TECHNICAL IMPLEMENTATION

SWITCH AAI / SHAREPOINT /ADFS

AGENDA

- Introduction
- Authentication
- Autorisation
- External Users
- User Profile Management
- Miscellaneous
- Question

INTRODUCTION

ABOUT ME

Joël Hasler
Head of DataCenter

Bachelor of Science in Computer Science
joel.hasler@ioz.ch
http://www.ioz.ch

INTRODUCTION

ABOUT IOZ

Organizational and Consulting

ioz Informations Organisations Zentrum AG

Technical (Development, Hosting, Installation)

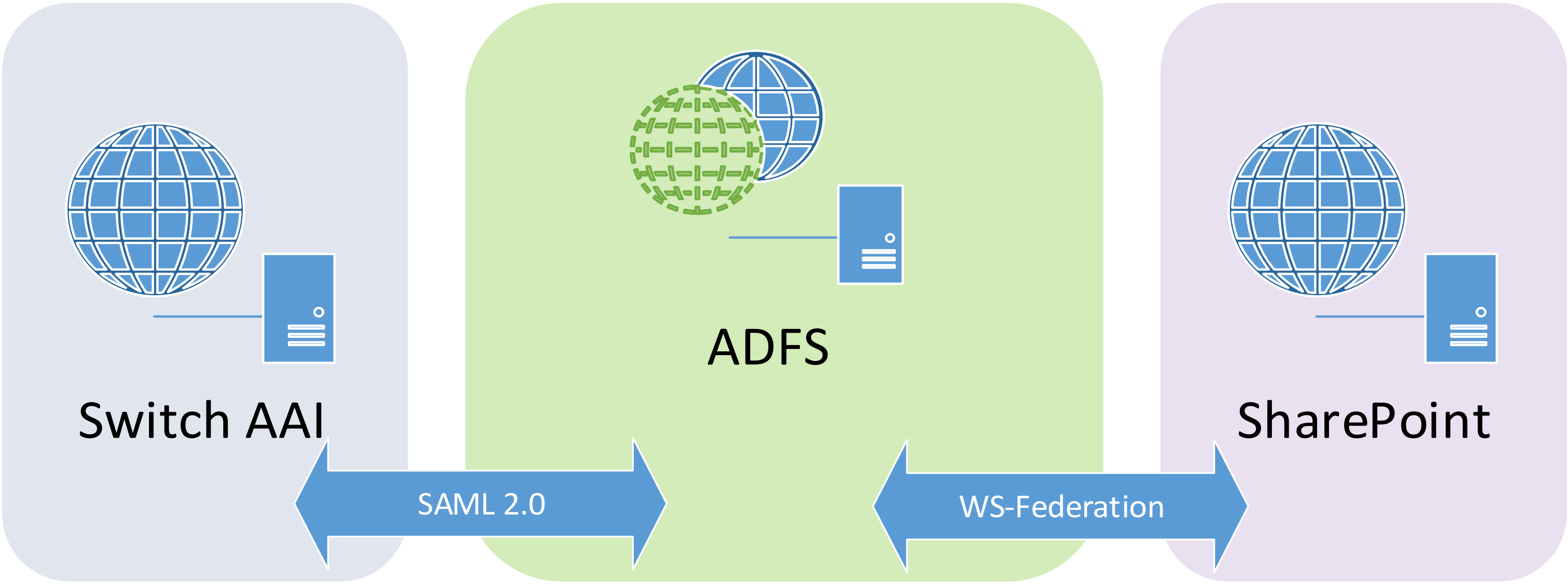
ioz DataCare AG

Certifications:

Microsoft Partner
Gold Portals and Collaboration
Silver Content Management
Silver Midmarket Solution Provider

