

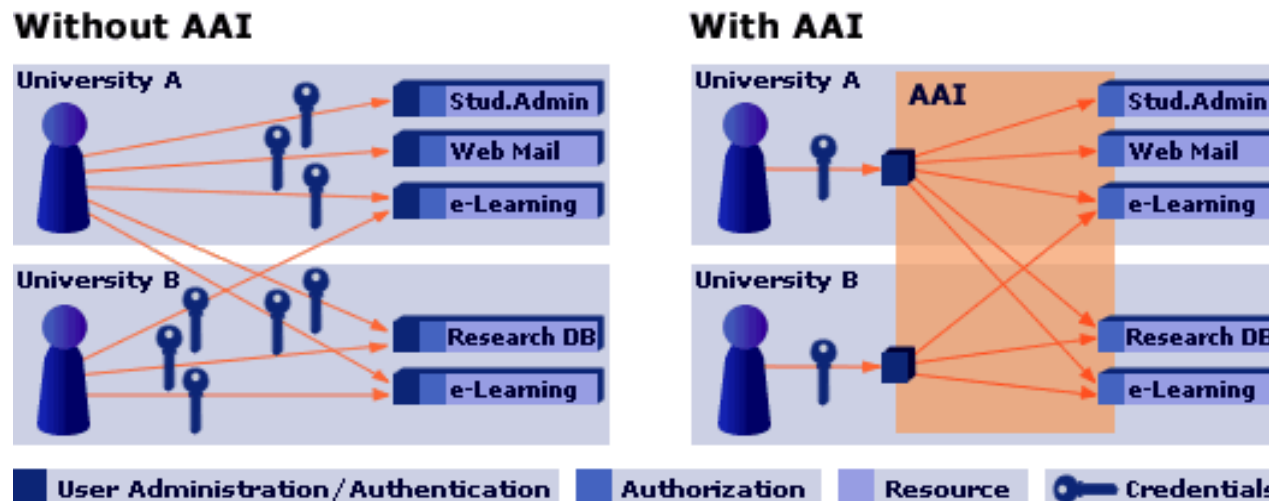
Technische Übersicht zu Shibboleth 2.0

Funktionalität und Einsatzbereiche am Beispiel
der **A**uthentifizierungs- und **A**utorisierungs-Infrastruktur
des **D**eutschen **F**orschungsnetzes (DFN-AAI)

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
- technische Umsetzung mithilfe der Shibboleth-Software
- Bestandteile von Shibboleth (IdP, SP, Metadaten, Zertifikate)
- Diskussion

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 einzige Netzidentität: einfacher kontrollierter Zugang zu verschiedenen Anbietern
- Single-Sign-On: nur einmal (pro Tag) eine Anmeldung erforderlich
- Standard-Software: keine Work-Arounds auf dem Client-Rechner mehr nötig (z.B. VPN-Software wegen IP-Begrenzung beim Anbieter)
- Datenschutz: Anbieter erhält nur die nötigsten Attribute die er braucht (z.B. die Rolle des Nutzers). Nutzer behält seine Anonymität

Vorteile für den Anbieter:

- Keine Userverwaltung (bzw. Pflege von IP-Listen) mehr
- kann verschiedenen User-Gruppen sehr flexibel verschiedene Zugriffe gestatten.
- Anbieter erreicht durch einen einzigen Vertragsabschluß eine Vielzahl von Anwendern die gleich behandelt werden können

Problem:

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

Lösung:

