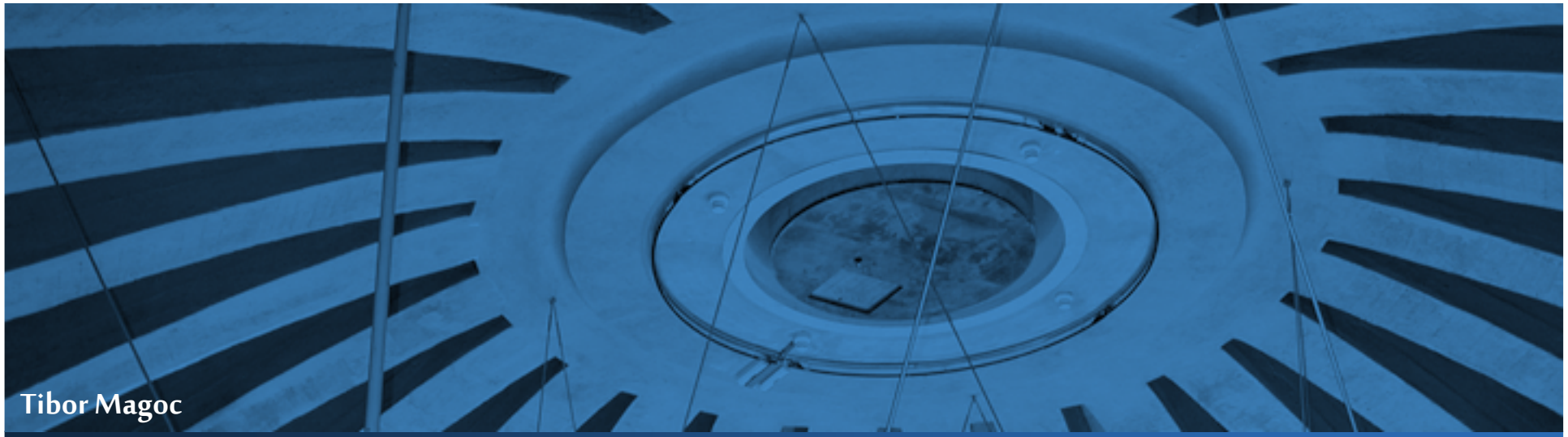
ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Informatikdienste

Informatikdienste der ETH Zürich

Active Directory
Federation Service



Tibor Magoc

Agenda

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

ADFS

- ADFS (Active Directory Federation Service)
  - **SAML**

    Security **A**ssertion **M**arkup **L**anguage

    - 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
Primeton 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

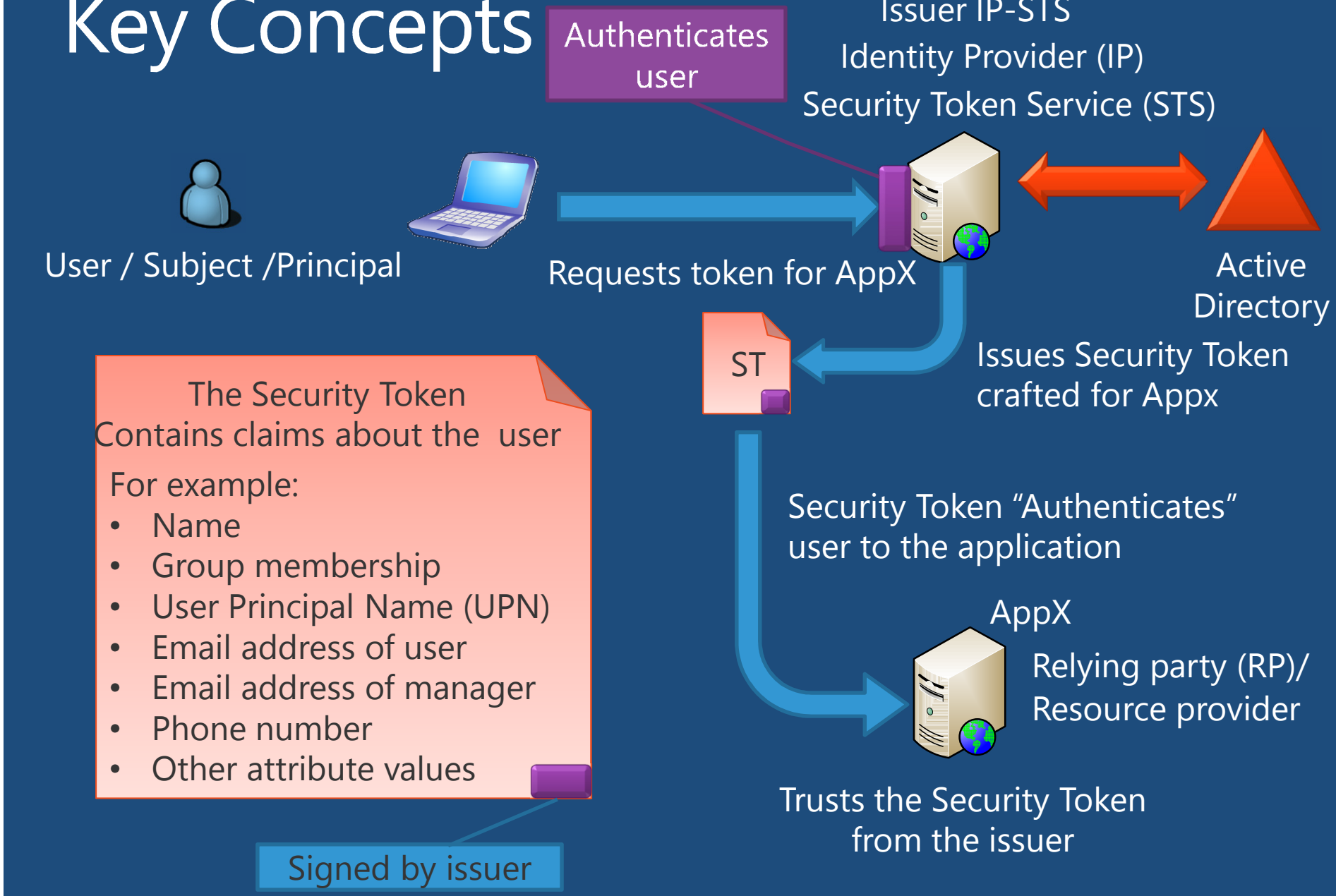
- components
  - Identity Provider (Idp / IP)
  - Service Provider (SP/ RP)
  - Discovery Service (WAYF)

    optional component

Claims-based Authentication

- Shibboleth
  - **LDAP**
  - relational database
- AD Federation
  - **Active Directory**
  - LDAP
  - SQL Server

