

# deutsches forschungsnetz

DEN

## Wir basteln einen Interceptor Flow

Shibboleth Workshop DFN/ZEDAT | 22./23. Nov. 2018

Wolfgang Pempe ([pempe@dfn.de](mailto:pempe@dfn.de))



- ▶ Attributfreigabe an Service Provider – unterschiedliche Rechtsgrundlagen
  1. „Freiwillige“ Nutzung – Art 6.1 a) → Einwilligung
  2. „Nützliche Dienste“ (z.B. hochschulintern) – Art. 6.1 e) oder f)  
→ berechtigtes Interesse der Einrichtung / des Dienstansbieters
  3. „Notwendige“ Dienste → Art. 88 mit BDSG § 26  
→ Durchführung des Beschäftigungsverhältnisses
- ▶ Unterschiedliche Gestaltung / Beschriftung des User Consent Moduls
- ▶ Logging: Unterscheidung der Anwendungsfälle → Nachweispflicht
- ▶ Vortrag der Forschungsstelle Recht im DFN auf der 69. Betriebstagung:  
[https://www.dfn.de/fileadmin/3Beratung/Betriebstagungen/bt69/BT69\\_AAI\\_DS-AAI-Verfahren\\_Strobel\\_Moerike.pdf](https://www.dfn.de/fileadmin/3Beratung/Betriebstagungen/bt69/BT69_AAI_DS-AAI-Verfahren_Strobel_Moerike.pdf)

# 1. Einwilligung

**DFN**  
DEUTSCHES FORSCHUNGSNETZ

**DFN Test IdP 3 (Development)**

Anmelden bei DFN SAML2 Test-SP

Benutzername

Passwort

Anmeldung nicht speichern

Lösche die frühere Einwilligung zur Weitergabe Ihrer Informationen an diesen Dienst.

Anmeldung

2018-11-22

Interceptors

**DFN**

DEUTSCHES FORSCHUNGSNETZ

**DFN**

DEUTSCHES FORSCHUNGSNETZ

Sie sind dabei auf diesen Dienst zuzugreifen:

**DFN SAML2 Test-SP** von DFN-Verein - Deutsches Forschungsnetz

Beschreibung dieses Dienstes:

*DFN Test-SP2 der DFN-AAI-Testföderation, SAML2-only*

[Zusätzliche Informationen über diesen Dienst](#)

## An den Dienst zu übermittelnde Informationen

Angezeigter Name	<b>Test DSGVO</b>
Berechtigung	<b>urn:mace:dir:entitlement:common-lib-terms</b>
Zugehörigkeit (+ Einrichtung)	<b>employee@testscope.dfn.de staff@testscope.dfn.de member@testscope.dfn.de</b>
E-Mail	<b>test-dsgvo@aai.dfn.de</b>
Heimatinstitution	<b>DFN Test Organization</b>

**Zusätzlich wird eine pseudonyme Kennung (transient oder persistent Id) übertragen.**

[Datenschutzinformationen dieses Dienstes](#)

Um auf den von Ihnen ausgewählten Dienst (Service Provider) zugreifen zu können, müssen die hier angezeigten Informationen an diesen Dienst übertragen werden.

- Ich willige ein, dass diese Informationen einmalig übertragen werden.
- Ich willige ein, dass diese Informationen in Zukunft an diesen Dienst übertragen werden. Diese Entscheidung kann jederzeit mit der Checkbox auf der Anmeldeseite geändert werden.

Einwilligungen können für die Zukunft jederzeit widerrufen werden. Durch den Widerruf von Einwilligungen wird die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung nicht berührt. Für bereits übertragene Informationen entfaltet daher der Widerruf keine Wirkung. Kontaktdaten entnehmen Sie bitte der [Datenschutzerklärung](#).

Abbrechen

[Drucken](#)

Informationen übertragen

## 2. Berechtigtes Interesse

**DFN**  
DEUTSCHES FORSCHUNGSNETZ

**DFN Test IdP 3 (Development)**

Anmelden bei DFN-AAI Attribute Viewer

Benutzername

Passwort

Anmeldung nicht speichern

Die an den Dienst zu übermittelnden Informationen erneut anzeigen.

