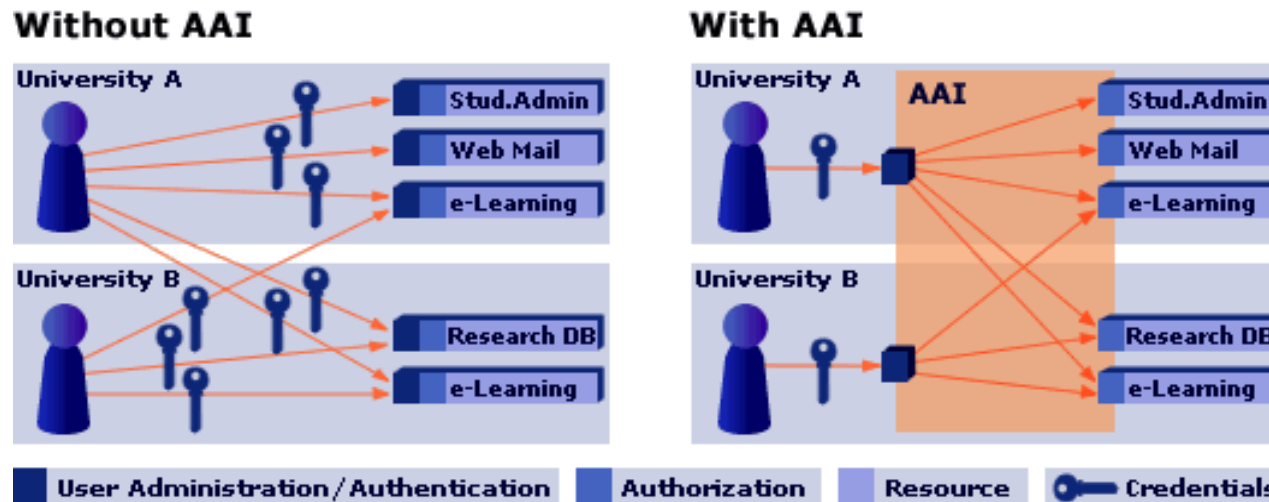


Einführung in Shibboleth

Raoul Borenius, DFN-AAI-Team
hotline@aai.dfn.de

- Zugriff auf geschützte Web-Ressourcen und die damit verbundenen Probleme
- die DFN-Föderation als mögliche Lösung
- prinzipielle Funktionsweise aus Nutzersicht
- Überblick über die Bestandteile von Shibboleth:
 - IdP
 - SP
 - Metadaten
 - Zertifikate

AAI: Zugriff auf geschützte Ressourcen



Zugriff ohne AAI:

Authentifizierung (Wer bin ich?) und Autorisierung (Was darf ich?) beim Anbieter!

- pro Anbieter einen Schlüssel/Identität
- Anbieter hat hohen Aufwand bei der Nutzerverwaltung
- in vielen Fällen wird dann auf IP-Kontrolle ausgewichen → Angebot nicht von überall zu erreichen

Zugriff mit AAI:

Trennung von Authentifizierung und Autorisierung!

- Authentifizierung immer bei der Heimateinrichtung (Uni)
- Übermittlung von Eigenschaften (Attribute) des Nutzers an den Anbieter, z.B. seinen Status (Student, Professor, Gast, Alumni, etc.)
- Autorisierung aufgrund dieser Attribute beim Anbieter (z.B. Rollenbasiert)

Vorteile für den Nutzer:

- eine Netzidentität für viele (alle?) Webangebote
- Single-Sign-On: nur einmal (pro Tag) eine Anmeldung erforderlich
- simple Software-Anforderungen
 - Web-Browser reicht!
 - keine VPN-Software o.ä.
- Datenschutz: anonymer/pseudonymer Zugriff auf das Angebot

Vorteile für den Anbieter:

- keine Userverwaltung (bzw. Pflege von IP-Listen) mehr
- flexible und einfache rollenbasierte Zugriffsverwaltung
- gleiche technische Rahmenbedingungen der Anwender über Einrichtungsgrenzen hinweg.

Problem:

Anbieter muss den von der Heimateinrichtung übermittelten Angaben (Attributen) zum Nutzer vertrauen können!

Lösung:

Schaffung von Vertrauensverhältnis durch eine Föderation!

Die Föderation “DFN-AAI” (Authentifizierungs- und Autorisierungs-Infrastruktur des Deutschen ForschungsNetzes)

- Bildet die Grundlage des **Vertrauensverhältnisses**
- Teilnehmer verpflichtet sich per Vertrag zur Einhaltung von **Spielregeln**
- die Spielregeln (**Föderations-Policy**) legt der DFN in Absprache mit den Teilnehmern fest, z.B.:
 - welcher Satz von Attributen wird verwendet (z.B. EduPerson, dfnEduPerson)
 - welche Anforderungen die x509-Zertifikate erfüllen müssen, welche zur Absicherung der Kommunikation zwischen Einrichtung und Anbieter verwendet werden
 - welche Regeln müssen bei der Pflege der IdM-Systeme an den Heimateinrichtungen beachtet werden, zB.:
 - Aktualität
 - Verifikation der Person vor Aufnahme
 - Existenz von definierten Prozessen bei Aufnahme bzw. Ausscheiden von Personen aus der Einrichtung
 - Datenschutz muß beachtet werden
 - alle Prozesse müssen Dokumentiert sein

- AAI-Software besteht aus zwei Haupt-Komponenten:
 - Identity-Provider (IdP) für Heimateinrichtung
 - Service-Provider (SP) für Anbieterseite
- Datenaustausch per **Security Assertion Markup Language (SAML)**
- SAML ist ein offener Standard, basierend auf XML
- DFN-AAI empfiehlt die Software “**Shibboleth**” des Internet2-Consortiums.
 - Open Source
 - implementiert in Java/C++
- freie Alternative auf PHP-Basis: “**simpleSAMLphp**”