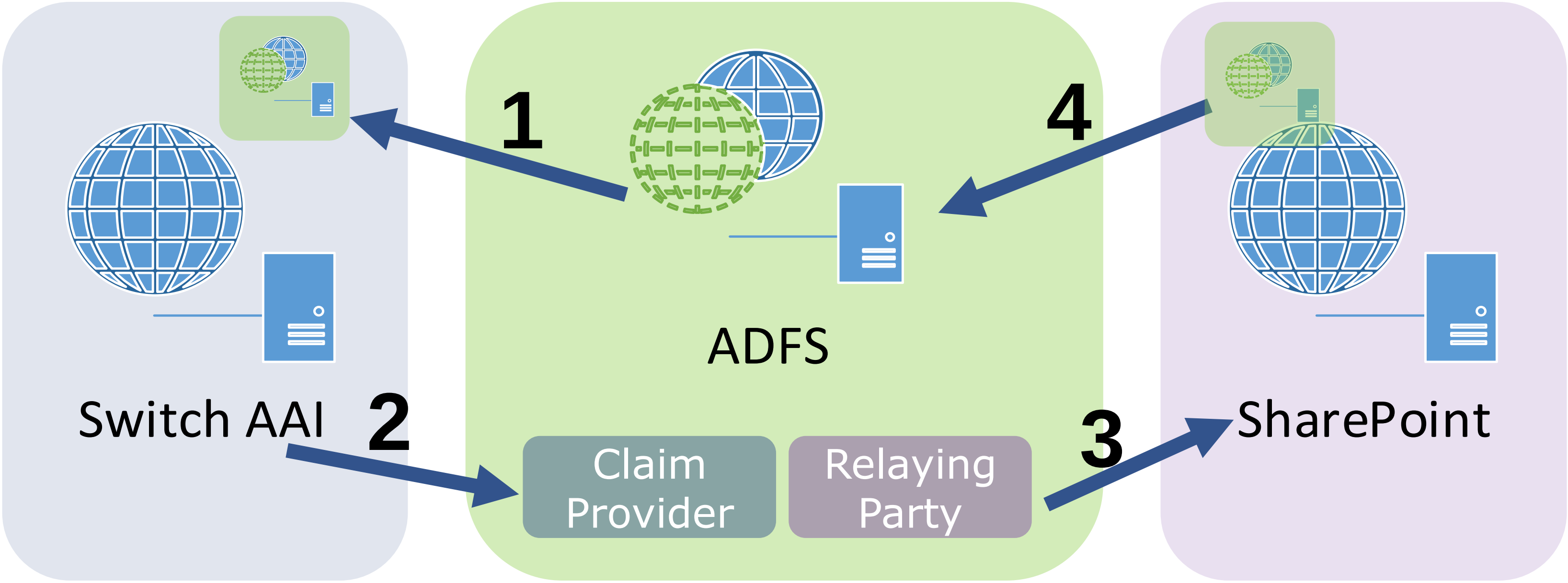
SQS

HOW TO AUTHENTICATE AGAINST SWITCH AAI?

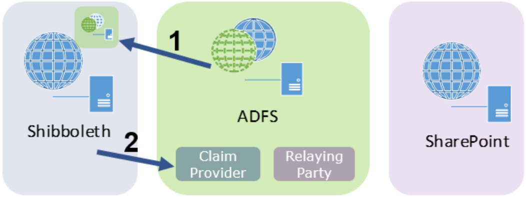


AUTHENTICATION

HOW TO AUTHENTICATE AGAINST SWITCH AAI?



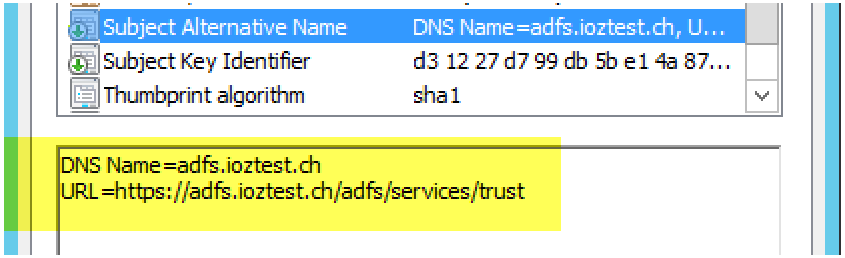
AUTHENTICATION



1. REGISTER SERVICE PROVIDER IN AAI

ADFS Side

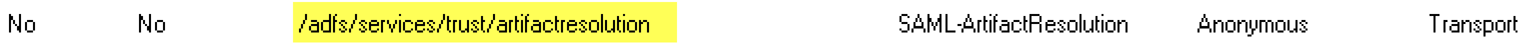
- Correct Certificate (Link: Certificate Requirements (AAI))
  - STS → Public Certificate (ex. Quovadis)
  - Service Communication → Self Signed



Subject Alternative Name	DNS Name=adfs.ioztest.ch, U...
Subject Key Identifier	d3 12 27 d7 99 db 5b e1 4a 87...
Thumbprint algorithm	sha1