Anmeldung

**DFN**  
DEUTSCHES FORSCHUNGSNETZ

**DFN**  
DEUTSCHES FORSCHUNGSNETZ

Sie sind dabei auf diesen Dienst zuzugreifen:

**DFN-AAI Attribute Viewer** von DFN-Verein - Deutsches Forschungsnetz

Beschreibung dieses Dienstes:

*DFN-AAI Attribute Viewer (Test-SP3)*

[Zusätzliche Informationen über diesen Dienst](#)

### An den Dienst zu übermittelnde Informationen

Angezeigter Name	<b>Test DSGVO</b>
Berechtigung	<b>urn:mace:dir:entitlement:common-lib-terms</b>
Zugehörigkeit (+ Einrichtung)	<b>employee@testscope.dfn.de staff@testscope.dfn.de member@testscope.dfn.de</b>
E-Mail	<b>test-dsgvo@aai.dfn.de</b>
Heimatinrichtung	<b>DFN Test Organization</b>
<b>Zusätzlich wird eine pseudonyme Kennung (transient oder persistent Id) übertragen.</b>	

[Datenschutzinformationen dieses Dienstes](#)

- Diese Informationen das nächste Mal wieder anzeigen.
- Diese Informationen zukünftig nicht mehr anzeigen. Diese Entscheidung kann jederzeit mit der Checkbox auf der Anmeldeseite geändert werden.

**Die Übertragung der o.g. Informationen erfolgt auf Grundlage von Art. 6 Abs. 1 lit. e oder f DSGVO. Sie können der Übertragung der o.g. Daten gem. Art. 21 DSGVO widersprechen. Schließen Sie hierzu den Browser und wenden sich an die in der [Datenschutzerklärung](#) bezeichnete verantwortliche Stelle.**

Weiter

# 3. Dienstl. Verpflichtung



**DFN**  
DEUTSCHES FORSCHUNGSNETZ

**DFN Test IdP 3 (Development)**

Anmelden bei DFN Test SP  
(SAML1+2)

Benutzername

Passwort

Anmeldung nicht speichern

Die an den Dienst zu übermittelnden Informationen erneut anzeigen.

Anmeldung



Sie sind dabei auf diesen Dienst zuzugreifen:  
**DFN Test SP (SAML1+2)** von DFN-Verein - Deutsches Forschungsnetz

Beschreibung dieses Dienstes:  
*SP der DFN-AAI-Testföderation, SAM11 und SAML2*

[Zusätzliche Informationen über diesen Dienst](#)

An den Dienst zu übermittelnde Informationen	
Angezeigter Name	<b>Test DSGVO</b>
Berechtigung	<b>urn:mace:dir:entitlement:common-lib-terms</b>
Zugehörigkeit (+ Einrichtung)	<b>employee@testscope.dfn.de staff@testscope.dfn.de member@testscope.dfn.de</b>
E-Mail	<b>test-dsgvo@aai.dfn.de</b>
Heimatinstitution	<b>DFN Test Organization</b>
<b>Zusätzlich wird eine pseudonyme Kennung (transient oder persistent Id) übertragen.</b>	

[Datenschutzinformationen dieses Dienstes](#)

- Diese Informationen das nächste Mal wieder anzeigen.
- Diese Informationen zukünftig nicht mehr anzeigen. Diese Entscheidung kann jederzeit mit der Checkbox auf der Anmeldeseite geändert werden.

**Die Übertragung der o.g. Informationen erfolgt auf Grundlage von Art. 88 DSGVO in Verbindung mit Paragraph 26 BDSG (Datenverarbeitung für Zwecke des Beschäftigungsverhältnisses).**

Weiter

- ▶ Information im Log, auf welcher Rechtsgrundlage die Übertragung der Attribute jeweils erfolgte (→ Nachweis)

```
20181121T084856Z|https://testsp2.aai.dfn.de/shibboleth|AttributeReleaseConsent|test-  
dsgvo|displayName,eduPersonEntitlement,eduPersonScopedAffiliation,mail,organizationName|kR33FLRFAn4ZFU  
iymKb1i8AgnGFaS/nvp5r2eTa9iqE=,x7wtAxaDrz4H9nu67g7puu14HK79scDoXKXNppyUJk8=,DCxIC73+Z0SzwqUtL6ujgvQP9x  
T6nL1OyBA6LDjJD9M=,hK4PLh/gyaz7lC1TMAjeGZFrkUD/vXOHwAcsgSBXQy8=,WuV3ah1ICyrESw87cx/YH08ZUnxrCM3FySsV6n  
X+fyM=|true,true,true,true,true  
20181121T085005Z|https://testsp3.aai.dfn.de/shibboleth|ClearAttributeReleaseConsent|test-dsgvo|||  
20181121T085114Z|https://testsp3.aai.dfn.de/shibboleth|AttributeReleaseInfo|test-  
dsgvo|displayName,eduPersonEntitlement,eduPersonScopedAffiliation,mail,organizationName|kR33FLRFAn4ZFU  
iymKb1i8AgnGFaS/nvp5r2eTa9iqE=,x7wtAxaDrz4H9nu67g7puu14HK79scDoXKXNppyUJk8=,DCxIC73+Z0SzwqUtL6ujgvQP9x  
T6nL1OyBA6LDjJD9M=,hK4PLh/gyaz7lC1TMAjeGZFrkUD/vXOHwAcsgSBXQy8=,WuV3ah1ICyrESw87cx/YH08ZUnxrCM3FySsV6n  
X+fyM=|true,true,true,true,true  
20181121T085216Z|https://testsp.aai.dfn.de/shibboleth|ClearAttributeReleaseConsent|test-dsgvo|||  
20181121T085301Z|https://testsp.aai.dfn.de/shibboleth|AttributeReleaseMust|test-  
dsgvo|displayName,eduPersonEntitlement,eduPersonScopedAffiliation,mail,organizationName|kR33FLRFAn4ZFU  
iymKb1i8AgnGFaS/nvp5r2eTa9iqE=,x7wtAxaDrz4H9nu67g7puu14HK79scDoXKXNppyUJk8=,DCxIC73+Z0SzwqUtL6ujgvQP9x  
T6nL1OyBA6LDjJD9M=,hK4PLh/gyaz7lC1TMAjeGZFrkUD/vXOHwAcsgSBXQy8=,WuV3ah1ICyrESw87cx/YH08ZUnxrCM3FySsV6n  
X+fyM=|true,true,true,true,true
```