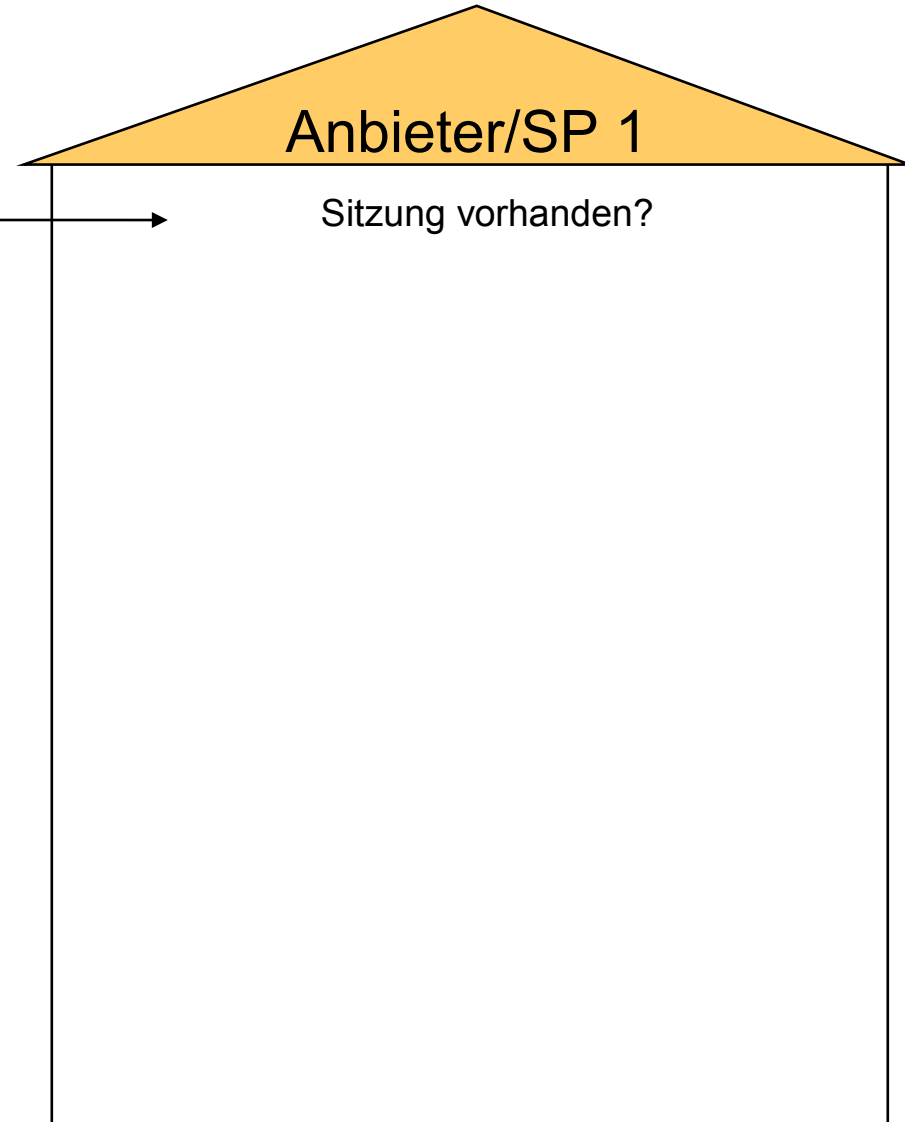




Benutzerin

Erster Zugriff

(1)



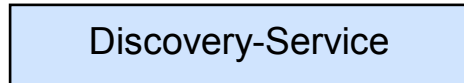
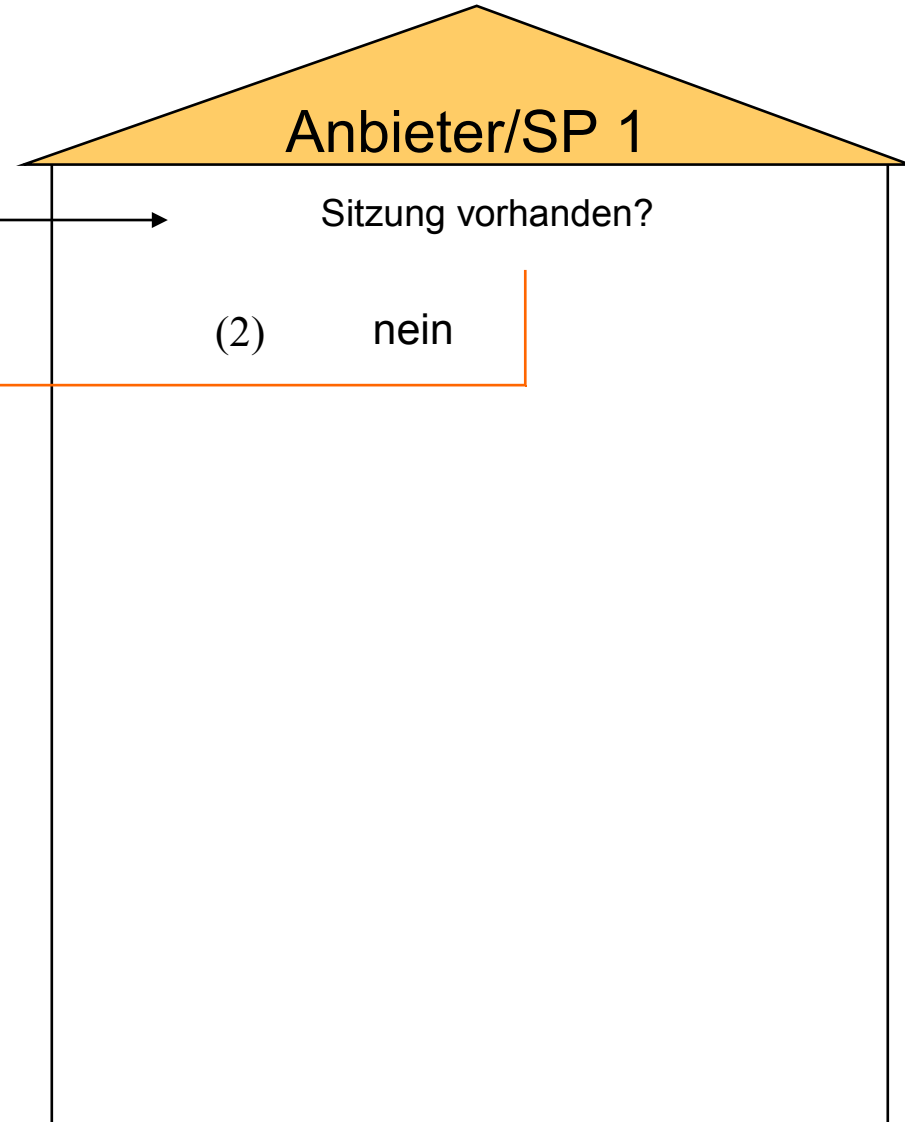
Heimateinrichtung (IdP)