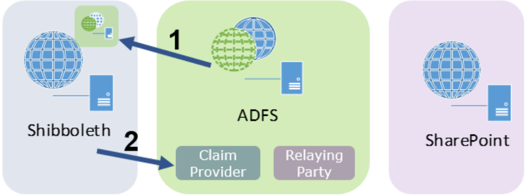
```
DNS Name=adfs.ioztest.ch
URL=https://adfs.ioztest.ch/adfs/services/trust
```

  - Federation Service Identifier (https not http)
- Disable Artifact Resolution Profile



No	No	/adfs/services/trust/artifactresolution	SAML-ArtifactResolution	Anonymous	Transport

AUTHENTICATION



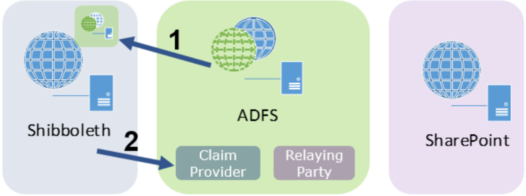
1. REGISTER SERVICE PROVIDER AN AAI

AAI Side

- Wizard mode do not work for ADFS registration
- Need to copy/paste ADFS Metadata XML Content
- Take care about Service Location
  - Only register HTTP-POST Binding
    urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST

→Problem with Back Channel Request and Artifact Profile

AUTHENTICATION



2. ADD IDP’S ON ADFS

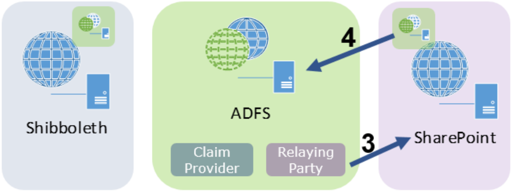
Problem:

- The Metadata File from AAI include all IDP’s in one XML File
- ADFS can only import one IDP per File

Solution

- SILA → CodePlex Solution
- Extract each IDP and import it into ADFS

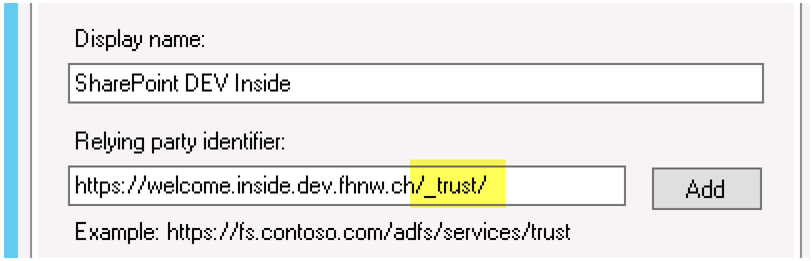
AUTHENTICATION



3. CREATE RELAYING PARTY ON ADFS

Important Steps

- Each WebApp URL need a Relaying Party
  → FHNW has 4 WebApps
- Relaying party identifier …/_trust/



Display name:

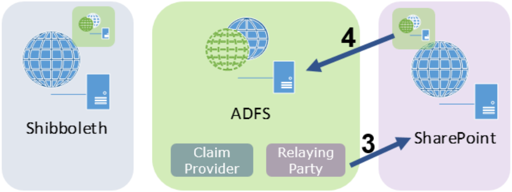
SharePoint DEV Inside

Relying party identifier:

https://welcome.inside.dev.fhnw.ch/_trust/

Example: https://fs.contoso.com/adfs/services/trust

AUTHENTICATION



4. CONFIGURE SHAREPOINT FOR ADFS

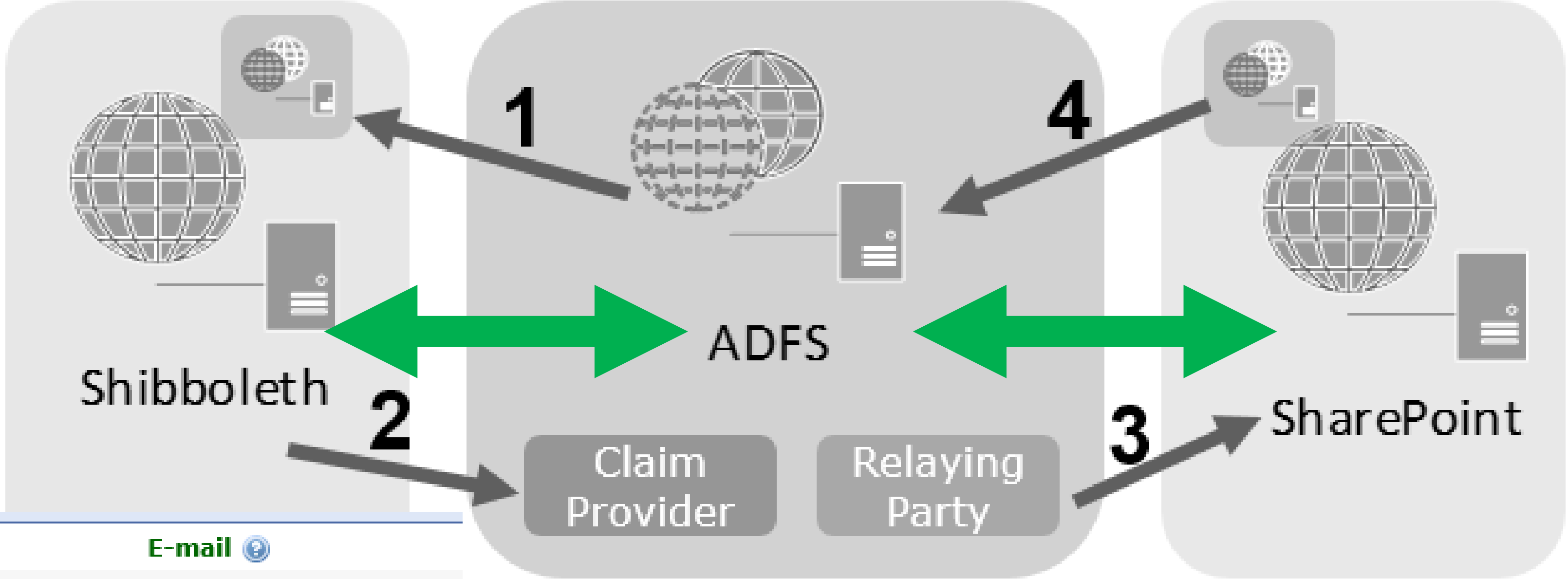
Required information from Step 3

- Token Certificate (.cer → without Private Key)
- STS URL
- Realm
- Attributes

New SPTrustedIdentityTokenIssuer

- Only with PowerShell
- One for all WebApps

AUTHENTICATION



E-mail

Home organization

Home organization type

Affiliation

Unique ID

Surname

Given name

Targeted ID/Persistent ID

Missing: Attribute Mapping

AUTHORIZATION

CLAIM RULES LANGUAGE

Condition / Issuance

```
c:[Type == "http://contoso.com/department"]
 =>issue(Type = “http://adatum.com/department”, Value = c.Value);
```

http://social.technet.microsoft.com/wiki/contents/articles/4792.understanding-claim-rule-language-in-ad-fs-2-0.aspx

Example

- How is Attribute HomeOrg passed from Shibboleth to SharePoint

AUTHORIZATION

ACCESS RIGHTS IN SHAREPOINT

There are no AD Groups → But we have Claim with Attributes ;-)

Attribute Affiliation

- Mapped in SharePoint as http://schemas.microsoft.com/ws/2008/06/identity/claims/role
- Set Permission based on Attribute Values
- Example:
    - All Users which have “staff” as Value in the Claim Attribute Affiliation have write Access to Site XY

AUTHORIZATION

ACCESS RIGHTS IN SHAREPOINT

Requirements

- Other faculties should also have access to SharePoint

Problem

- Affiliation has to be unique

Idea:

- Combination of Affiliation Value with Home Organization
- Ex.: staff@fhnw.ch

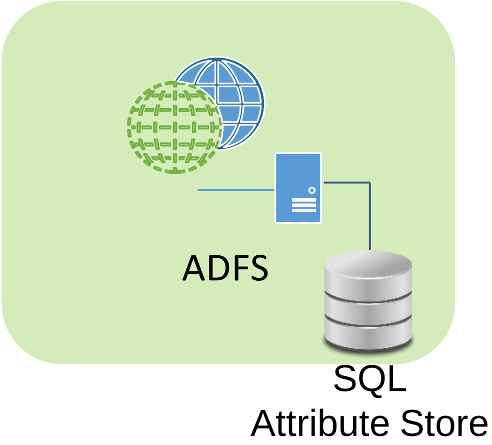
ACCESS RIGHTS IN SHAREPOINT

Implementation

- Claim Rule Language can modify Claim Values
  - Can use alternative Attribute Stores (LDAP and SQL)
  - SQL Attribute Store to add extra intelligents over a Stored Procedure

Claim Input ex.