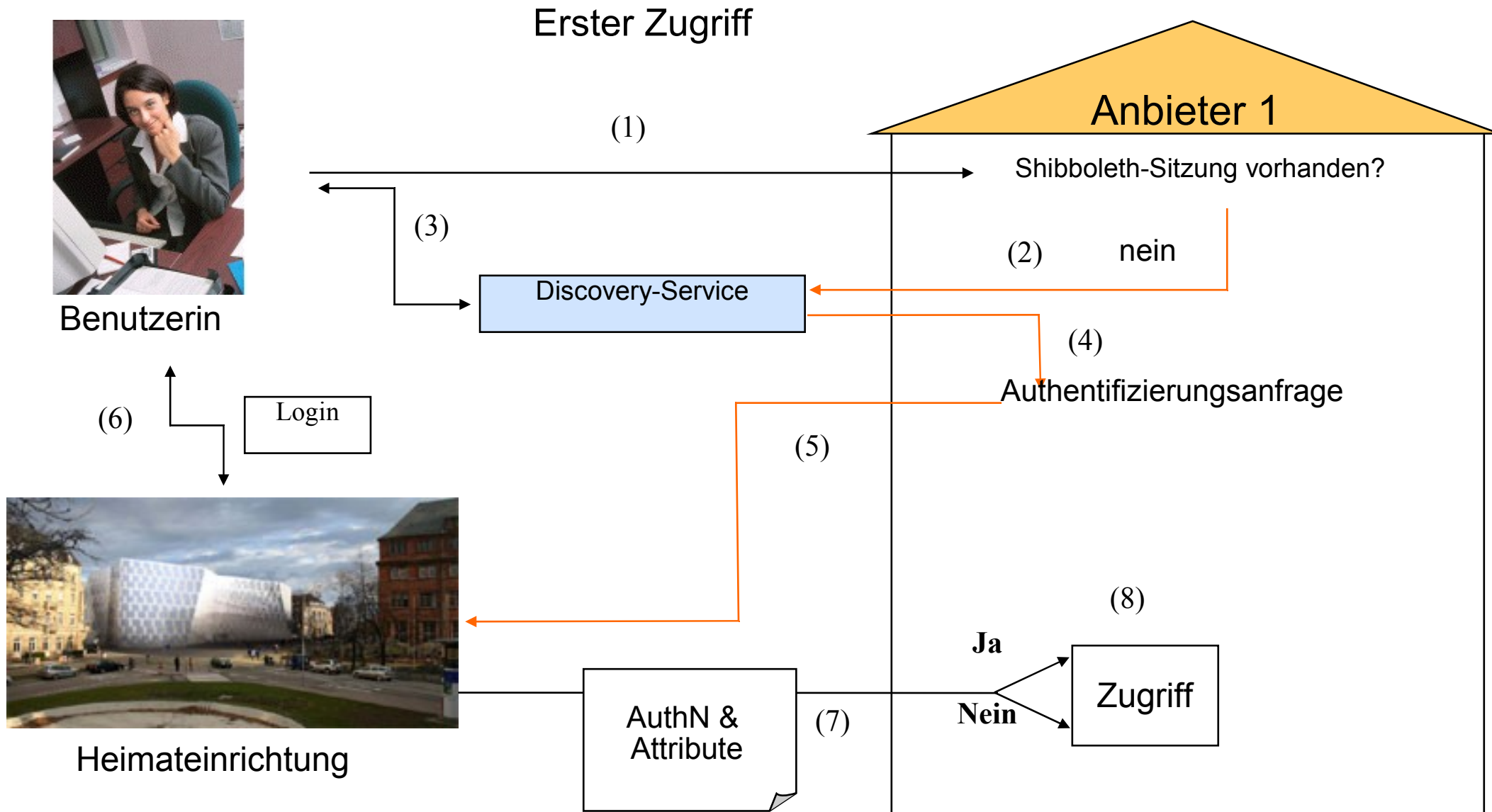
Schaffung von Vertrauensverhältnis durch eine Föderation!

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)
 - 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



- Die DFN-AAI verwendet wie die meisten europäischen Föderationen die Software “**Shibboleth**” des Internet2-Consortiums.
- Shibboleth besteht aus zwei Haupt-Komponenten:
 - Identity-Provider (IdP) für die Heimateinrichtung
 - Service-Provider (SP) für die Anbieterseite.
- der Datenaustausch zwischen diesen Komponenten geschieht per **Security Assertion Markup Language (SAML)**
- SAML ist ein offener Standard, basierend auf XML
- die SAML-Implementierung Shibboleth ist Open Source, d.h. frei erhältlich für verschiedene Systeme.