Benutzerin

Erster Zugriff

(1)

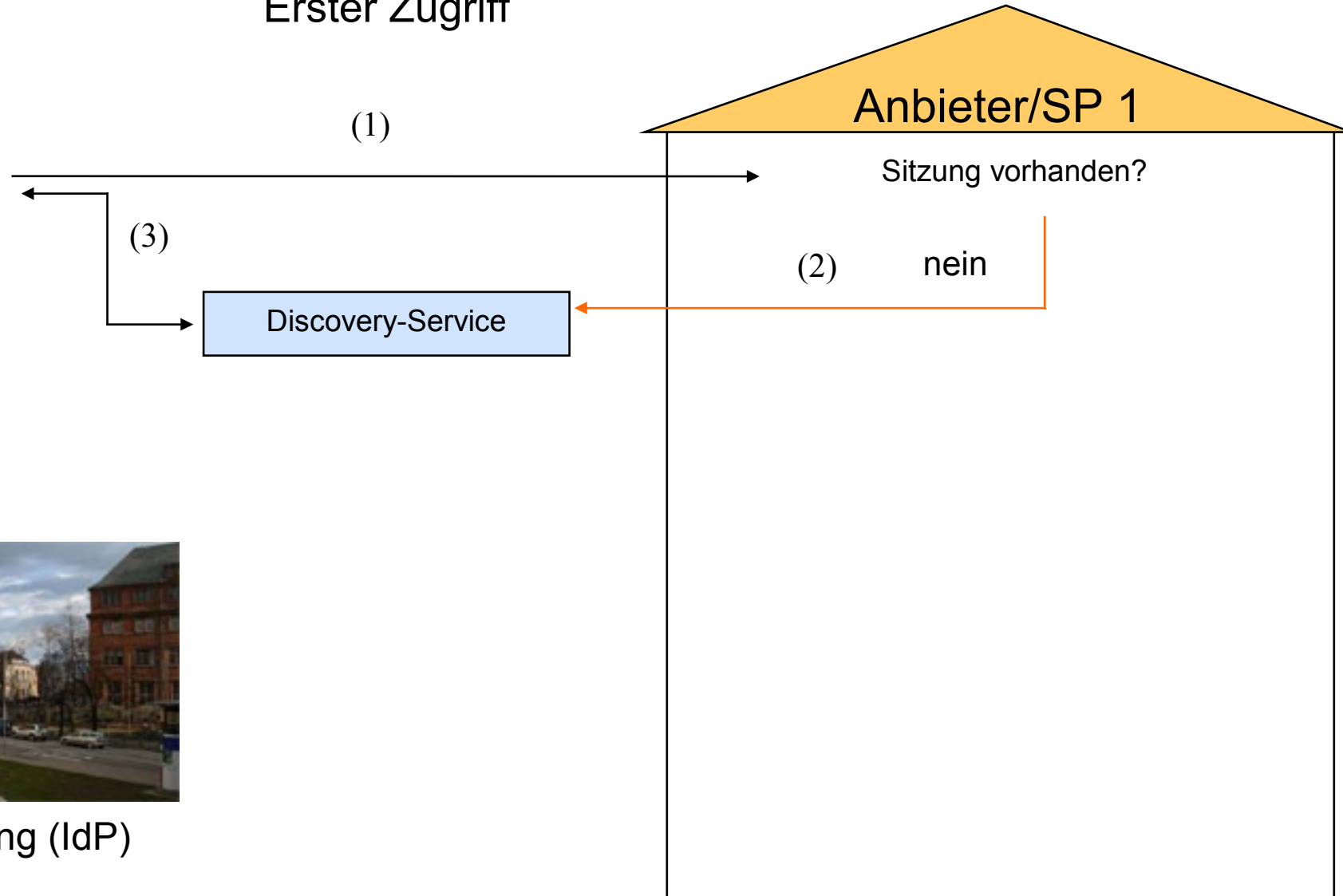


Heimatinrichtung (IdP)

