

Shibboleth IdP-Erweiterungen an der Freien Universität Berlin

Informative Login-Webseiten, JAAS-Login-
Module, Login-Handler, IdP-Logout, spezielle
Datenkonnektoren

Inhalt

- Einsatz von Shibboleth
- Anforderungen an das Login
- Realisierung des Logins
 - Informative Login-Webseite
 - JAAS-Login-Modul-Implementierungen
 - Login-Optionen
 - Authentication Context Classes
 - Login-Handler-Implementierung
- Anforderungen an das Logout
- Realisierung des Logouts
 - Logout-Mechanismus
 - Logout-Webseiten
- (Spezielle Datenkonnektoren)

Einsatz von Shibboleth

- Teilnahme an DFN-AAI („Advanced“ Föderation)
- Eigene Föderation mit aktuell 34 Systemen (~50% produktiv)
- Nicht nur mit Fokus Single Sign-On, sondern auch für latent unsichere Systeme, die eine Authentifizierung gegen zentrales IDM benötigen

Anforderungen an das Login

- Praxiserfahrung: Direkter Aufruf der Login-Webseite (bookmarked) soll zu einem sprechenden Fehler führen
- Praxiserfahrung: Prüfung und Hinweis auf deaktivierte Cookies auf Login-Webseite
- Beim erstmaligen Login sollen Informationen zum verwendeten Service Provider auf der Login-Seite angezeigt werden
- Authentifizierung gegen zwei Account-Domänen
 - FU-Accounts und Intranet-Accounts
 - Intranet-Accounts sind Teilmenge
 - In beiden Domänen gleicher Benutzername
 - Passwörter sind aber unterschiedlich
 - Es sollen also beide Passwörter funktionieren
 - Service Provider müssen zum Teil wissen, welcher Account verwendet wurde (normales Passwort oder Intranet-Passwort)
- Einführung starker Authentifizierungsverfahren (Evaluation)

Direkter Aufruf der Login-Webseite

i.d.R. `https://<hostname>/<path-to-idp-webapp>/Authn/UserPassword`



Home » Dienstübersicht

Fehler

Sie haben die Login-Seite direkt aufgerufen oder Ihre Sitzung ist abgelaufen!

Bitte wählen Sie zunächst die Webanwendung, für die Sie sich anmelden möchten, aus der nachfolgenden Liste aus.

Webanwendungen, die am Single Sign-On teilnehmen:

Bitte beachten Sie, dass manche Anwendungen nicht für alle Benutzer zugänglich sind.

BIOS	Beschaffung im Online Shop - dienstliche Beschaffungen für Mitarbeiter der Freien Universität Berlin
Blogs	Blogs für Lehrende und Mitarbeiter/innen der Freien Universität Berlin
EasyDB	Digitalisierte Bildbestände des Fachbereichs Geschichts- und Kulturwissenschaften der Freien Universität und digitalisierte Bildbestände des Museums für Asiatische Kunst
SEP	System zur Selbsterfassung der Publikationen für Angehörige der Freien Universität Berlin

Direkter Aufruf der Login-Webseite, technisch

- Prüfung, ob Login-Context vorhanden ist
- Wenn Login-Context fehlt, dann muss geprüft werden, ob Cookies gesetzt werden können (Testcookie wird generiert)
- Wenn setzen von Cookies möglich und Login-Context fehlt, dann zu 99% direkter Aufruf des Logins ohne vorherige Auswahl eines Service Providers

→ Java Hilfsklassen werden auf Anfrage bereitgestellt

Direkter Aufruf der Login-Webseite, Quellcode

```
if (entityId == null) {
    try {
        LoginContext loginContext = LoginContextHelper.getLoginContext(request, this);
        if (loginContext != null) {
            entityId = loginContext.getRelyingPartyId();
        }
    } catch (CookiesNotAvailableException e) {
        ...
        CookieHelper.setTestCookie(request, response);
        String url = UrlHelper.buildUrl(request, TEST_COOKIE_PAGE);
        response.sendRedirect(url);
        return;
    } catch (LoginContextNotAvailableException e) {
        ...
        String url = UrlHelper.buildUrl(request, NO_SP_SELECTED_PAGE);
        response.sendRedirect(url);
        return;
    }
}
...
}
```

Informative Login-Webseite

[ZEDAT](#) [FU Berlin](#)

Single Sign-On



[Home » Login](#)

[« zurück](#)

[- Zugangsdaten](#)

[- Hilfe](#)

Single Sign-On der Freien Universität Berlin

Nach der Anmeldung können Sie die Webanwendung BIOS sowie weitere an das Single Sign-On angeschlossene Webanwendungen nutzen, ohne erneut nach Benutzernamen und Passwort gefragt zu werden.

