagement” group and if employee’s organization “Titus”

C1:[type == “http://schemas.microsoft.com/ws/2008/06/identity/claims/role”, value == “SeniorManagement”]

&&

C2:[type == “http://schemas.microsoft.com/ws/2008/06/identity/claims /organization”, value == “Titus”]

=> issue(type = “http://schemas.qalabs.local/EmployeePermission”, value = “FullControl”)

- Sending a new claim based in the value of two existing AD attributes

WWW.TITUS.COM | © TITUS. ALL RIGHTS RESERVED |

Configuration: Transforming Claims

- ADFSv2 Claims Rule Language
- Example: Send custom claim “ClearanceCaveatPolicy” with value that concatenates the Clearance claim and Caveat claim

```
C1:[type == “http://schemas.sp.local/Clearance”]
&&
C2:[type == “http://schemas.sp.local/Caveats”]
=> issue(type = “http://schemas.sp.local/ClearanceCaveat”, value = c1.value + c2.value);
```

- Simple case of AND’ing values together to enforce a policy
- For more information: http://technet.microsoft.com/en-us/library/dd807118(WS.10).aspx

WWW.TITUS.COM | © TITUS. ALL RIGHTS RESERVED |

Configuration: SharePoint 2010 Server

1. Create a new Web Application in Central Admin
   - Select Claims Based Authentication, Use port 443 and SSL
   - Use NTLM as Claims Authentication Type to start
   - Ensure public URL matches the one in the ADFSv2 certificate – trust between this web app and the ADFSv2 server
   - Do not create a site collection yet
2. In IIS, SharePoint site that uses SSL, select Edit Bindings to validate settings
3. Run PowerShell script to map claim types

WWW.TITUS.COM | © TITUS. ALL RIGHTS RESERVED |

Configuration: Use PowerShell to Map Claim Types in SharePoint

```
# Make sure the claim types are properly defined in the ADFS server
$map = New-SPClaimTypeMapping -IncomingClaimType
"http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress" -IncomingClaimTypeDisplayName "EmailAddress" -
SameAsIncoming
$map2 = New-SPClaimTypeMapping -IncomingClaimType "http://schemas.microsoft.com/ws/2008/06/identity/claims/role" -
IncomingClaimTypeDisplayName "Role" -SameAsIncoming
$map3 = New-SPClaimTypeMapping -IncomingClaimType "http://schemas.sp.local/EmployeeStatus" -
IncomingClaimTypeDisplayName "EmployeeStatus" -SameAsIncoming

# The realm will identify the web app in ADFS. It is generally created in the form "urn:foo:bar"
$realm = "urn:sp-server-2010.sp.local:sharepoint2010"

# Use the certificate that has been exported from the ADFS server
$cert = New-Object System.Security.Cryptography.X509Certificates.X509Certificate2("c:\adfs20Certificate.cer")

# The url below will tell SharePoint where to redirect to in order to authenticate with the STS
# so this should have the ADFS url, plus the protocol (Windows integrated security - "/adfs/ls")
$signinurl = "https://adfs20.sp.local/adfs/ls"

# Adds the STS (AD FS 2.0) to SharePoint
$ap = New-SPTrustedIdentityTokenIssuer -Name "ADFS20 Provider" -Description "SharePoint secured by ADFS20" -realm
$realm -ImportTrustCertificate $cert -ClaimsMappings $map,$map2,$map3 -SignInUrl $signinurl -IdentifierClaim
$map.InputClaimType

# The certificate imported from the ADFS should be added to the trusted store
New-SPTrustedRootAuthority -Name "ADFS Token Signing Root Authority" -Certificate $cert
```


WWW.TITUS.COM | © TITUS. ALL RIGHTS RESERVED |

Configuration: Add/Map a New Claim Type
(after initial config)

```
# Adding a new claim mapping to an existing provider in SharePoint
$ti=Get-SPTrustedIdentityTokenIssuer

$ti.ClaimTypes.Add("http://schemas.sp.local/TitusDepartment")

$ti.Update()

$TitusDepartmentClaim=New-SPClaimTypeMapping -IncomingClaimType
"http://schemas.sp.local/TitusDepartment"-IncomingClaimTypeDisplayName
"TitusDepartment" –SameAsIncoming

Add-SPClaimTypeMapping –Identity $TitusDepartmentClaim -TrustedIdentityTokenIssure $ti
```


WWW.TITUS.COM | © TITUS. ALL RIGHTS RESERVED |

Configuration: Remove a Claim Type
(after initial config)

```
#Remove a mapped claim type from an existing provider in SharePoint
$ti=Get-SPTrustedIdentityTokenIssuer

foreach ($c in $ti.ClaimTypeInformation) { if ($c.DisplayName –eq “TitusDepartment”)
{ $mapping = $c; } }

Remove-SPClaimTypeMapping –Identity $mapping –TrustedIdentityTokenIssuer $ti

$ti.ClaimTypes.Remove(“http://schemas.sp.local/TitusDepartment”)

$ti.Update()
```


WWW.TITUS.COM | © TITUS. ALL RIGHTS RESERVED |

Configuration: SharePoint 2010 (Cont'd)

4. In Central Admin, access the Authentication Providers for your web application
    - Click Default and select Trusted Identity Provider and ADFSv2 Provider (or SAML Provider)
5. Create your site collection
    - If you have multiple web applications, ensure you select the correct one
6. Create Sites and Libraries
7. Deploy your Application or 3rd Party Application that makes use of Claims for Authorization

WWW.TITUS.COM | © TITUS. ALL RIGHTS RESERVED |