- Affiliation: staff
- HomeOrg: fhnw.ch
- max.muster@fhnw.ch

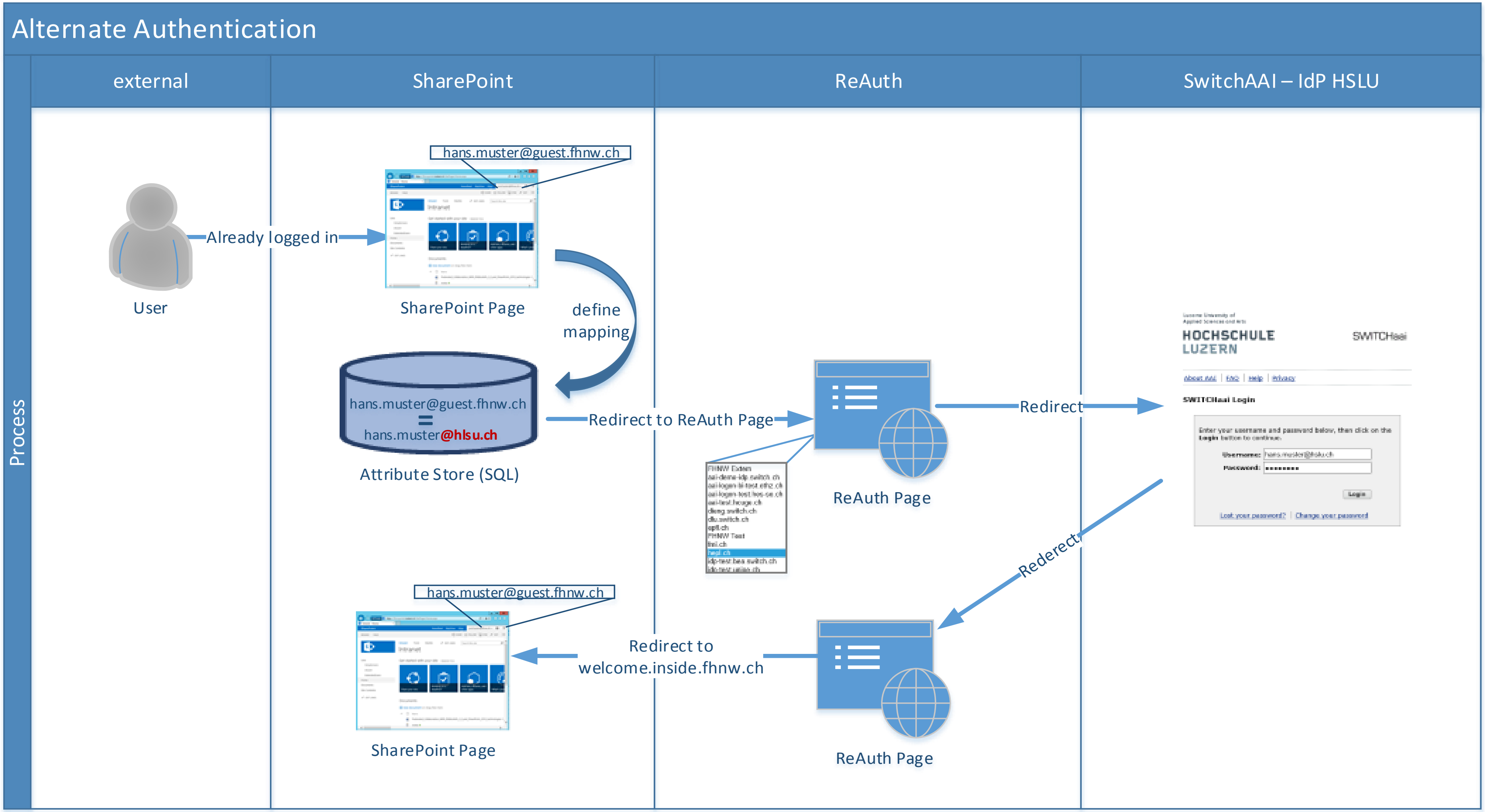


Outputs ex.