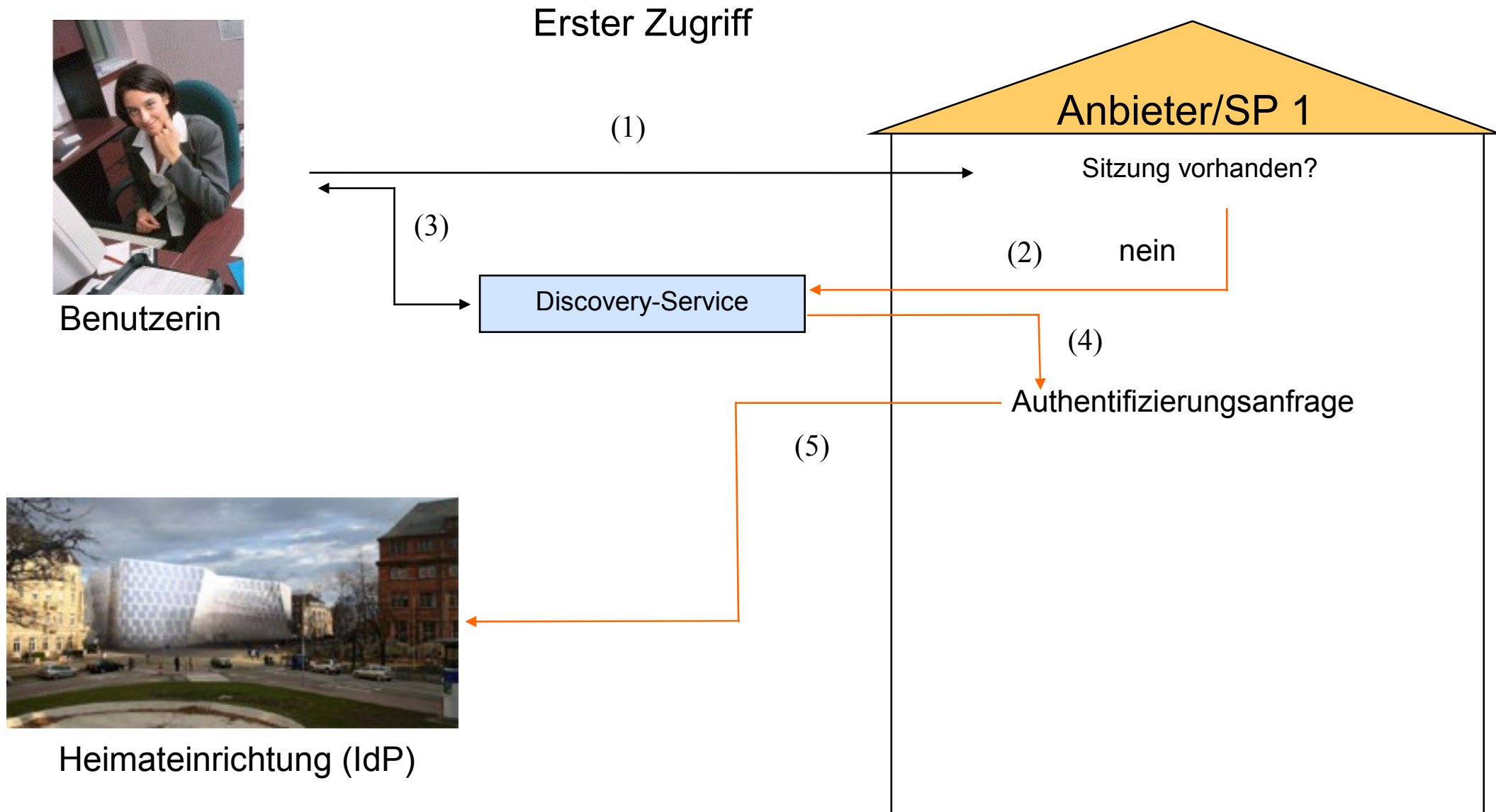


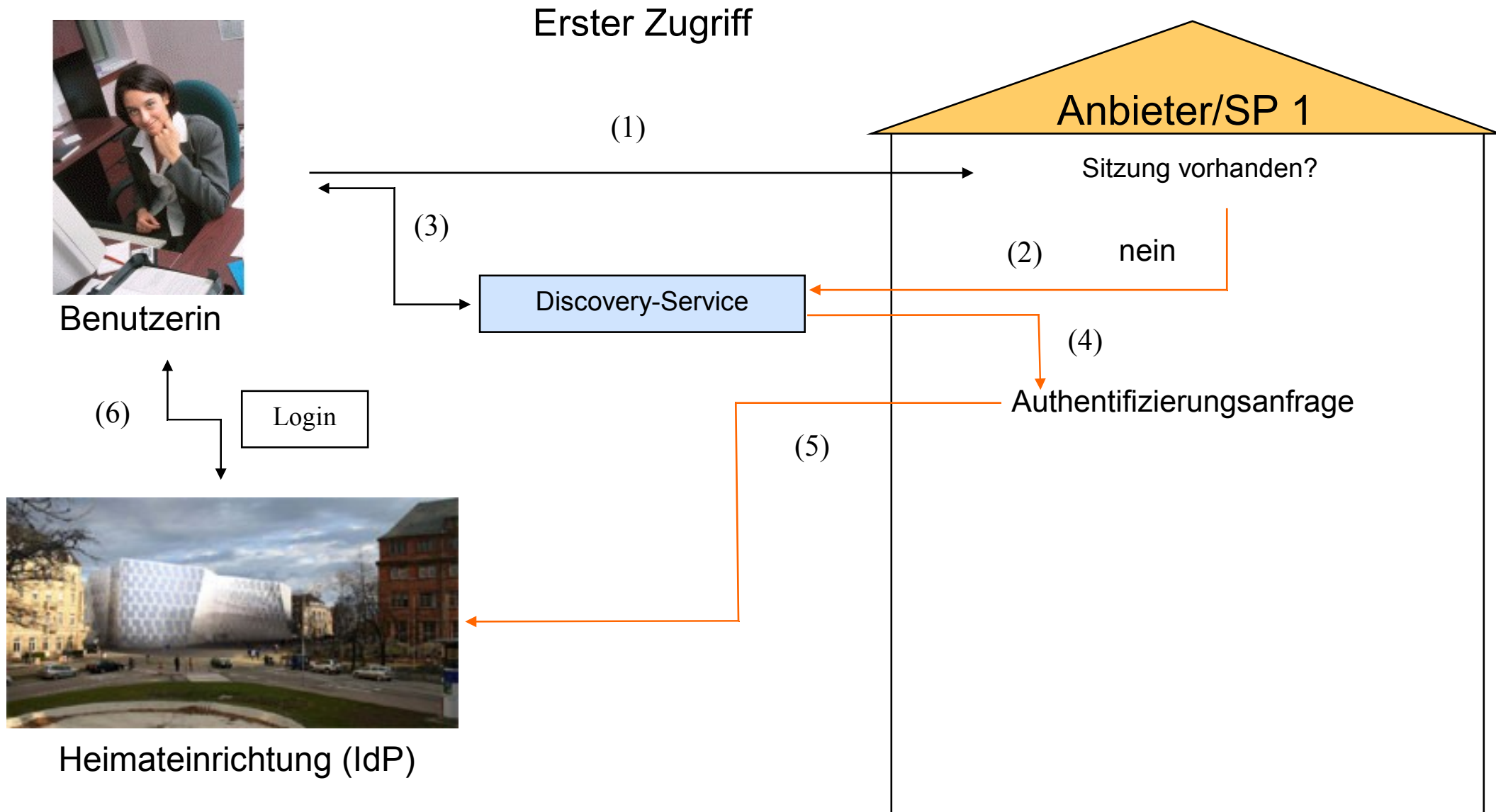
Benutzerin