Key Concepts



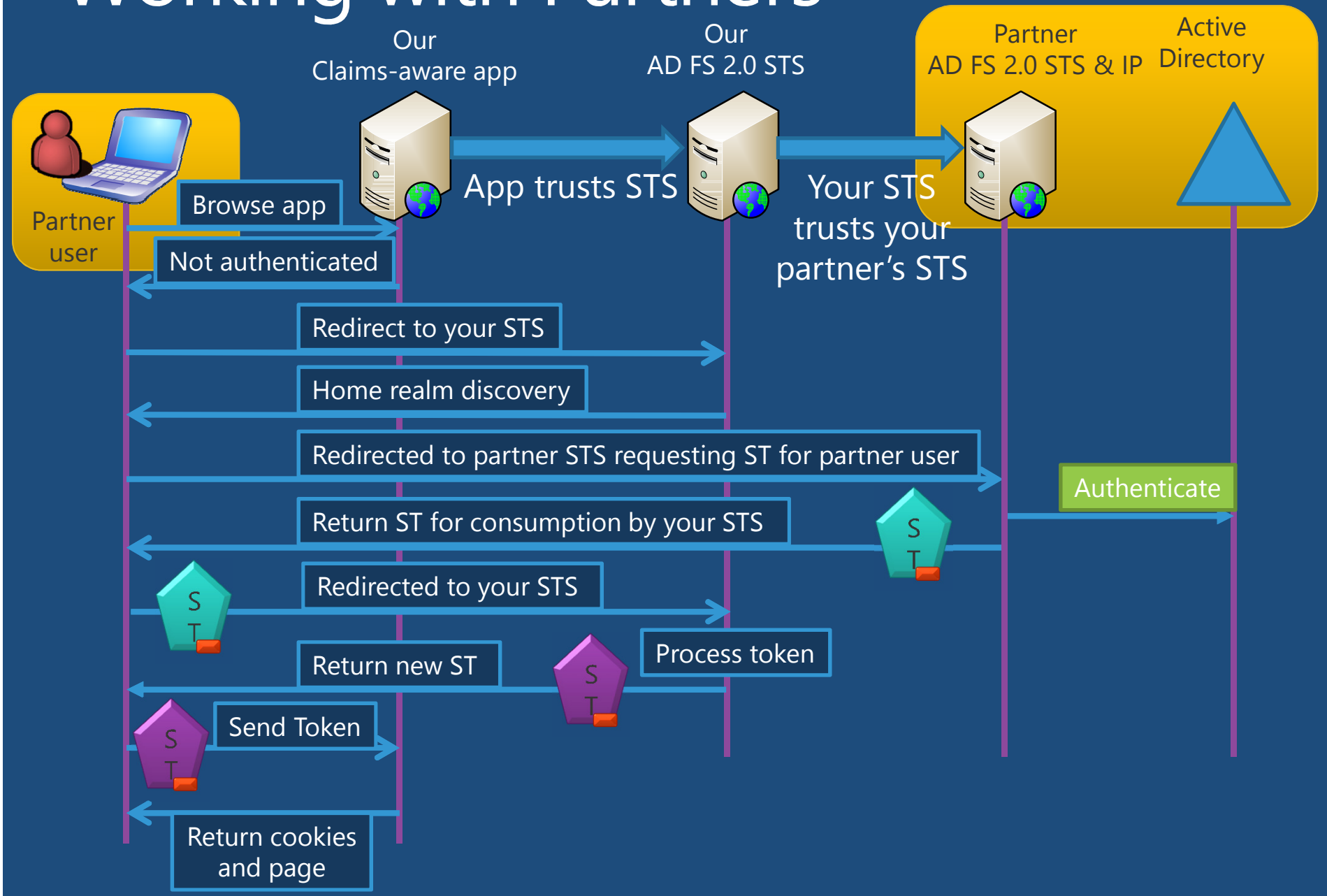
Claims-based authentication

- **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

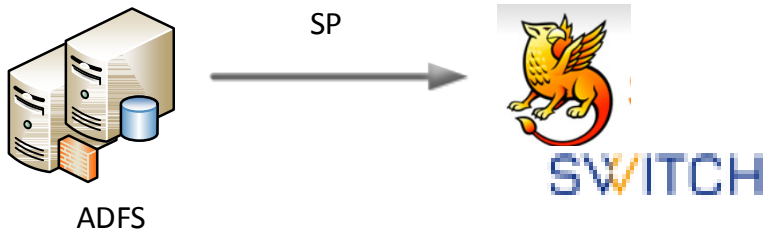
- Active Directory Federation Service
- Claims-based authentication
- **Interaction**
- ADFS Infrastructure