Bitte melden Sie sich an.

Single Sign-On

Benutzername:

Passwort:

Anmelden

Hinweis

Bitte verwenden Sie die Zugangsdaten Ihres FU-Accounts, die Sie von der ZEDAT erhalten haben.

BIOS

Beschaffung im Online Shop - dienstliche Beschaffungen für Mitarbeiter der Freien Universität Berlin

Informative Login-Webseite, technisch

- Ermittlung der entityId des Service Providers
- Informationen aus LDAP holen
- Implementierung setzt auf Attribute-Resolver auf
- Einfache Anpassung der service.xml

```
<srv:Service id="fudis.ServiceProviderResolver"
    xsi:type="attribute-resolver:ShibbolethAttributeResolver">
    <srv:ConfigurationResource file="$IDP_HOME$/conf/fudis-spi-resolver.xml"
        xsi:type="resource:FilesystemResource" />
</srv:Service>
```

```
<srv:Service id="shibboleth.ServiceServletContextAttributeExporter"
    depends-on="shibboleth.AttributeResolver shibboleth.AttributeFilterEngine
        ... fudis.ServiceProviderResolver"
    xsi:type="srv:ServletContextAttributeExporter" />
```

→ Java Hilfsklassen werden auf Anfrage bereitgestellt

Anforderung: Authentifizierung gegen zwei Account-Domänen

Variante 1:

- Mit JAAS gegen LDAP
- login.config mit `edu.vt.middleware.ldap.jaas.LdapLoginModule`
- `setLdapPrincipal=„false“` & `setLdapDnPrincipal=„true“`
(erst ab vt-ldap 3.x)
- Ergebnis: DN wird dem Attribute-Resolver als Principal-Name (PN) übergeben
- Problem: Ermittlung des DN in anderer Account-Domäne sehr aufwändig
→ komplizierte attribute-resolver.xml mit min. zwei zusätzlichen LDAP-Requests
- `setLdapPrincipal=„true“` & `setLdapDnPrincipal=„true“` ist unsinnige Konfiguration, da immer nur der erste Principal aus einem Set vom IdP ausgewertet wird
→ das ist der `LdapPrincipal` und NICHT der `LdapDnPrincipal`

Anforderung: Authentifizierung gegen zwei Account-Domänen

Variante 2:

- Erweiterung von `edu.vt.middleware.ldap.jaas.LdapLoginModule`
- Option: `setPrincipalNameAttribute` (z.B. uid)
 - Attributwert aus LDAP ersetzt Wert aus Eingabemaske
 - z.B. keine Leerzeichen am Ende des Benutzernamens, die bei LDAP ja keine Probleme bereiten
 - Authentifizierung mit z.B. E-Mail-Adresse möglich (wie bei Verwendung des DN's)
- Option: `setRealm` (z.B. @intranet.fu-berlin.de)
 - wird an den `PrincipalName` angehängt

→ Modul wird auf Anfrage bereitgestellt

JAAS-Login-Modul für Exlibris (Aleph)

- UB enthält Nutzer, die nicht dem zentralen IDM bekannt sind
- z.B. Bürgerinnen und Bürger aus Berlin und Brandenburg
- Eigener IdP mit Authentifizierung gegen UB-Benutzer
- Technisch Nutzung des XService von Exlibris zur Authentifizierung
→ Implementierung eines speziellen JAAS-Login-Moduls für XService-Protokoll
- **Gesamtes Thema „UB und Shibboleth“ ist eigener Vortrag**
→ weitere Account-Domäne muss betrachtet werden