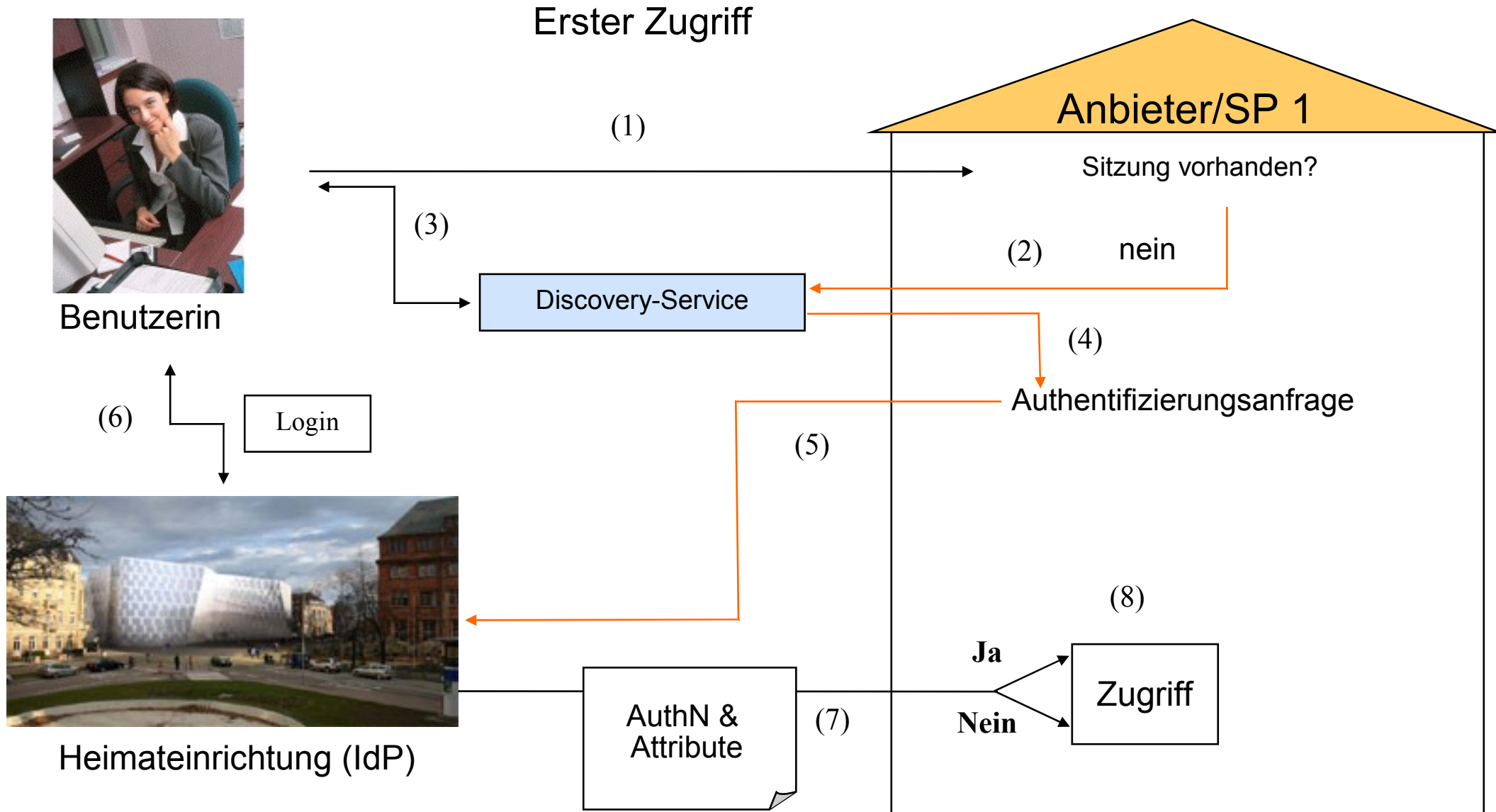
Erster Zugriff



Heimatinrichtung (IdP)





