Informatikdienste der ETH Zürich

Active Directory
Federation Service
Agenda

- Active Directory Federation Service
- Claims-based authentication
- Interaction
- ADFS Infrastructure
ADFS

- ADFS (Active Directory Federation Service)
  - SAML
    Security Assertion Markup Language
    - 2001 developed by the OASIS-Konsortium
    - XML-based-Framework
      Exchange of authentication and authorization Information
    - Goal
      single sign-on (SSO), distributed transaction, authorization
      «mostly for WebServices»
ADFS

OASIS

Advancing open standards for the information society

The official name is the Security Services Technical Committee (SSTC).

It is sometimes unofficially called the "SAML TC" or the "SSTC/SAML committee".

**TC Sponsors**

- Avaya, Inc.
- Covisint, a Compuware Company
- EMC
- Hewlett-Packard
- IBM
- Jericho Systems
- Microsoft
- Nokia Corporation
- Oracle
- Ping Identity Corporation
- Primeon Technologies, Inc.
- Red Hat
- SAP AG
- The Boeing Company
- Tiani "Spirit" GmbH
- Veterans Health Administration

*Organizations listed above are OASIS Sponsor-level members who have representatives serving on this TC.*
Agenda

- Active Directory Federation Service
- Claims-based authentication
- Interaction
- ADFS Infrastructure
Claims-based authentication

- components
  - Identity Provider (Idp / IP)
  - Service Provider (SP/ RP)
  - Discovery Service (WAYF)
    - optional component
Claims-based Authentication

- Shibboleth
  - LDAP
  - relational database

- AD Federation
  - Active Directory
  - LDAP
  - SQL Server
Key Concepts

User / Subject /Principal

The Security Token Contains claims about the user
For example:
- Name
- Group membership
- User Principal Name (UPN)
- Email address of user
- Email address of manager
- Phone number
- Other attribute values

Signed by issuer

Issuer IP-STS
Identity Provider (IP)
Security Token Service (STS)

Requests token for AppX

Issues Security Token crafted for AppX

ST

Security Token “Authenticates” user to the application

AppX
Relying party (RP)/ Resource provider

Trusts the Security Token from the issuer

Active Directory
Claims-based authentication

- **Why ADFS?**
  - Sharepoint claims-based authorisation
  - New Microsoft applications
    - such SMB 3.0 Claim Aware
  - Integration of Dynamic Access Control
  - Form-based Authentication
  - Windows integrated Authentication
  - use of external non-SWITCH AAI resources or Idp
Agenda

- Active Directory Federation Service
- Claims-based authentication
- Interaction
- ADFS Infrastructure
Working with Partners

Our Claims-aware app

Redirected to partner STS requesting ST for partner user

Return ST for consumption by your STS

Return new ST

Send Token

Return cookies and page

Our AD FS 2.0 STS

App trusts STS

Your STS trusts your partner’s STS

Partner AD FS 2.0 STS & IP

Active Directory

Authenticate

Browse app

Not authenticated

Redirect to your STS

Home realm discovery

Redirected to partner STS requesting ST for partner user

Return ST for consumption by your STS

Redirected to your STS

Return new ST

Process token
Intraction

- Authentication Shibboleth SWITCH AAI
  - Register ADFS as a SP in SWITCH AAI
**Intraction**

- **Authentication Shibboleth SWITCH AAI**
  - Register the Application such as SharePoint in ADFS as an SP/RP
Intraction

- Authentication Shibboleth SWITCH AAI
  - Add the required Idp’s to ADFS and configure the claim rules
    (no self-signed certificates)
Interaction

- Google, Facebook, Yahoo! and Microsoft Live ID
  - Azure ACS (Access Control Service) with **SharePoint 2010**
    - Request a Namespace in Azure ACS

![Diagram](image.png)
Interaction

- Google, Facebook, Yahoo! and Microsoft Live ID
  - Azure ACS (Access Control Service) with **SharePoint 2010**
    - Register the ADFS Server in Azure ACS
Interaction

- Google, Facebook, Yahoo! and Microsoft Live ID
  - Azure ACS (Access Control Service) with SharePoint 2010
    - Register your Sharepoint in Azure ACS

![Diagram showing interaction between ADFS, Azure ACS, and SharePoint 2010]
Interaction
Interaction

Sign in to My Application

Sign in using your account on:

- **Windows Live ID**
- **Yahoo!**
- **Facebook**
- **Google**
- **Contoso Corp.**

---

SharePoint 2010

Azure ACS
Interaction

Anmelden

ETH Zürich Test DT

Für die Website, auf die Sie zugreifen möchten, ist eine Anmeldung erforderlich. Wählen Sie aus der folgenden Liste Ihre Organisation aus.

- EPFL EPF Lausanne
- ETH Zürich AAI
- ETH Zürich Production
- ETH Zürich Resource
- FMH - Friedrich Miescher Institute
- PSI_achst

© 2013 ETH Zürich | Impressum | 24.01.2013
Interaction

- Google, Facebook, Yahoo! and Microsoft Live ID
  - Azure ACS (Access Control Service) with SharePoint 2013
    - Request a Namespace in Azure ACS
Interaction

- Google, Facebook, Yahoo! and Microsoft Live ID
  - Azure ACS (Access Control Service) with SharePoint 2013
    - Register your SharePoint in Azure ACS
Interaction

- Google, Facebook, Yahoo! and Microsoft Live ID
  - Azure ACS (Access Control Service) with SharePoint 2013
    - SharePoint 2013 supports more than 1 Claim provider for a zone
Interaction

Sign in to My Application

Sign in using your account on:

- Windows Live ID
- Yahoo!
- Facebook
- Google
- Contoso Corp.

SharePoint 2013
Interaction

Anmelden

ETH Zürich Test DT

Für die Website, auf die Sie zugreifen möchten, ist eine Anmeldung erforderlich. Wählen Sie aus der folgenden Liste Ihre Organisation aus.

<table>
<thead>
<tr>
<th>ETH Zürich AAI</th>
</tr>
</thead>
<tbody>
<tr>
<td>ETH Zürich Production</td>
</tr>
<tr>
<td>ETH Zürich Resource</td>
</tr>
<tr>
<td>FMI - Friedrich Miescher Institute</td>
</tr>
<tr>
<td>PSI_achat</td>
</tr>
</tbody>
</table>

© 2012 ETH Zürich | Impressum | 24.01.2013

Contoso Corp.
Interaction

Sign in to My Application

Sign in using your account on:

- Windows Live ID
- Yahoo!
- Facebook
- Google
- Contoso Corp.

SharePoint 2013

Namespace Google
Namespace LiveID
Namespace OpenID
Agenda

- Active Directory Federation Service
- Claims-based authentication
- Interaction
- ADFS Infrastructure
Planing ADFS

- Proxy Server / STS Server
  - Form-Based Authentication / Windows Integrated Authentication

- Certificates
  - SSL, token signing, token encryption

- WID (Windows Internal Database) or SQL

- Administration IP / RP

- Attribute store
WWW
Form-Based Authentication

DMZ
ADFS Proxy
ADFS Proxy RES
SharePoint

Intranet
Windows Integrated Authentication
ADFS STS
ADFS STS RES
Shibboleth ETH Zürich

ETH Zürich
Swiss Federal Institute of Technology Zürich