Login-Optionen in SAML2

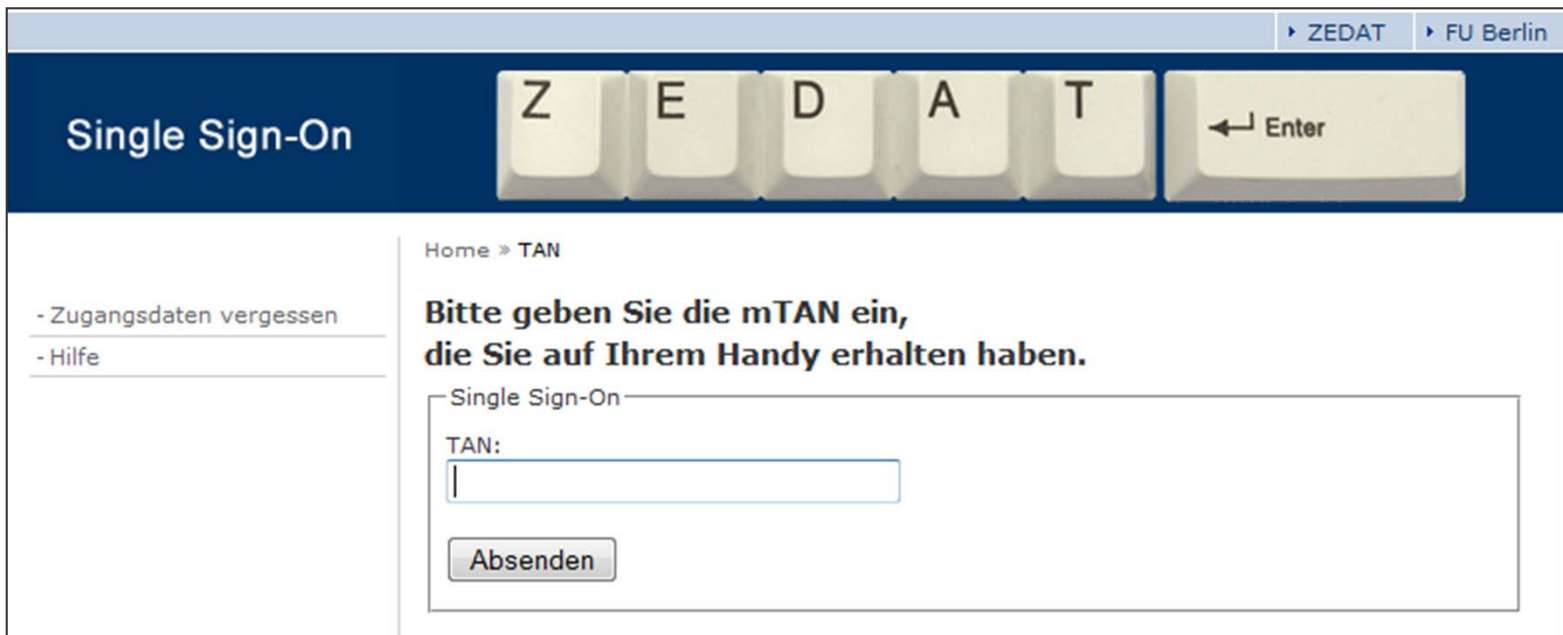
- forceAuthn: Benutzer erhält in jedem Fall eine Login-Maske (in Abhängigkeit vom Wert isPassive)
- isPassive: Benutzer wird authentifiziert, ohne eine Login-Maske angezeigt zu bekommen
- <http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf>
- Optionen werden vom Service Provider gesetzt (beide per Default „false“)
- <https://spaces.internet2.edu/display/SHIB2/NativeSPSessionInitiator#NativeSPSessionInitiator-SAML2SessionInitiator%28ProtocolHandler%29>

Authentication Context Classes in SAML2

- <http://docs.oasis-open.org/security/saml/v2.0/saml-authn-context-2.0-os.pdf>
- Hierarchie von Klassen
- Service Provider legt benötigte Klasse fest
- authnContextClassRef (URI)
- authnContextComparison ("exact", "minimum", "maximum", "better") (default is "exact")
- Standard-Klasse:
urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport
- <https://spaces.internet2.edu/display/SHIB2/NativeSPSessionInitiator#NativeSPSessionInitiator-SAML2SessionInitiator%28ProtocolHandler%29>
- Vom IdP akzeptierte Klassen werden in handler.xml festgelegt
- IdP in der Version 2.2.x kann Hierarchie nicht verarbeiten, es geht nur exakter Vergleich
- Problem: Hierarchie muss festgelegt werden → nicht immer einfach

Login-Handler-Implementierung

- Nach Benutzername und Passwort werden weitere Authentifizierungsverfahren nachgelagert
- Der Benutzername ist ja bereits bekannt