Working with Partners



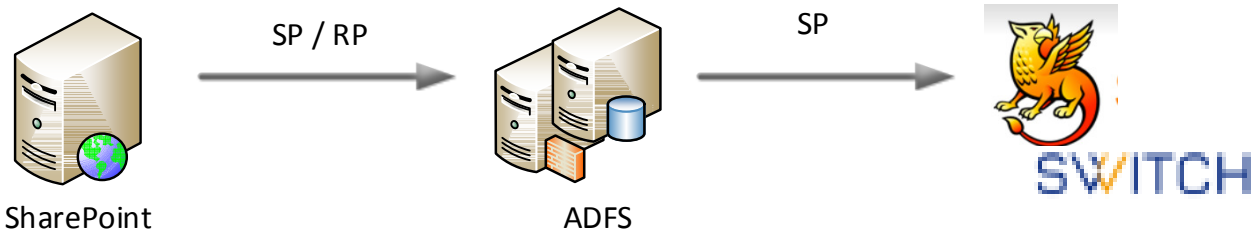
Intraction

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



Intraction

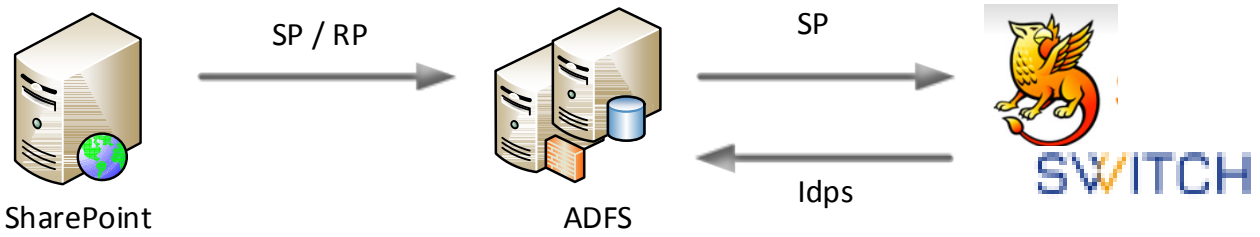
- Authentication Shibboleth SWITCH AAI
  - Register the Application such as SharePoint in ADFS as an SP/RP



Intraction

- Authentication Shibboleth SWITCH AAI

  - Add the required Idp's to ADFS and configure the claim rules (no self-signed certificates)