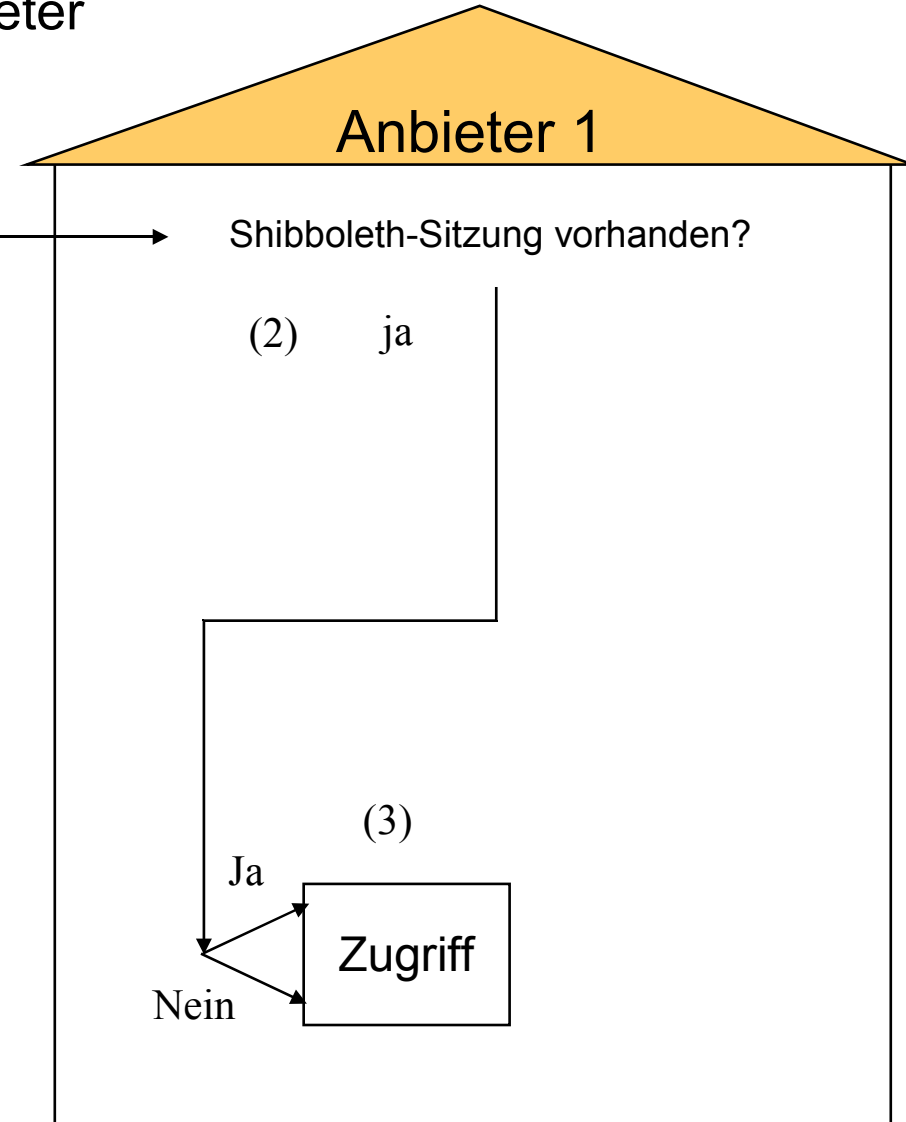


Zweiter Zugriff gleicher Anbieter



Benutzerin

(1)



Anbieter 1

Shibboleth-Sitzung vorhanden?