The screenshot shows a web browser window with a blue header bar. On the right side of the header, there are two links: 'ZEDAT' and 'FU Berlin'. Below the header, the main content area has a dark blue bar with the text 'Single Sign-On' on the left. To the right of this bar is a graphic of keyboard keys for 'Z', 'E', 'D', 'A', 'T', and an 'Enter' key. Below this, the main content area is white. On the left side of this area, there are two links: '- Zugangsdaten vergessen' and '- Hilfe'. To the right of these links, there is a breadcrumb trail 'Home » TAN'. Below the breadcrumb, there is a bold instruction: 'Bitte geben Sie die mTAN ein, die Sie auf Ihrem Handy erhalten haben.' Below this instruction, there is a label 'Single Sign-On' followed by a large text input field. Inside the input field, the text 'TAN:' is visible. Below the input field, there is a button labeled 'Absenden'.

DEMO!

→ Implementierungsdetails werden auf Anfrage mitgeteilt

Anforderungen an das Logout

- Sehr kontroverse Diskussion innerhalb der FU Berlin
- Von „nur Aufforderung zum Schließen aller Browserfenster“ bis „Single Logout (SLO)“ alles gewünscht
- SLO wird vom Service Provider in der Version 2.x unterstützt, vom IdP aber noch nicht
- <https://spaces.internet2.edu/display/SHIB2/SLOIssues>

Umsetzung des Logouts an der FU Berlin

- Webanwendung auf Service Provider löscht eigene Session
- Anschließend wird lokaler Shibboleth-Logout beim Service Provider aufgerufen

```
<LogoutInitiator type="Chaining" Location="/Logout" relayState="cookie">  
  <!--LogoutInitiator type="SAML2" template="bindingTemplate.html"/-->  
  <LogoutInitiator type="Local"/>  
</LogoutInitiator>
```

- In localLogout.html Weiterleitung zu einer Logout-Seite auf dem IdP
 - IdP löscht Session
 - **ACHTUNG:** Aufgrund eines Filters in der web.xml reicht es nicht, die Cookies zu löschen. Es ist auch keine „saubere Lösung“
 - Nachteil der Lösung: Sessions auf anderen Service Providern leben eventuell noch weiter → Benutzer wird aber angezeigt, auf welchen Webseiten er wahrscheinlich noch angemeldet ist
- Java Hilfsklassen werden auf Anfrage bereitgestellt

Logout-Webseiten

[ZEDAT](#) [FU Berlin](#)

Single Sign-On

Z E D A T Enter

[Home](#) » [Logout](#)

Abmeldung vom Single Sign-On der Freien Universität Berlin

Sie haben sich in dieser Sitzung bei den folgenden Webanwendungen angemeldet:

- [Blogs](#)
- [Softwareportal](#)

Wenn Sie mit einer der Anwendungen weiterarbeiten wollen, klicken Sie einfach auf das entsprechende Link in der Liste.

Bitte klicken Sie hier, um sich wirklich abzumelden.

Single Sign-On

abmelden

Hinweis

Wenn Sie sich jetzt abmelden, dann sind Sie vom Single Sign-On der Freien Universität Berlin abgemeldet. Es kann jedoch sein, dass Sie noch für eine befristete Zeit bei den von Ihnen besuchten Webanwendungen angemeldet bleiben.

Um ganz sicher zugehen, dass Sie von allen Webanwendungen abgemeldet sind, schließen Sie bitte nach dem Abmelden **alle** Browserfenster.

Spezielle Datenkonnektoren

- Nach erfolgreicher Authentifizierung holt sich IdP Daten zu dem Benutzer aus verschiedenen Datenquellen
 - Datenquellen und Attribute werden in attribute-resolver.xml definiert
 - Es existieren Standard-Konnektoren zu LDAP und SQL
 - z.B. Webservice-Konnektoren müssen selbst implementiert werden
 - <https://spaces.internet2.edu/display/SHIB2/IdPDevExtDataCtr>
 - Bestimmte Datenquellen sollen nur bei Bedarf angefragt werden
 - z.B. Finanzdaten für wenige spezielle Service Provider
 - Nimmt Last von bestimmten Systemen
 - Implementierung, bei der der Datenkonnektor nur für bestimmte Service Provider aktiv wird
- Implementierungsdetails werden auf Anfrage mitgeteilt

Ende, Kontakt, Diskussion

Vielen Dank!

E-Mail: steffen.hofmann@fu-berlin.de