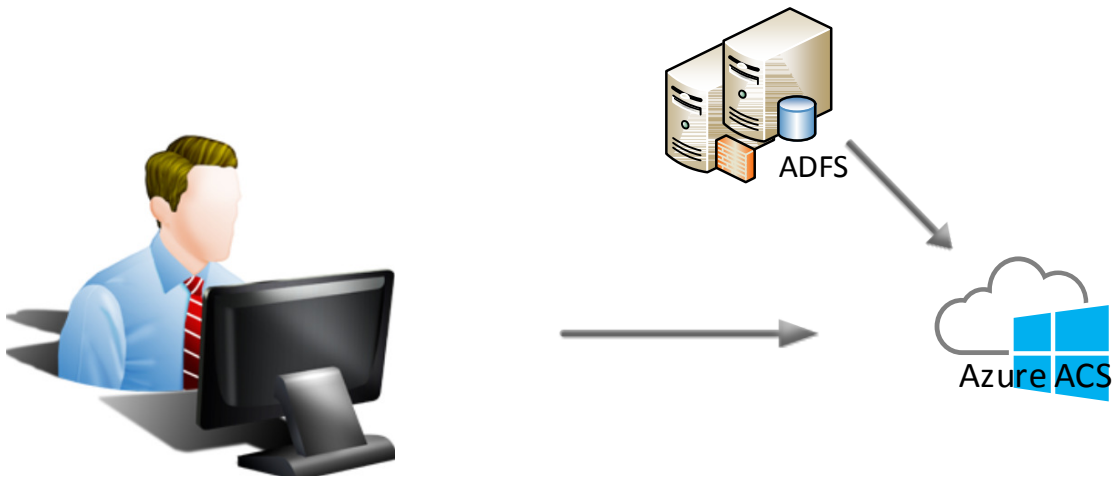


Interaction

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

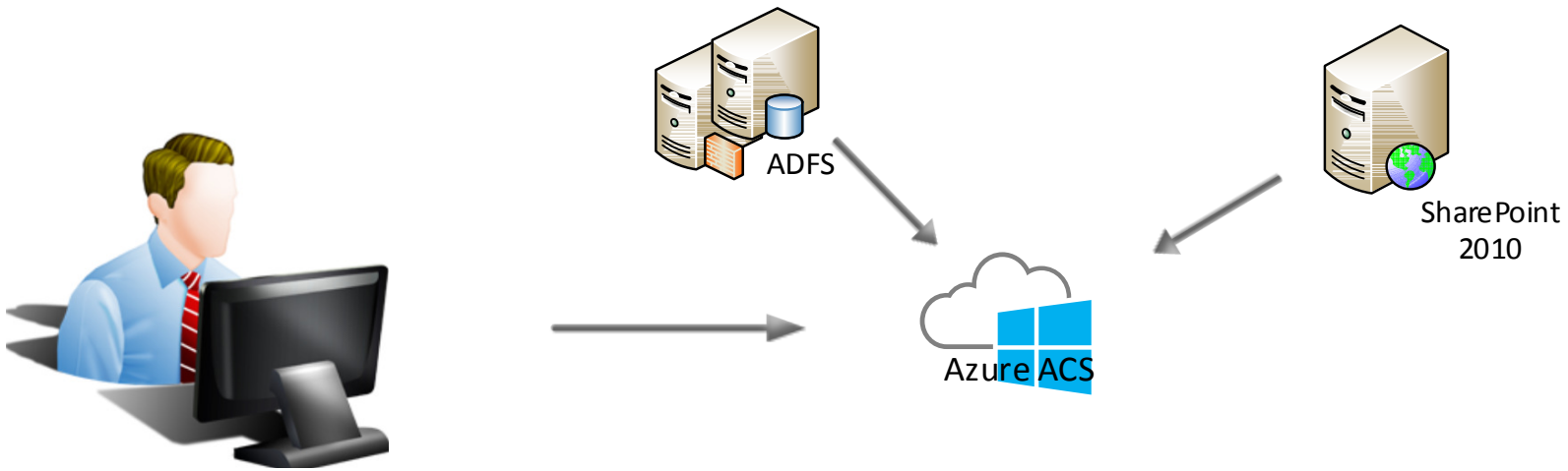
Interaction

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

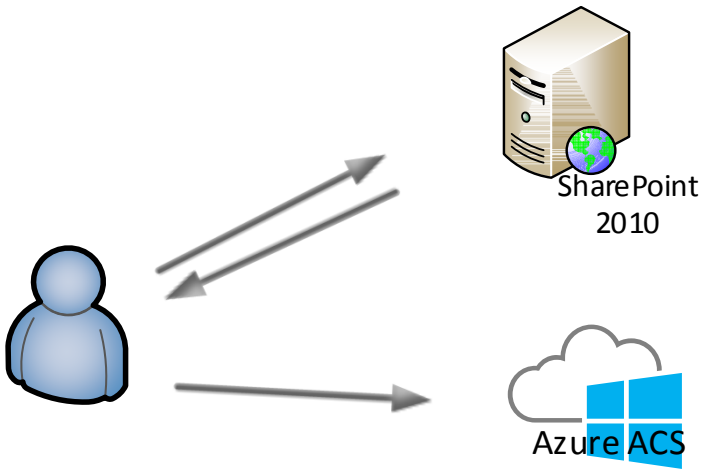


Interaction

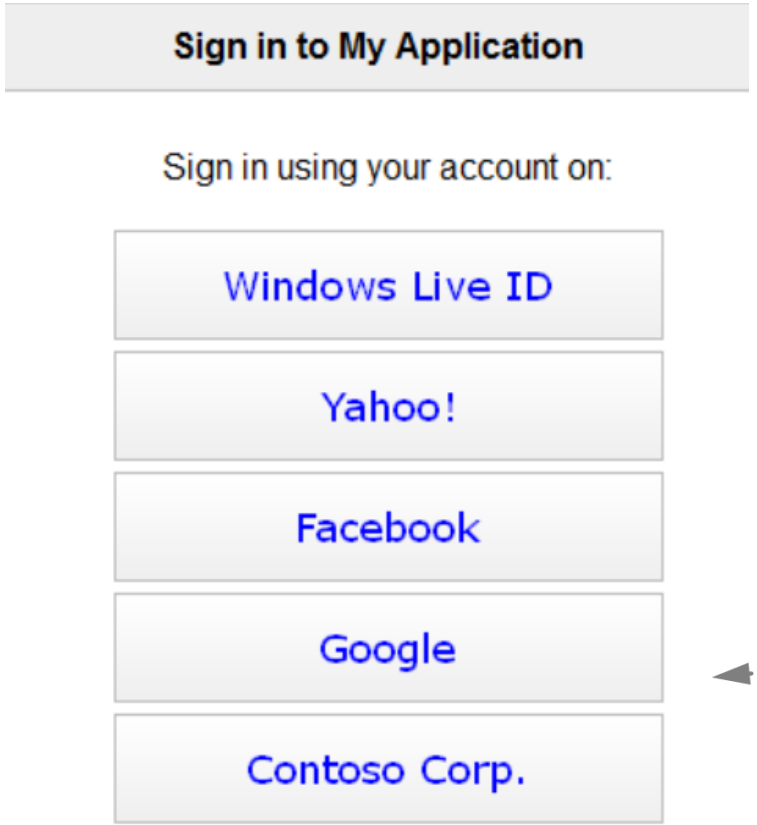
- Google, Facebook, Yahoo! and Microsoft Live ID
  - Azure ACS (Access Control Service) with **SharePoint 2010**
    - Register your Sharepoint in Azure ACS