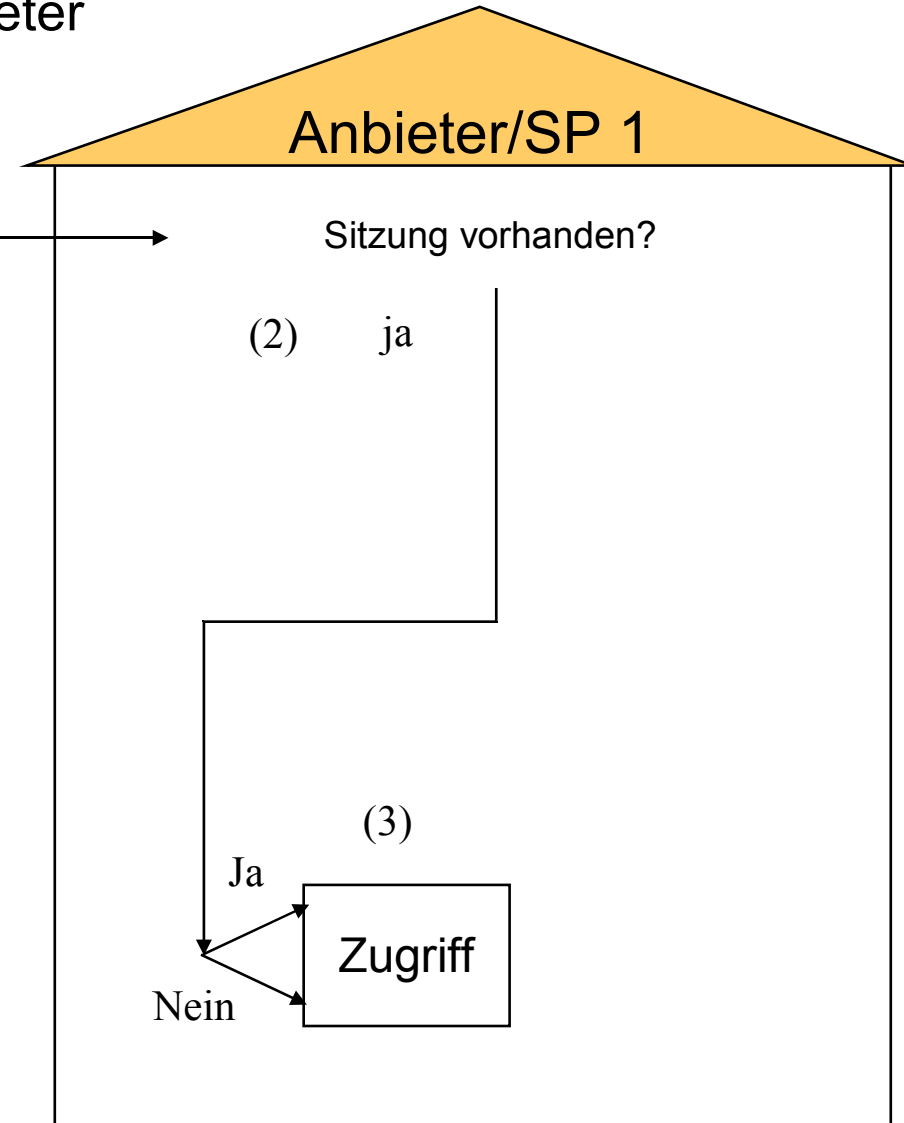


Zweiter Zugriff gleicher Anbieter



Benutzerin

(1)



Heimateinrichtung (IdP)

