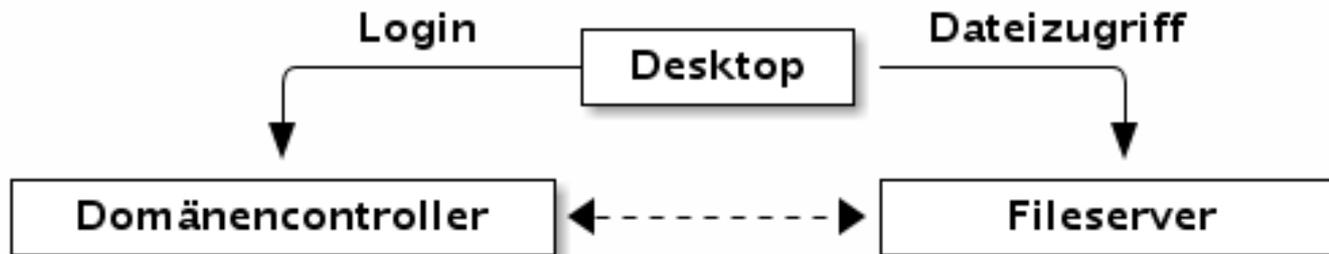


Web-Single-Sign-On in der LUH

- Begriffsklärung
- Technischer Ablauf
- Umsetzung an der LUH
- Vor- und Nachteile

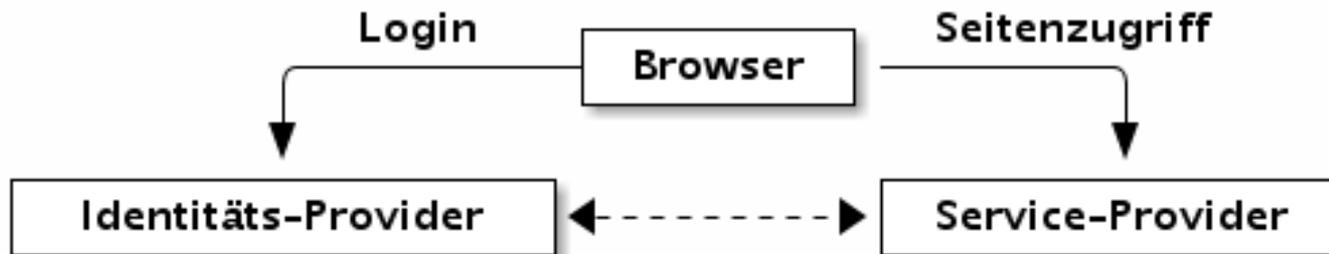
Begriffsklärung

- Single Sign-on: Benutzer meldet sich zu Beginn seiner „Sitzung“ an und hat dann Zugriff auf viele Anwendungen.
 - z.B. Active Directory:



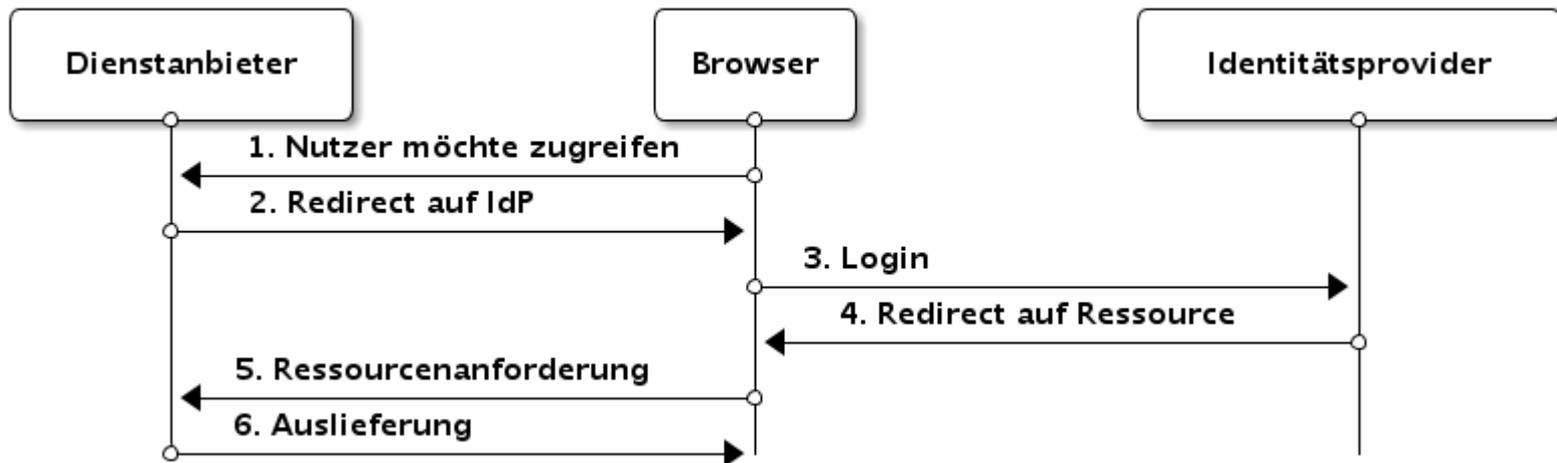
Begriffsklärung

- WebSSO: SSO übertragen auf Webanwendungen, also SSO „über den Webbrowser“:



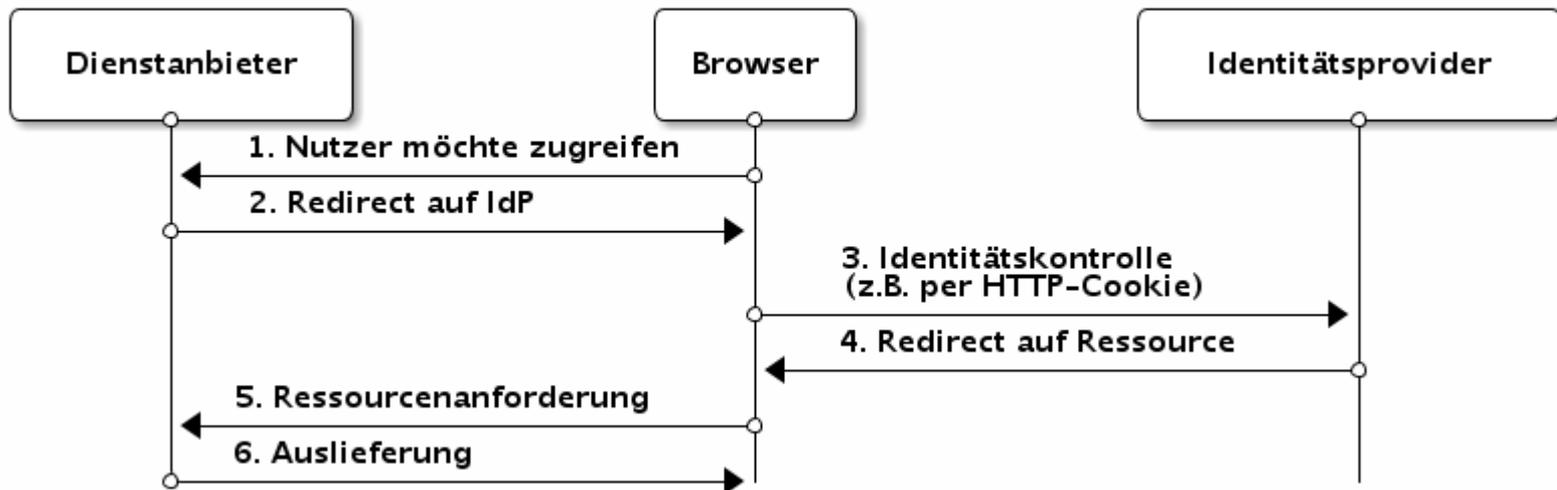
Technischer Ablauf

- Erstanmeldung zu Beginn der Sitzung



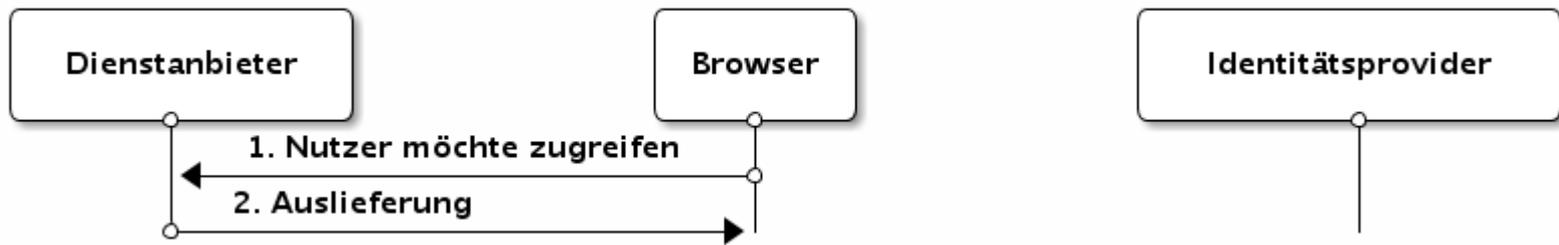
Technischer Ablauf

- Zugriff auf weitere Ressource bei anderem Anbieter



Technischer Ablauf

- Zugriff auf weitere Ressource bei gleichem Anbieter



Technischer Ablauf

- Sitzungskontrolle üblicherweise per HTTP-Cookies, bei IdP und SP
 - Es existieren also immer mindestens zwei Sessions auf zwei verschiedenen Servern
- Möglichkeiten zum Finden des zuständigen IdPs:
 - Hartverdrahtet in der Anwendung
 - Codiert im Benutzernamen (OpenID)
 - Bilden einer Föderation, Discovery Service (alt: WAYF)

Unterschiede zwischen Shibboleth und OpenID

- Bei Shibboleth findet Kommunikation nur über Browser statt (front channel communication)
 - Daher: Registrierung der SPs nötig
- Der Shibboleth-IdP kann weitere Benutzerattribute übertragen
 - Oder auch gar keine, d.h. es ist eine anonyme Anmeldung möglich.
 - Dagegen wird bei OpenID stets nur genau die ID übertragen (in der alten Version, OpenID 2.0 unterstützt auch Attribute)

Umsetzung an der LUH

- Jeder registrierte Benutzer des IdM kann sich einen sogenannten WebSSO-Account anlegen.
- Dieser Account gilt sowohl für den Shibboleth- als auch für den OpenID-Dienst.
- Der Accountname ist die LUH-ID
 - Bei OpenID allerdings mit Präfix <https://uni-h.de/>, also z.B. <https://uni-h.de/RRZ-NH1>

Umsetzung an der LUH



Leibniz
Universität
Hannover

R | R | Z | N
Regionales Rechenzentrum für Niedersachsen

English

Angemeldet als TES-T1L

Account-Manager (dev)

▶ IT-Dienste

- Pers. Daten
- E-Mail ändern
- Verwendung pers. Daten
- Abmelden

IT-Dienste

IT-Dienste ?

Die folgenden Zugänge sind bereits für Sie eingerichtet:

Dienst	Benutzername	Status	Aktionen
IdM / HIS	TES-T1L	aktiv	Passwort ändern

Die Benutzung der Dienste unterliegt den [Nutzungsbedingungen](#).

Für folgende Dienste können Sie noch Zugänge beantragen:

- WLAN / VPN
- Stud.IP
- PC-Pool MaPhy
- MSDN-AA
- WebSSO / OpenID
- E-Mail
- Campus-PC

RRZN Aktuelle Meldungen

22.11.2011: Systemarbeiten auf den TYPO3-Servern
Am kommenden Dienstag, 22.11.2011, werden wir umfangreiche Updates auf den Serversystemen der...