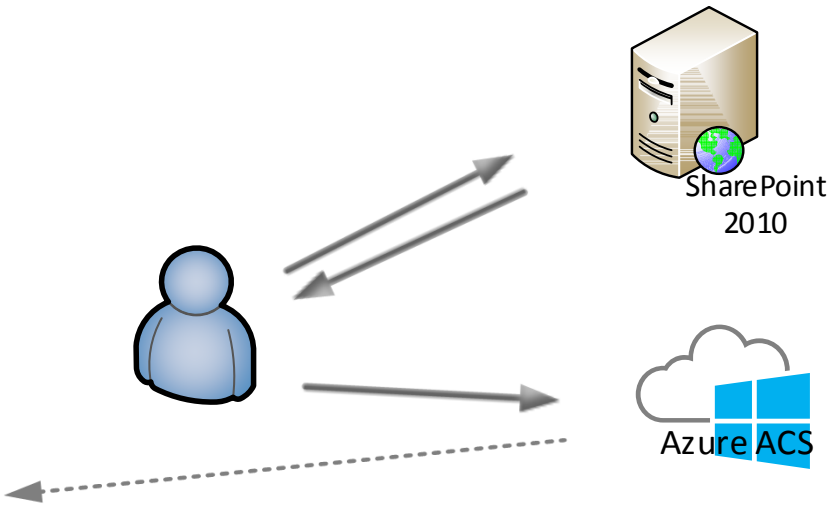


Interaction

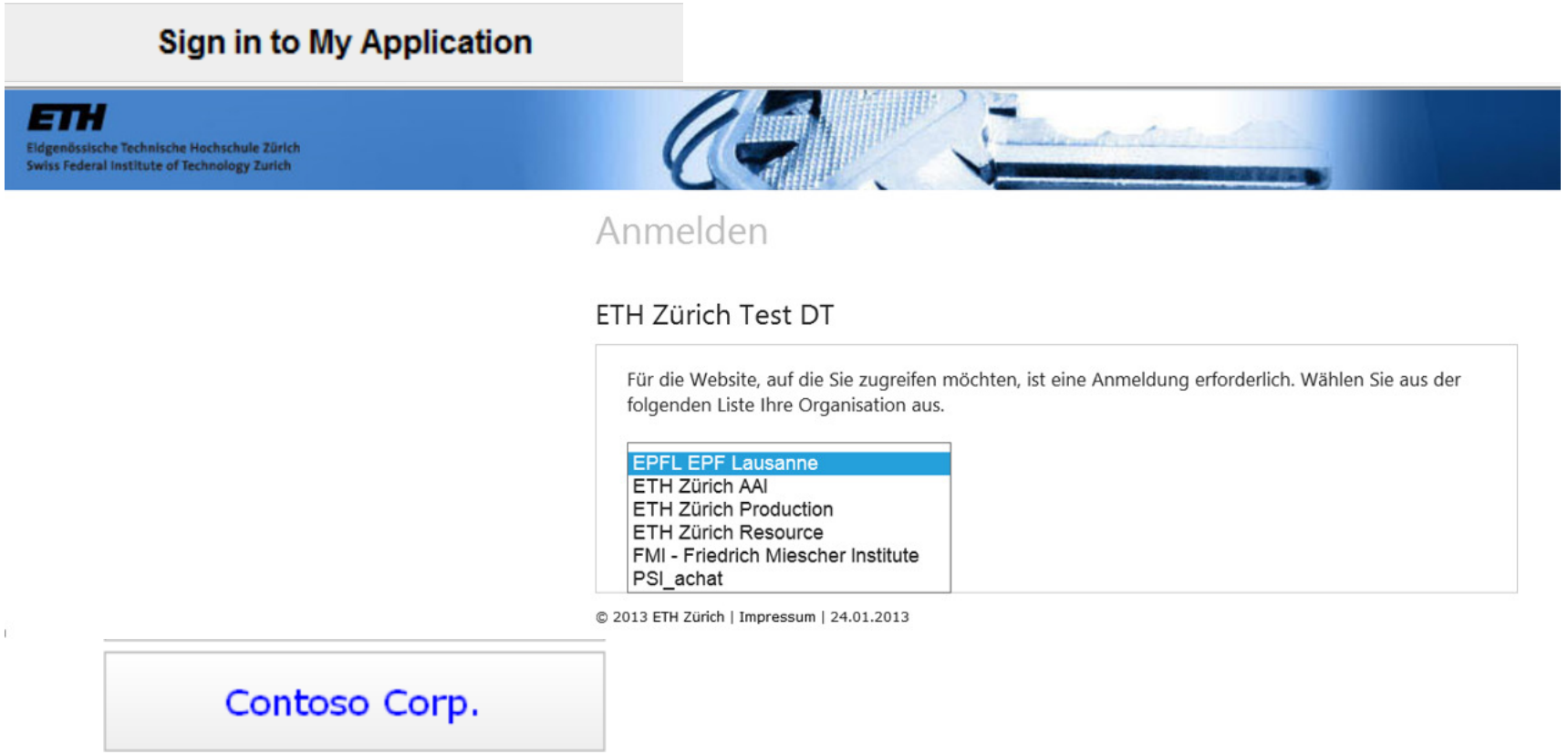


Interaction





Interaction

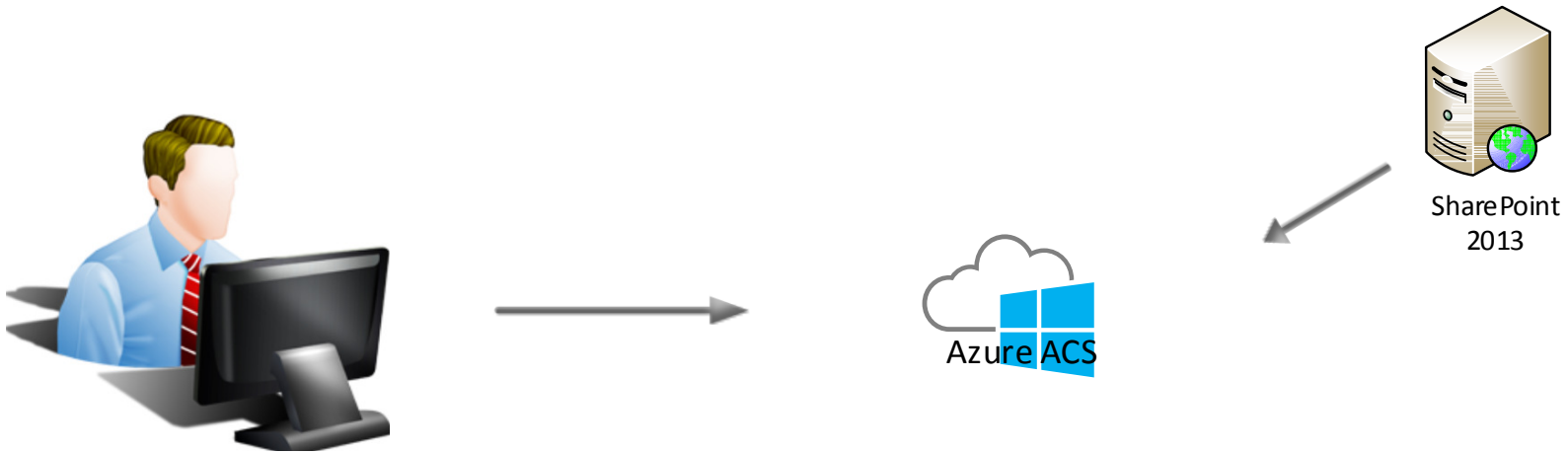


Interaction

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