## Technische Umsetzung

---

---

---



# Flow aus bestehendem Interceptor erstellen

`./system/flows/intercept/attribute-release-beans.xml` und

`./system/flows/intercept/attribute-release-flow.xml`

1.

jeweils kopieren nach:

`./flows/intercept/attribute-info/attribute-info-beans.xml`

`./flows/intercept/attribute-info/attribute-info-flow.xml`

2.

und

`./flows/intercept/attribute-must/attribute-must-beans.xml`

`./flows/intercept/attribute-must/attribute-must-flow.xml`

3.

## Pfade anpassen

In den \*-bean.xml Dateien die relativen Pfadangaben anpassen:

```
<    <import resource="../../conf/audit-system.xml" />
---
>    <import resource="../../system/conf/audit-system.xml" />
```

Desgleichen in den \*-flow.xml Dateien

```
<    <bean-import resource="attribute-release-beans.xml" />
---
>    <bean-import resource="attribute-info-beans.xml" />
```

2.

bzw.

```
<    <bean-import resource="attribute-release-beans.xml" />
---
>    <bean-import resource="attribute-must-beans.xml" />
```

3.

attribute-info-flow.xml

```
<action-state id="ExtractConsent">
  <evaluate expression="ExtractConsent" />
  <evaluate expression="'AttributeReleaseInfo'" />

  <transition on="'AttributeReleaseInfo'" to="'AttributeReleaseInfo'" />
</action-state>

<!-- Write 'AttributeReleaseInfo' event to consent audit log. -->
<action-state id="'AttributeReleaseInfo'">
  <evaluate expression="PopulateConsentAuditContext" />
  <evaluate expression="WriteAttributeReleaseConsentAuditLog" />
  <evaluate expression="'proceed'" />

  <transition on="proceed" to="TestForDoNotRememberConsent" />
</action-state>
```

# Bezeichnung des Events im Log

3.

DFN

attribute-must-flow.xml

```
<action-state id="ExtractConsent">
  <evaluate expression="ExtractConsent" />
  <evaluate expression="'AttributeReleaseMust'" />

  <transition on="'AttributeReleaseMust'" to="'AttributeReleaseMust'" />
</action-state>

<!-- Write 'AttributeReleaseMust' event to consent audit log. -->
<action-state id="'AttributeReleaseMust'">
  <evaluate expression="PopulateConsentAuditContext" />
  <evaluate expression="WriteAttributeReleaseConsentAuditLog" />
  <evaluate expression="'proceed'" />

  <transition on="proceed" to="TestForDoNotRememberConsent" />
</action-state>
```

## Neue Flows bekannt machen (1)

... und mit Activation Conditions verknüpfen:

`/conf/intercept/profile-intercept.xml`

```
<bean id="shibboleth.AvailableInterceptFlows" parent="shibboleth.DefaultInterceptFlows" lazy-init="true">
  <property name="sourceList">
    <list merge="true">
      <bean id="intercept/context-check" parent="shibboleth.InterceptFlow" />

      <bean id="intercept/expiring-password" parent="shibboleth.InterceptFlow" />

      <bean id="intercept/terms-of-use" parent="shibboleth.consent.TermsOfUseFlow" />

      <bean id="intercept/attribute-release" parent="shibboleth.consent.AttributeReleaseFlow"
        p:activationCondition-ref="attribute_release_cond" />

      <bean id="intercept/attribute-info" parent="shibboleth.consent.AttributeReleaseFlow"
        p:activationCondition-ref="attribute_info_cond" />

      <bean id="intercept/attribute-must" parent="shibboleth.consent.AttributeReleaseFlow"
        p:activationCondition-ref="attribute must cond" />
    </list>
  </property>
</bean>
```