Stellenangebote
In der Einrichtung Zentrale Services Informationstechnologie (vormals RRZN) sind folgende Stellen...

[mehr...](#)

Online-Aktuell - Leibniz Universität Hannover

Termin Tipp: Technologieorientierte Kooperationen in Europa sicher gestalten
Informationsveranstaltung für Unternehmen, Wissenschaftlerinnen und Wissenschaftler

Nominierung für den Titel "Professor des Jahres 2011"
Prof. Dr.-Ing. Udo Nackenhorst landet bundesweit auf dem zweiten Platz

[mehr...](#)

[Impressum](#) [support\(at\)idm.uni-hannover.de](mailto:support(at)idm.uni-hannover.de)

Umsetzung an der LUH – Shibboleth-IdP

- Der Shibboleth-IdP ist eine Java-Applikation
 - läuft innerhalb Tomcat, hinter Apache-Webserver
- kann im IdM-Backend gespeicherte Attribute liefern
 - z.B. LUH-ID, Vor- und Nachname, E-Mail-Adresse, Statusgruppe(n) (student, staff, faculty etc.), Matrikelnummer, Pseudonym
- Die Attribute werden nur an berechnigte Anbieter und nur nach Zustimmung des Nutzers weitergegeben

Umsetzung an der LUH - Shibboleth-IdP



Leibniz
Universität
Hannover

R | R | Z | N |
Regionales Rechenzentrum für Niedersachsen

WebSSO
Zum Account-Manager

WebSSO-Login



Der Service-Provider mit der ID

<https://dev.idm.uni-hannover.de/shibboleth>

bittet Sie, sich über den WebSSO-Dienst der LUH anzumelden.

Wenn Sie noch keinen Zugang zum WebSSO-Dienst der LUH haben, können Sie ihn im [Account-Manager](#) beantragen.

Kennung:

Passwort:

Attributfreigabe zurücksetzen

support(at)idm.uni-hannover.de

Umsetzung an der LUH – Shibboleth-SP

- Pilotinstallation eines SP
 - Software-Quelle: Verteilung von Mathematica-Lizenzen
 - Debian-Server mit Apache, PHP und Shibboleth-Plugin
- Debian-Paket libapache2-mod-shib2 out-of-the-box nutzbar
 - Im Wesentlichen müssen nur die Metadaten des IdP, also das Zertifikat, eingebunden werden
 - Das Plugin muss dann nur noch in die Webseiten-Konfiguration eingebunden werden (nächste Folie)

Umsetzung an der LUH - Shibboleth-SP

Nur angemeldete Nutzer sollen Zugriff haben:

```
<Location /secure-sso>  
    AuthType shibboleth  
    ShibRequireSession On  
    require valid-user  
</Location>
```