(2) ja

(3)

Ja

Zugriff

Nein



Heimateinrichtung

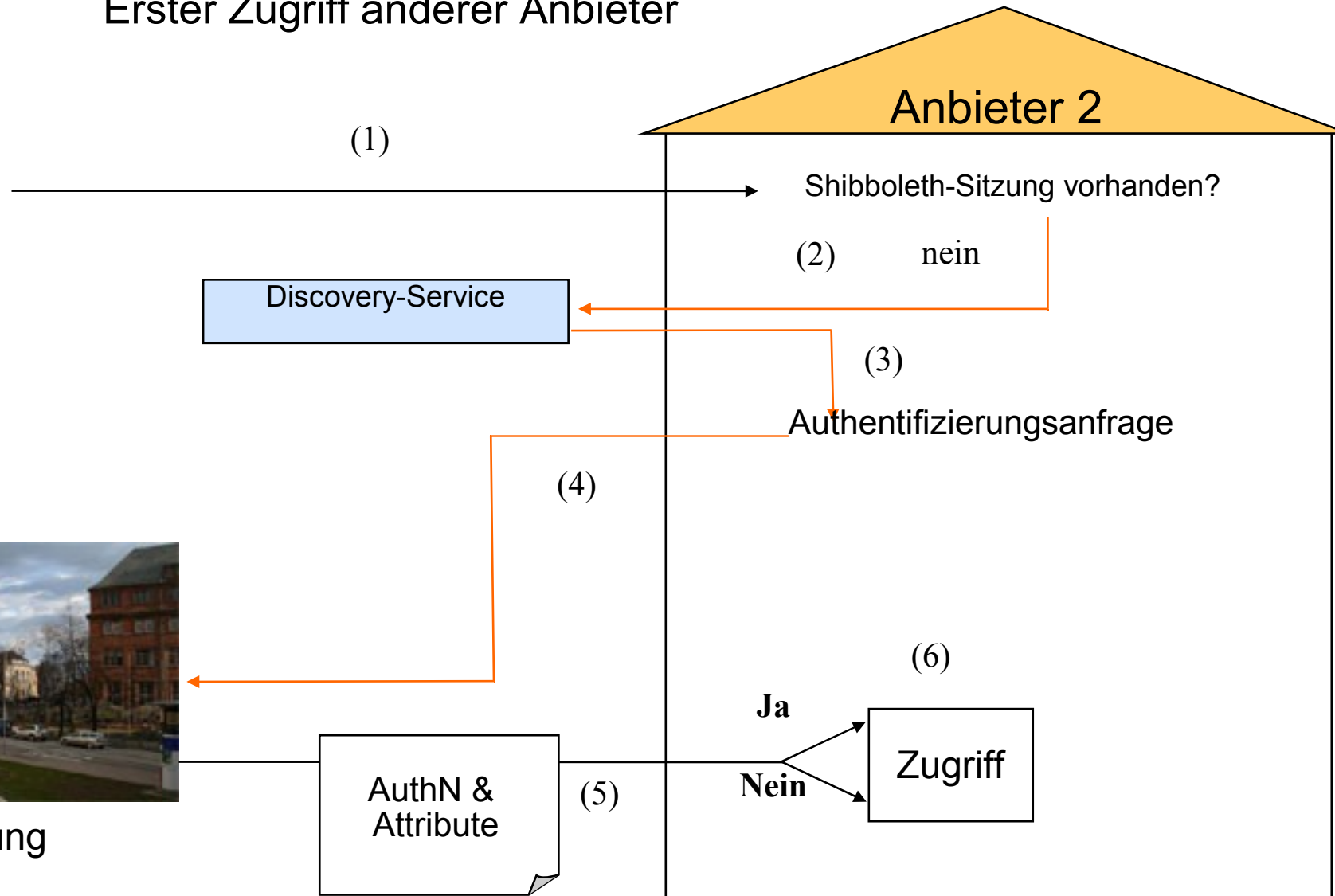
Erster Zugriff anderer Anbieter

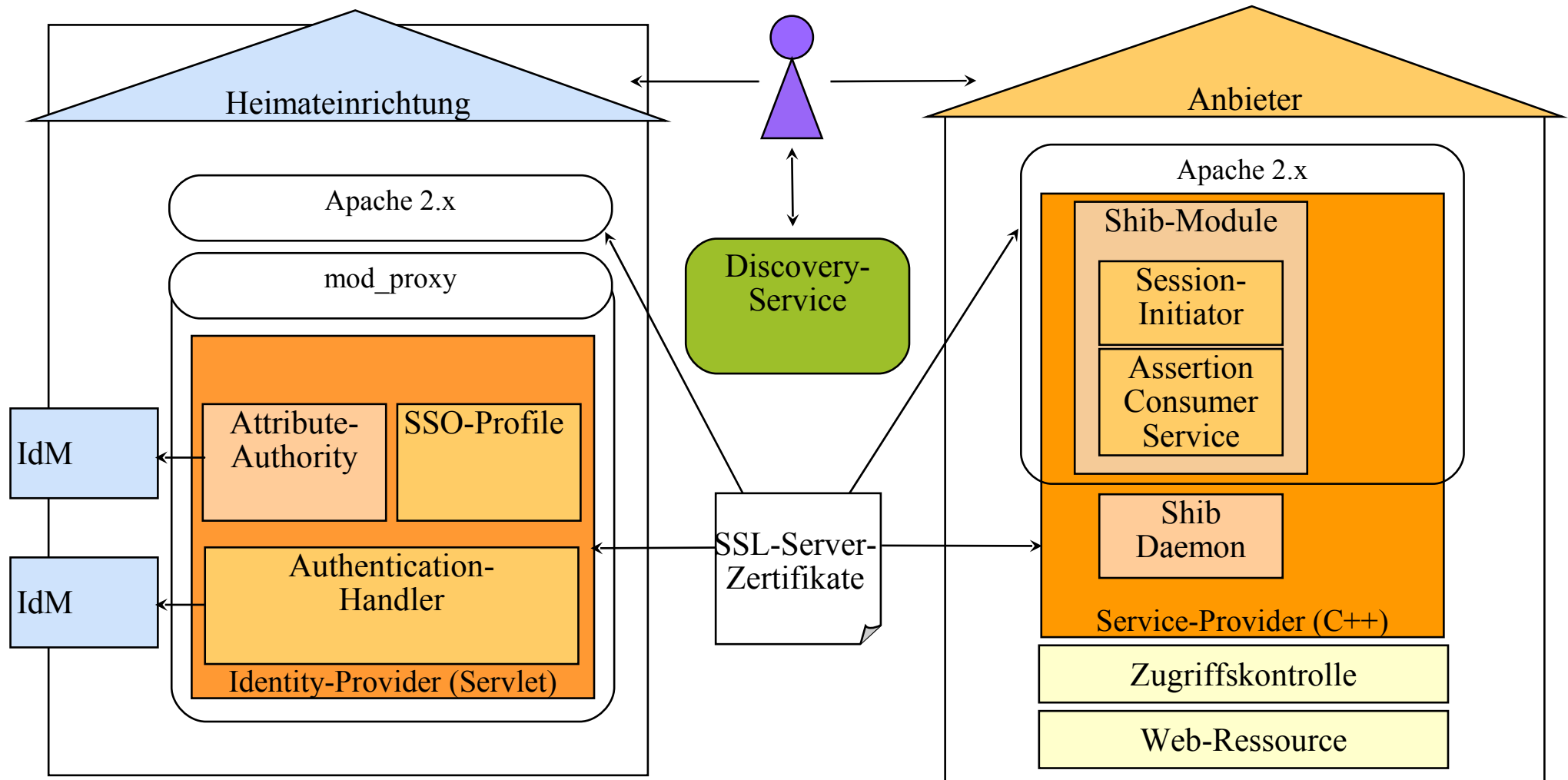


Benutzerin

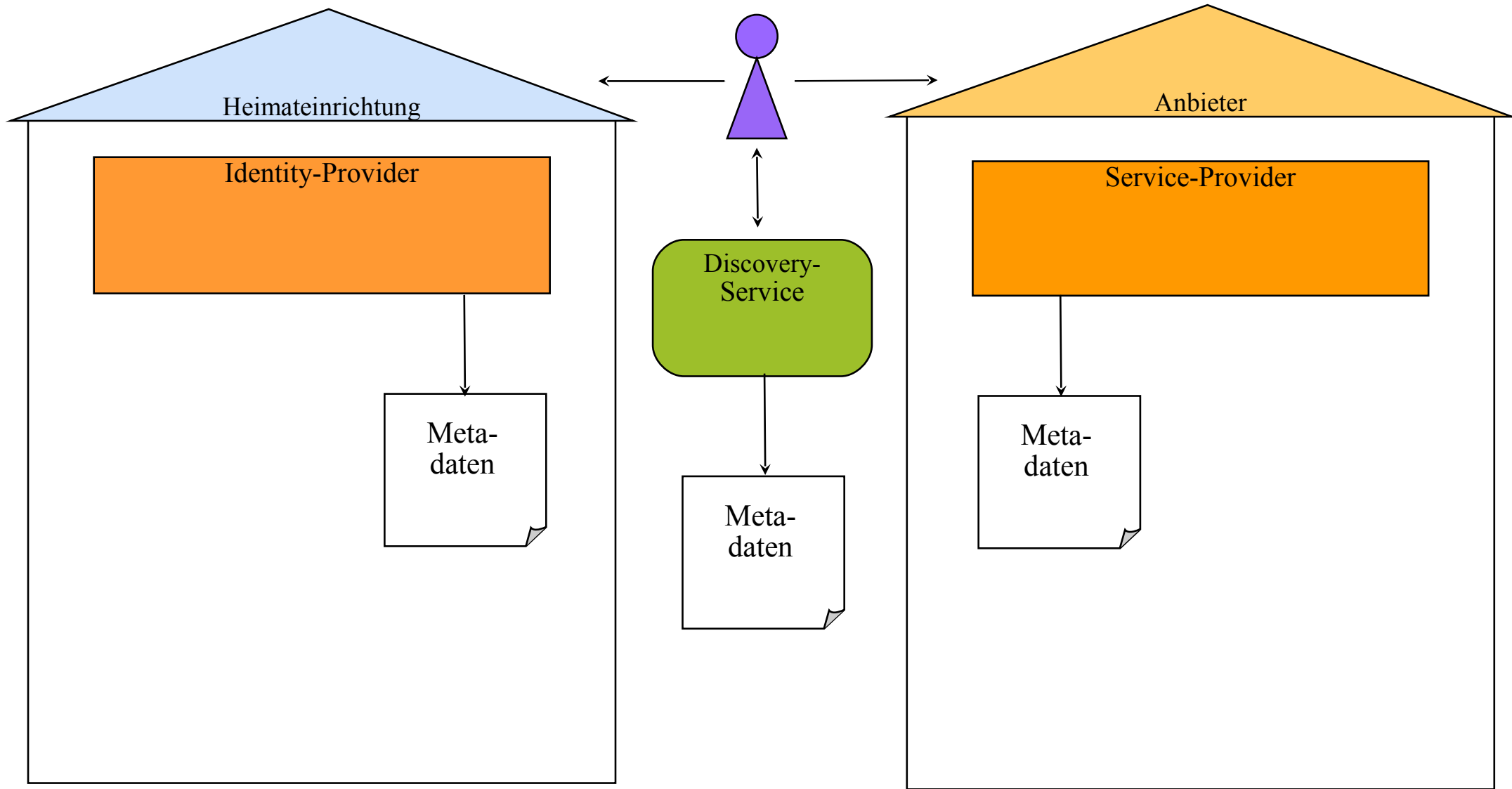


Heimateinrichtung





Woher “kennen” sich eigentlich Anbieter und Heimateinrichtung?



- Die Metadaten bilden die Föderation auf technischer Ebene ab
- Sie beinhalten eine vollständige Liste aller teilnehmenden Anbieter (SPs) und Einrichtungen (IdPs) mit deren Kommunikationsendpunkten:

```
<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/TANBgkqhkiG9w0BAQUFADCBBhjELMAkGA1UEBhMC
REUxHjAcBgNVBAoTFVVueXZlcnNpdGFldCBGcmVpYnVyZzEWMBQGA1UECxmNUNmVj
aGVue
...
w/gKdispD1t7/n/INb8BdDuqHXn90ft6ymtGFL3ktyLU6FwdiexcVLw7mky+WG56
2ERqngwPct4mRDP6O58BIZ4=
          </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
- aber: Root-Im-Browser-Problem (Mozilla-Familie)

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>