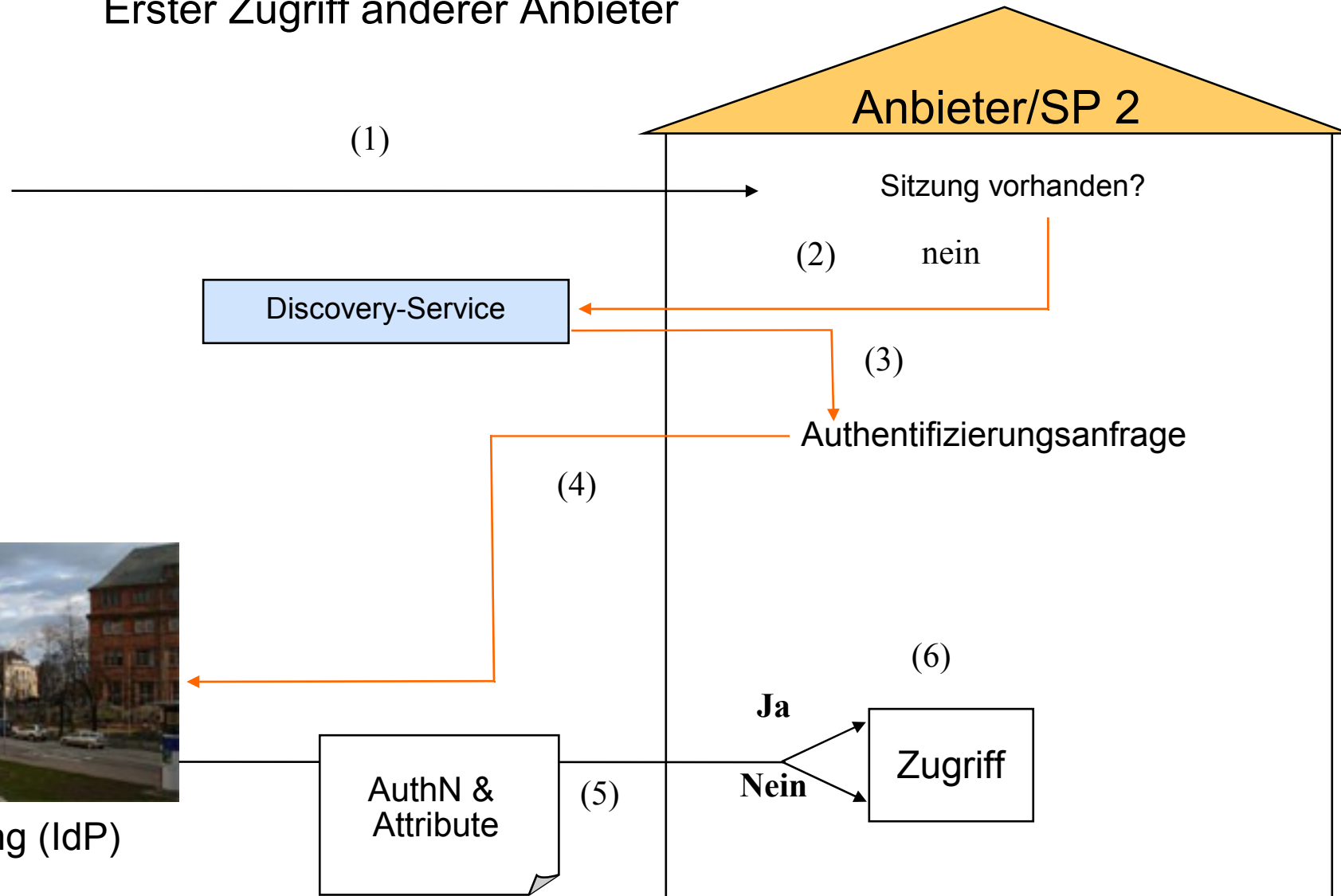
Erster Zugriff anderer Anbieter

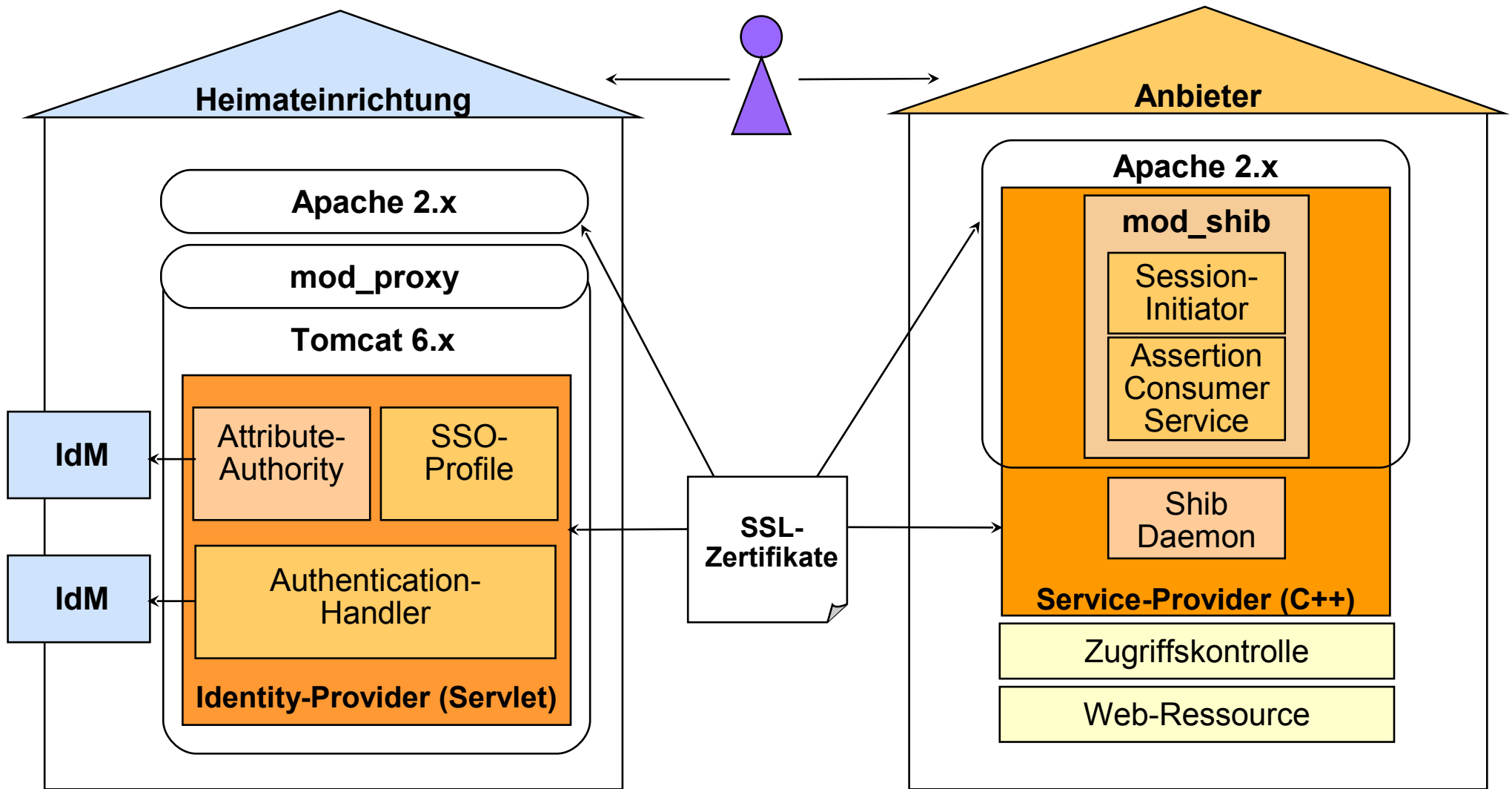


Benutzerin

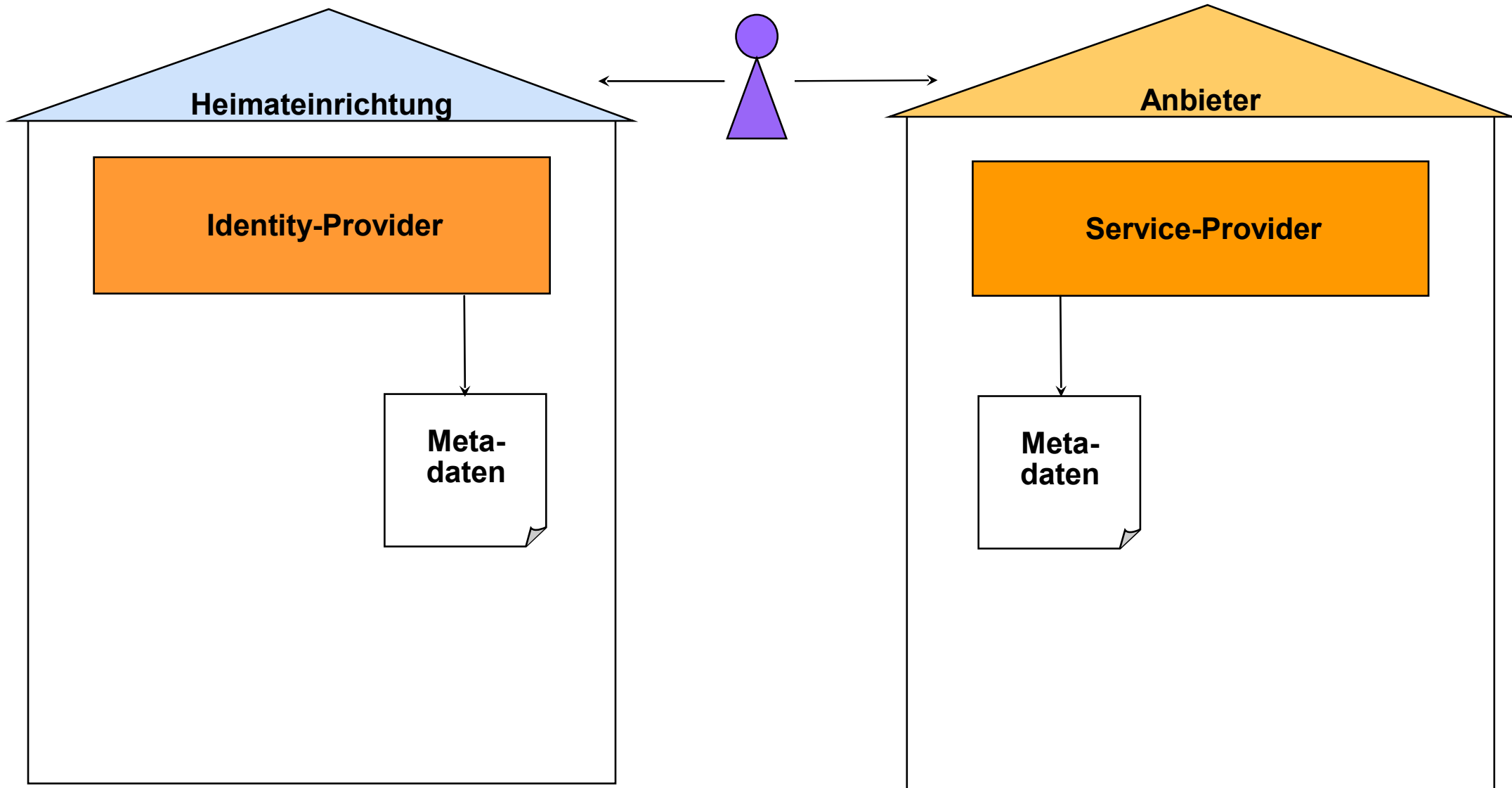


Heimateinrichtung (IdP)





Woher “kennen” sich Anbieter und Heimateinrichtung?



- Metadaten bilden die Föderation auf technischer Ebene ab
- vollständige Liste aller SPs und IdPs mit Kommunikationsparametern (URLs, Zertifikate, Scopes)

```
<EntityDescriptor entityID="https://mylogin.uni-freiburg.de/shibboleth">
  <IDPSSODescriptor protocolSupportEnumeration="urn:oasis:names:tc:SAML:1.1:protocol urn:mace:shibboleth:1.0">
    <Extensions>
      <shibmeta:Scope regexp="false">uni-freiburg.de</shibmeta:Scope>
    </Extensions>
    <KeyDescriptor use="signing">
      <ds:KeyInfo>
        <ds:X509Data>
          <ds:X509Certificate>
MIIFfTCCBGWgAwIBAgIECwSA/TANBgkqhkiG9w0BAQUFADCBhjELMAkGA1UEBhMC
REUxHjAcBgNVBAoTFVVueXZlcnNpdGFldCBGcmVpYnVyZzEWMBQGA1UECXMNUmVj
aGVue
...
w/gKdispD1t7/n/INb8BdDuqHXn90ft6ymtGFL3ktyLU6FwdiexcVLw7mky+WG56
2ERqngPct4mRDp6O58BIZ4=
          </ds:X509Certificate>
        </ds:X509Data>
      </ds:KeyInfo>
    </KeyDescriptor>
    <ArtifactResolutionService Binding="urn:oasis:names:tc:SAML:1.0:bindings:SOAP-binding"
      Location="https://mylogin.uni-freiburg.de:8443/idp/mylogin/Artifact" index="0"/>
    <NameIDFormat>urn:mace:shibboleth:1.0:nameIdentifier</NameIDFormat>