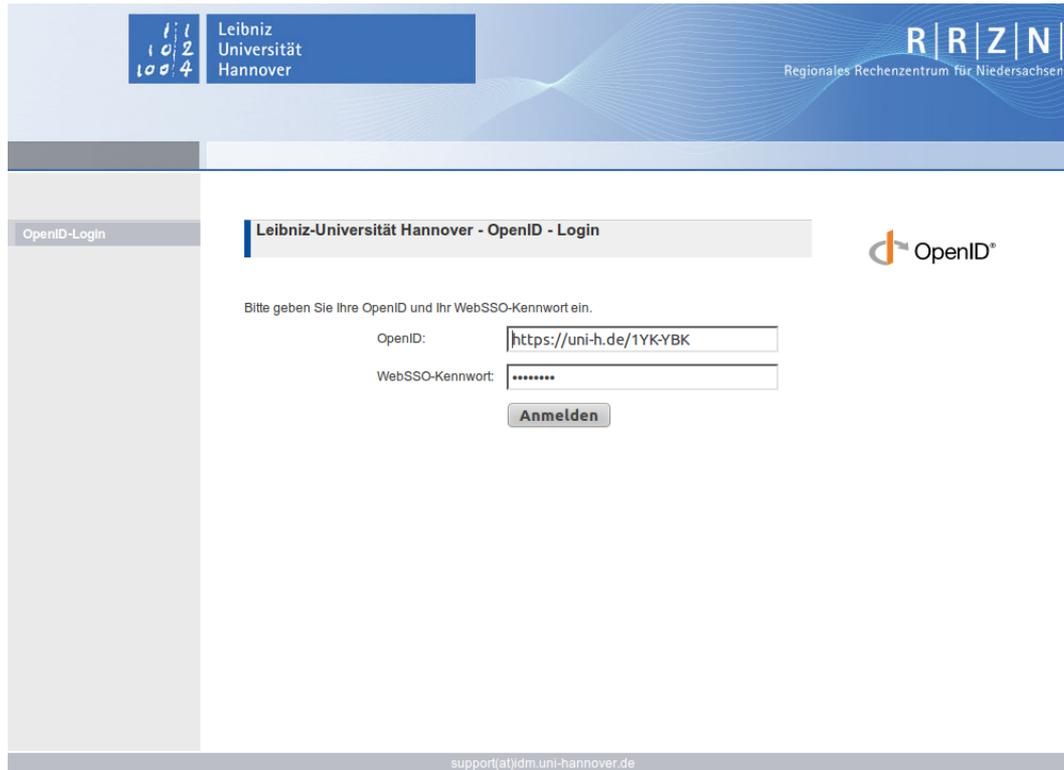
Umsetzung an der LUH - Shibboleth-SP

Nur Nutzer der Statusgruppe `staff` sollen Zugriff haben:

```
<Location /secure-sso>  
    AuthType shibboleth  
    ShibRequireSession On  
    require scopedAffiliation ~ ^staff@uni-hannover\.de  
</Location>
```

Umsetzung an der LUH - OpenID-IdP

- Eigenentwicklung, basierend auf einem Zend-Modul, lediglich Webfrontend und Authentifizierungsschicht wurden ergänzt.



Leibniz
Universität
Hannover

R | Z | N |
Regionales Rechenzentrum für Niedersachsen

OpenID-Login

Leibniz-Universität Hannover - OpenID - Login

OpenID®

Bitte geben Sie Ihre OpenID und Ihr WebSSO-Kennwort ein.

OpenID:

WebSSO-Kennwort:

Anmelden

support(at)idm.uni-hannover.de

Umsetzung an der LUH - OpenID-SP

- Pilotverfahren mit Oryx-Installation (BPMN-Tool)
- Debian-Paket libapache2-mod-auth-openid ist benutzbar.
 - Relativ einfach, nur Einstellungen in Apache-Konfiguration nötig:

```
<Location /openid/secure>  
    AuthType OpenID  
    require valid-user  
    AuthOpenIDTrusted ^https://uni-h.de/idp/idp.php$  
</Location>
```

- Eingabemöglichkeit für OpenID muss geschaffen werden.

Vorteile

- Nicht jede kleine Webanwendung braucht eine komplette Passwortverwaltung. Vergessene Passwörter und ausgelaufene Nutzer betreffen nur den IdP-Betreiber.
 - aber: Rechteverwaltung weiterhin nötig
- Die Hürde für den Benutzer, sich registrieren zu müssen, fällt weg. Anwendungen können einfacher „ausprobiert“ werden.
 - aber: Achtung bei der Anzeige der Benutzernamen (in Foren, etc.)

Nachteile

- Jede angebundene Anwendung ist abhängig von einem funktionierenden WebSSO-Server.
 - Redundanz
- Ein kompromittiertes Passwort betrifft viele Anwendungen
 - keine kritischen Systeme anbinden
- Es existiert kein zuverlässiges, gleichwertiges Single-Log-out-Verfahren.
 - Nutzer müssen „erzogen“ werden