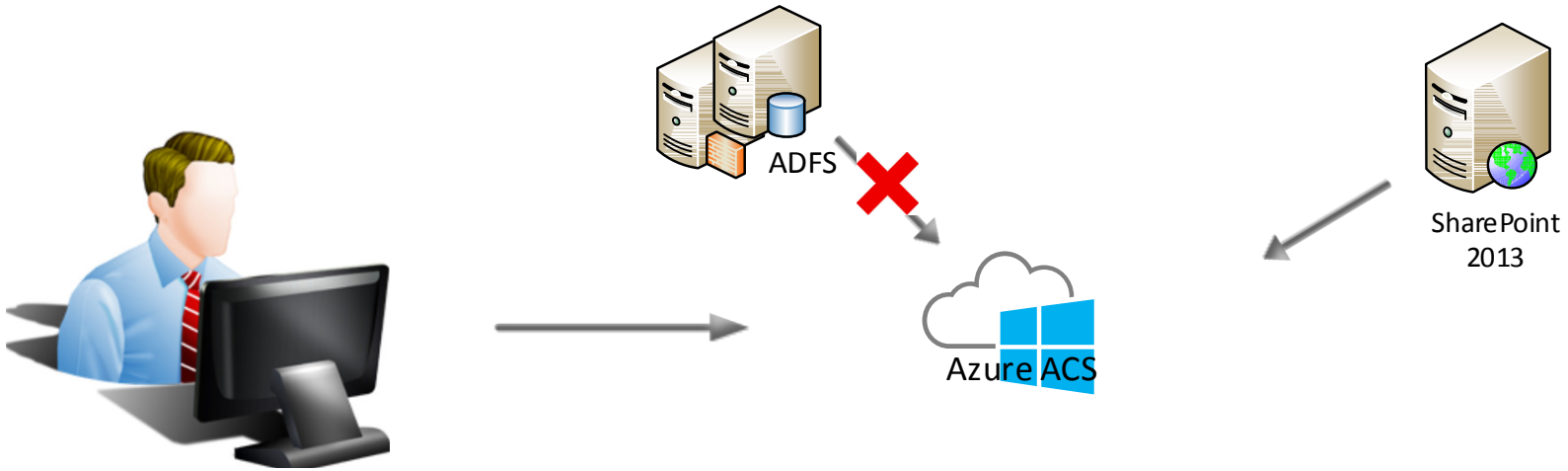
Interaction

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

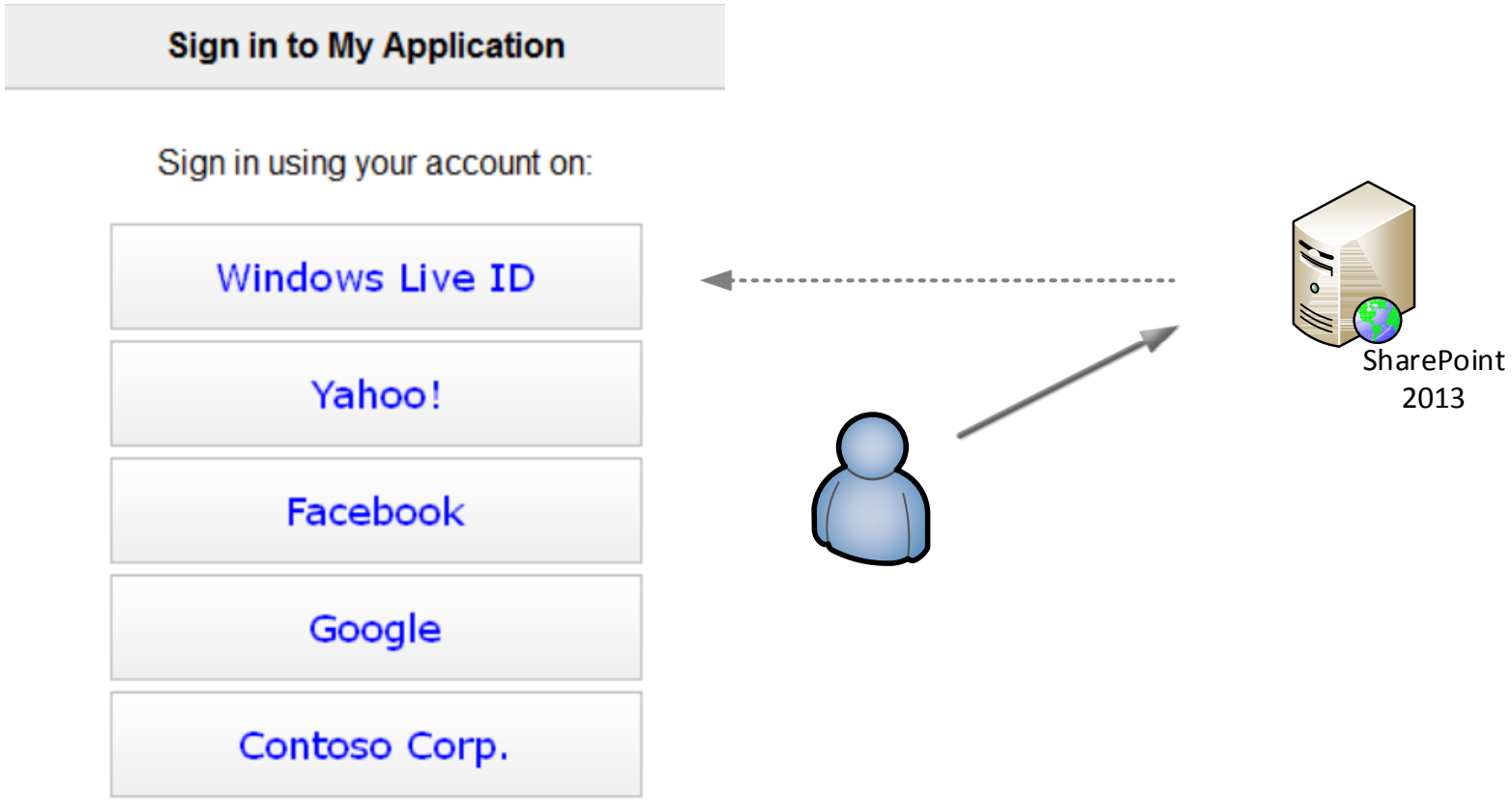


Interaction

- 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

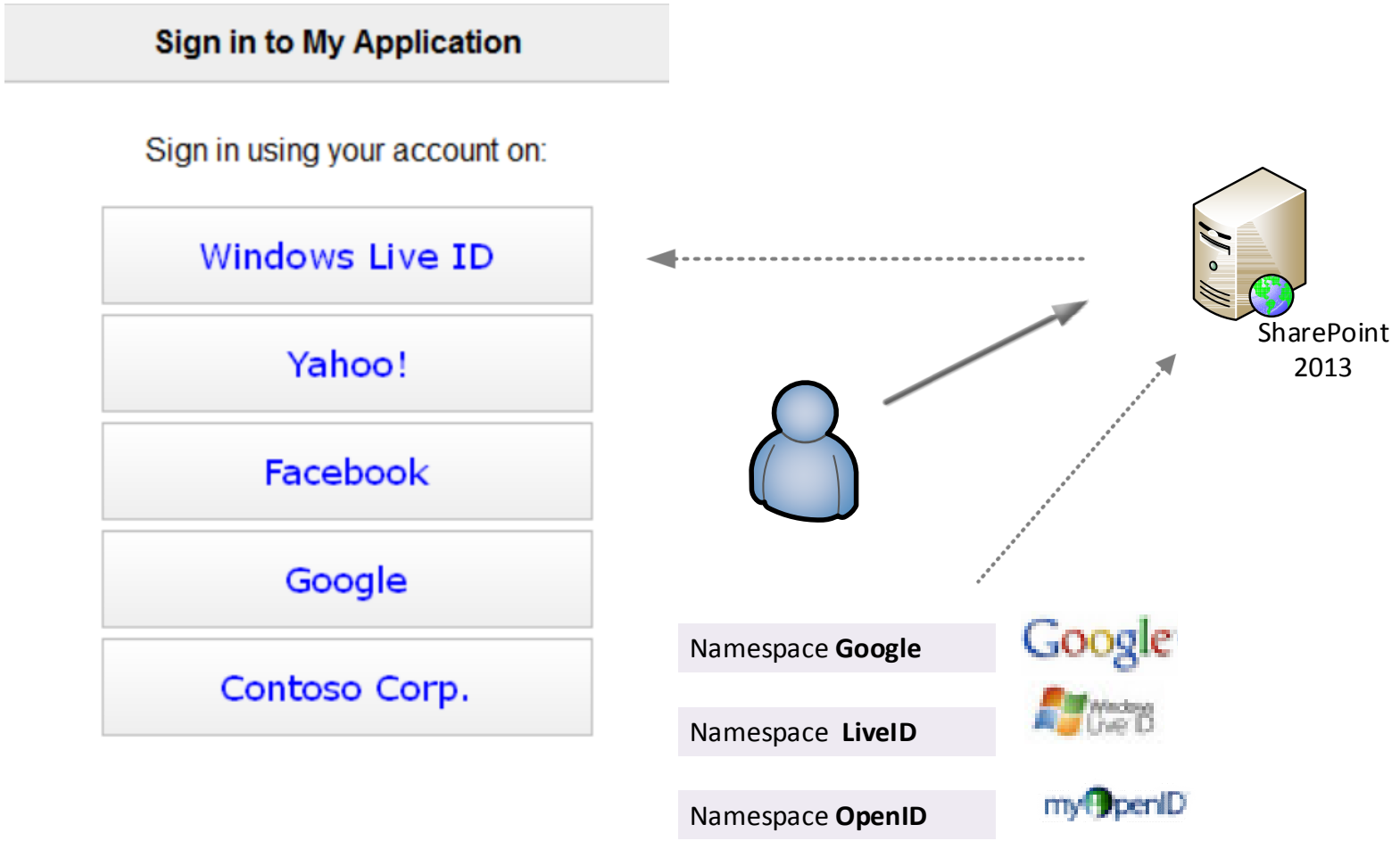