    <SingleSignOnService Binding="urn:mace:shibboleth:1.0:profiles:AuthnRequest"
      Location="https://mylogin.uni-freiburg.de/idp/mylogin/SSO"/>
  </IDPSSODescriptor>
  ...
</EntityDescriptor>
```

Zertifikate

a.) “externe” Zertifikate

- zu finden im Web-Angebot des SPs und in der Login-Seite des IdPs
- für Nutzer “sichtbar”, d.h. entscheidend ist ob der Browser diese überprüfen kann (root-im-Browser-Problem)
- müssen nicht in den Metadaten der DFN-AAI enthalten sein.

b.) “interne” Zertifikate

- Identifikation der Föderationsteilnehmer untereinander
- Signierung und Verschlüsselung der SAML-Kommunikation
- müssen in den Metadaten der DFN-AAI eingetragen werden.
- müssen den Anforderungen der DFN-AAI genügen.

In der Praxis gibt es oft keine Trennung.

Welche Zertifikate können genommen werden?

a.) DFN-PKI-Zertifikat:

- kostenlos und uneingeschränkt einsetzbar in der AAI
- in vielen Wissenschaftseinrichtungen einfach verfügbar
- Root-Im-Browser-Problem (Mozilla-Familie) mittlerweile gelöst!

b.) kommerzielle Zertifikate:

- kostenpflichtig
- nicht alle Zertifikate in der AAI einsetzbar (Policy!)

Empfehlung:

- DFN-PKI für Shibboleth (“intern”)
- falls nötig: kommerzielles Zertifikat für Apache (“extern”)
- mittelfristig DFN-Zertifikat für beides.

Für alle technischen Fragen rund um die DFN-AAI:

E-Mail: hotline@aai.dfn.de

Web: <https://www.aai.dfn.de>