## Neue Flows bekannt machen (2)

`/conf/relying-party.xml`

```
<bean id="shibboleth.DefaultRelyingParty" parent="RelyingParty">
  <property name="profileConfigurations">
    <list>
      <bean parent="SAML2.SSO" p:postAuthenticationFlows="#{{'terms-of-use',
        'attribute-release', 'attribute-info', 'attribute-must'}}" />
      <ref bean="SAML2.ECP" />
      <ref bean="SAML2.Logout" />
      <ref bean="SAML2.AttributeQuery" />
      <ref bean="SAML2.ArtifactResolution" />
    </list>
  </property>
</bean>
```

## Activation Conditions

... können in `/conf/intercept/profile-intercept.xml` oder separat, z.B. `./conf/activation-conditions.xml` o.ä. definiert werden. Im letztgegannten Fall muss die betreffende Datei in `profile-intercept.xml` referenziert werden:

```
<import resource="../activation-conditions.xml" />
```

→ Beispiel: `/conf/intercept/profile-intercept.xml`

Doku im Shib-Wiki: <https://wiki.shibboleth.net/confluence/x/S4BKAQ>

# Views und Message Properties (1)

- ▶ Unter `./views/intercept` zusätzlich zu `attribute-release.vm`

**1.**

entsprechende Views anlegen:

- ▶ `attribute-info.vm`

**2.**

- ▶ `attribute-must.vm`

**3.**

- ▶ Diese nach Bedarf anpassen, z.B.

```
<div style="float:left;">
  <p><b>
    #springMessageText("idp.attribute-info.information", "Honestly, you have no choice...")
  </b></p>
</div>
<p style="text-align: center;">
  <input type="submit" name="_eventId_proceed"
  value="#springMessageText("idp.attribute-info.accept", "OK")">
</p>
```

**2.**



## Views und Message Properties (2)

- ▶ Bei `attribute-must.vm` sähe das so aus:

```
<div style="float:left;">
  <p><b>
    #springMessageText("idp.attribute-must.information", "Honestly, you have no choice...")
  </b></p>
</div>
<p style="text-align:center;">
  <input type="submit" name="_eventId_proceed"
  value="#springMessageText("idp.attribute-must.accept", "OK")">
</p>
```

3.

- ▶ Message Properties unter `./messages/messages.properties`

```
idp.attribute-info.accept=Weiter
idp.attribute-must.accept=Weiter
idp.attribute-info.information=Die Übertragung der o.g. Informationen erfolgt auf Grundlage von Art. 6 Abs. 1 lit. e oder f
DSGVO. Sie können der Übertragung der o.g. Daten gem. Art. 21 DSGVO widersprechen. Schließen Sie hierzu den Browser und wend
en sich an die in der <a href="https://www.aai.dfn.de/fileadmin/documents/datenschutz/test-idp.html" target="_blank">Datensc
hutzerklärung</a> bezeichnete verantwortliche Stelle.
idp.attribute-must.information=Die Übertragung der o.g. Informationen erfolgt auf Grundlage von Art. 88 DSGVO in Verbindung
mit Paragraph 26 BDSG (Datenverarbeitung für Zwecke des Beschäftigungsverhältnisses).
```

## Views und Message Properties (3)

- ▶ Beschriftung in `login.vm` dem jeweiligen Use Case anpassen:

```
<div class="form-element-wrapper">
  <input id="_shib_idp_revokeConsent" type="checkbox" name="_shib_idp_revokeConsent" value="true">
  #if ($custom.get("attr_info_sp").apply($profileRequestContext) or $custom.get("attr_must_sp").apply($profileRequestContext))
    <label for="_shib_idp_revokeConsent">#springMessageText("idp.attribute-info.revoke", "Display attribute info again")</label>
  #else
    <label for="_shib_idp_revokeConsent">#springMessageText("idp.attribute-release.revoke",
      "Clear prior granting of permission for release of your information to this service.")</label>
  #end
</div>
```

- ▶ Activation Conditions in `./conf/global.xml` → `CustomViewContext`:

```
<util:map id="shibboleth.CustomViewContext">
  <entry key="attr_must_sp">
    <ref bean="attribute_must_sps"/>
  </entry>
  <entry key="attr_info_sp">
    <ref bean="attribute_info_sps"/>
  </entry>
</util:map>
```

# Vielen Dank! Fragen? Kommentare?

# DFN

## ► Kontakt

### ► DFN-AAI Team

E-Mail: [aai@dfn.de](mailto:aai@dfn.de)

Tel.: +49-30-884299-9124

Fax: +49-30-884299-370

Adresse:

DFN-Verein, Geschäftsstelle

Alexanderplatz 1

D-10178 Berlin