- staff@fhnw.ch
- students@fhnw.ch
- member@fhnw.ch
- affiliate@fhnw.ch
- unauthorized

Link: Claims Encoding

EXTERNAL USERS - ALTERNATIVE LOGIN

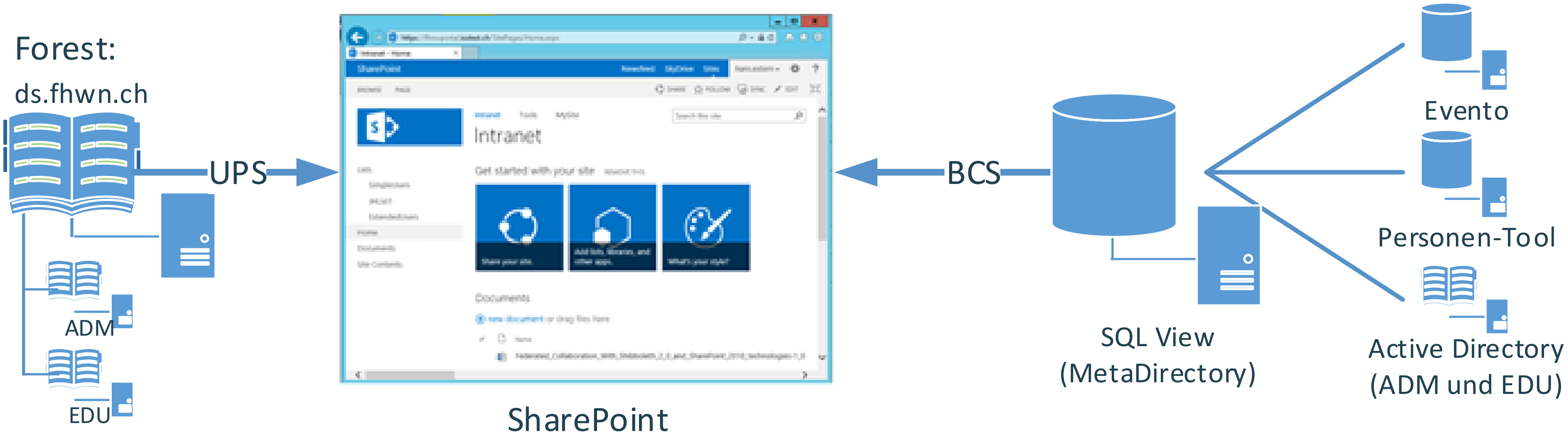


Enter your username and password below, then click on the **Login** button to continue.

Username: hans.muster@hslu.ch
Password: ●●●●●●●●

USER PROFILE MANAGEMENT

OVERVIEW (STAFF AND STUDENT)

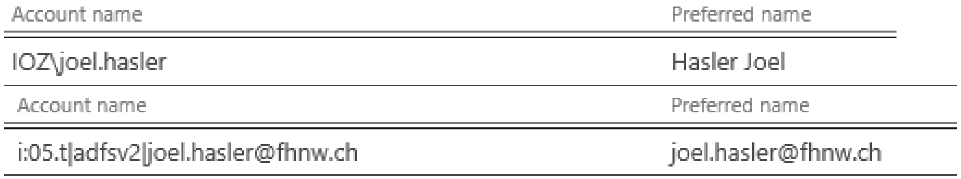


USER PROFILE MANAGEMENT

PROBLEMS

BCS

- Require Full AD User → AD Import
- Double user Profiles → Merge over Claim Identifier



Account name	Preferred name
IOZ\joel.hasler	Hasler Joel

Account name	Preferred name
i:05.t|adfsv2|joel.hasler@fhnw.ch	joel.hasler@fhnw.ch

UPS

- Not possible to run a sync per connection → run in parallel
- AD sync has complete first → BCS Import failed
- Run UPS Sync twice over PowerShell

MISC

Windows Authentication

- Problem: Need for SharePoint internal User → ex. Search
- Solution: extend WebApp and Crawl default URLs

Self Service Portal

- Req.: Ability for external Users to change Password and edit Profile
- Solution: Custom SharePoint Solution only for external users

Claim Authentication

- Problem: People Picker cannot validate if user exist or not
- Solution: Custom Claim Provider check against UPS

QUESTIONS