Interaction



Interaction

Interaction

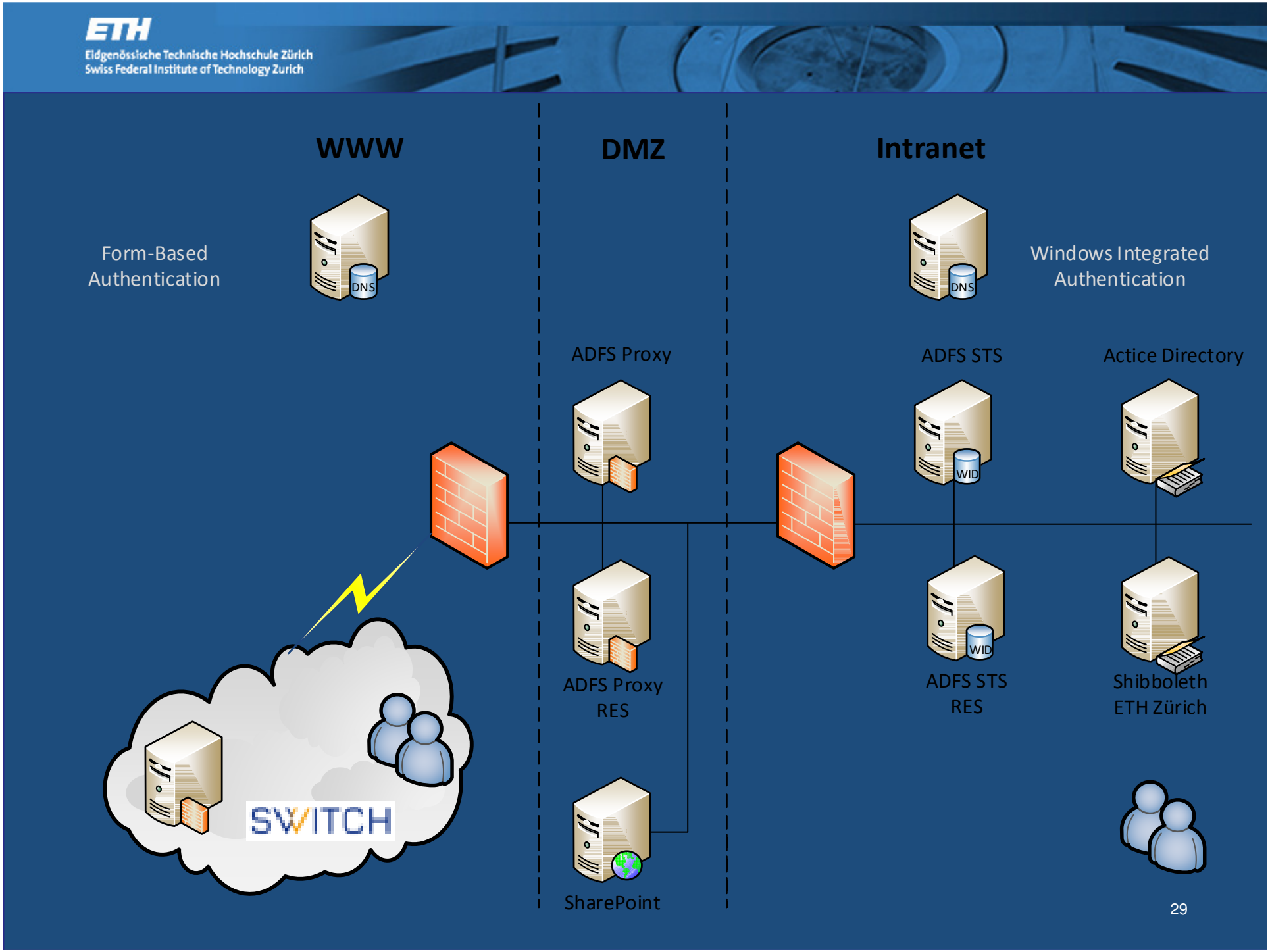


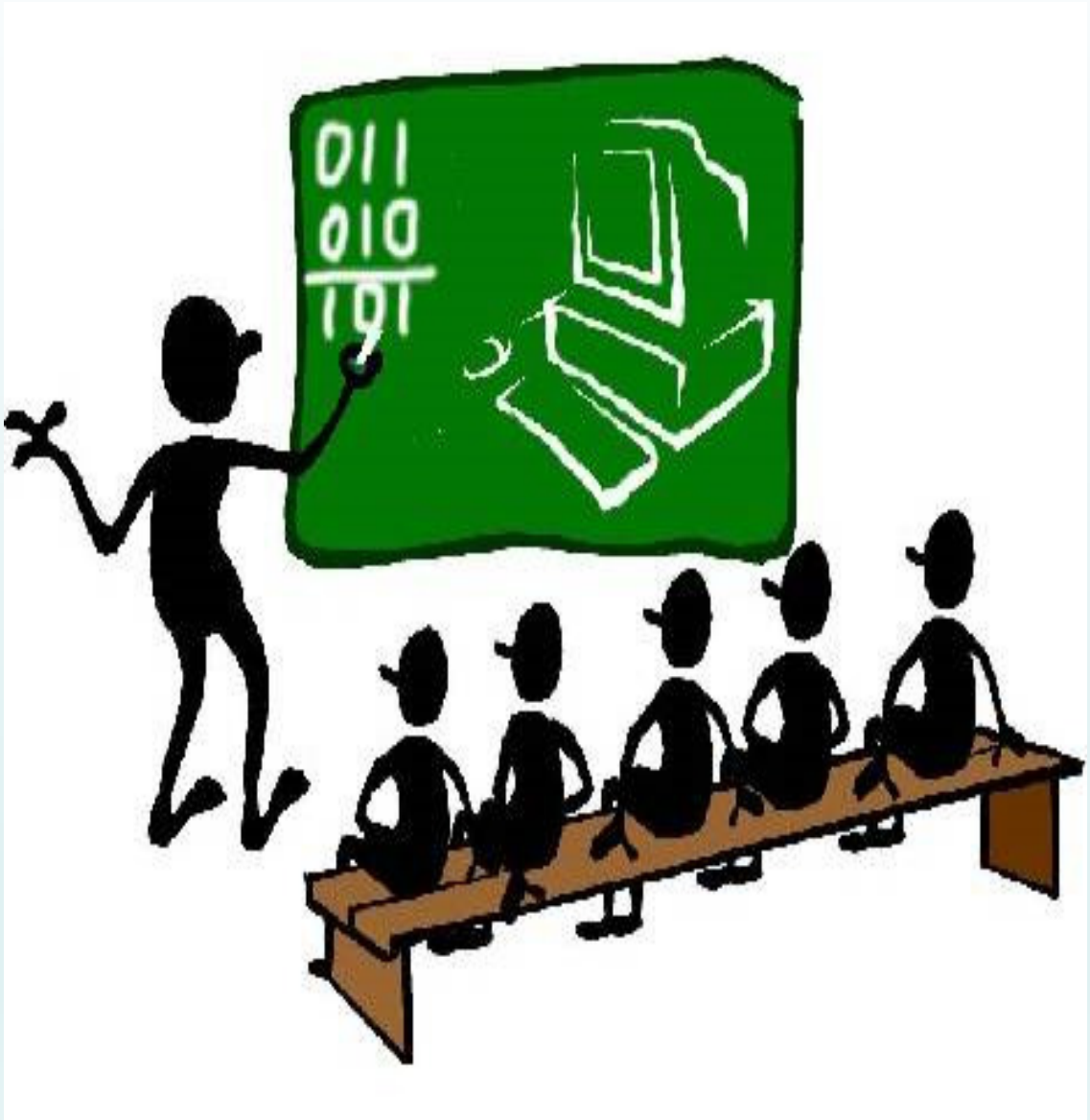
Agenda

- Active Directory Federation Service
- Claims-based authetication
- 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
DMZ
Intranet
Form-Based Authentication
DNS
DNS
Windows Integrated Authentication
ADFS Proxy
ADFS STS
Actice Directory
WID
WID
ADFS Proxy RES
ADFS STS RES
Shibboleth ETH Zürich
SWITCH
SharePoint


011
010
101