

DFN-AAI: Anmeldung, Testumgebung, Betrieb

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

- Wie melde ich mich an?
- Wie benutze ich die Testumgebung?
- Wie wird in die Produktiv-Föderation gewechselt?
- Fragen und Diskussion

a.) Der 'offizielle' (aber vielleicht lange und mühsame) Weg: Abschluß Teilnehmervertrag mit dem DFN:

Berechtigt zur Benutzung des Testsystems und Teilnahme an der Produktionsförderung

b.) Der formlose und schnelle Weg: Anmeldung per Mail oder Telefon (<https://www.aai.dfn.de/kontakt/>)

Berechtigt nur zur Benutzung des Testsystems

Wie benutze ich die Testumgebung?

Eingabe der Provider-Metadaten unter <https://www.aai.dfn.de/verwaltung/metadaten/>

The image displays three screenshots of the DFN-AAI web interface, illustrating the process of entering provider metadata.

Left Screenshot: Benutzer Anmeldung
The user login page shows a navigation menu on the left and a login form. The form includes fields for "Benutzername:" (containing "md0") and "Passwort:" (containing "*****"), and an "Anmelden" button.

Middle Screenshot: Metadatenverwaltung
The metadata management page shows a navigation menu and a list of metadata categories. A table titled "Providerliste" displays the following data:

Nr	Name	Typ	Fc
7	SP der DFN Testumgebung	SP	DF
6	IdP der DFN Testumgebung	IdP	DF
94	zzz internal Test-IDP (do not use)	IdP	DF
100	test-idp	IdP	DF

Below the table, there is a note: "Bitte beachten Sie dass es bis zu einer Stunde d in den Metadaten aufgenommen worden sind. In vollen Stunde neu generiert." and the next step: "Nächster Schritt: Services bekanntgeben".

Right Screenshot: Formular - Konqueror
The form editing page shows a navigation menu and a form for editing provider metadata. The form includes the following fields:

- Typ* (?)**: SP
- Name* (?)**: SP der DFN Testumgebung
- DisplayName (?)**: DFN Test SP
- Beschreibung (?)**: SP der DFN-AAI-Testföderation
- URL (?)**: https://www.aai.dfn.de/
- Helpdesk (?)**: hotline@aai.dfn.de
- EntityId* (?)**: https://testsp.aai.dfn.de/shibboleth-sp
- techn. Kontakt (?)**: hotline@aai.dfn.de
- admin. Kontakt (?)**: kaehler@dfn.de

The form includes an "Absenden" button.

Wie benutze ich die Testumgebung?

Test Ihres Service Providers mithilfe unseres Test-Identity Providers:

SP-Konfig (shibboleth.xml): wayfURL="https://wayf.aai.dfn.de/DFN-AAI-Test/wayf/"

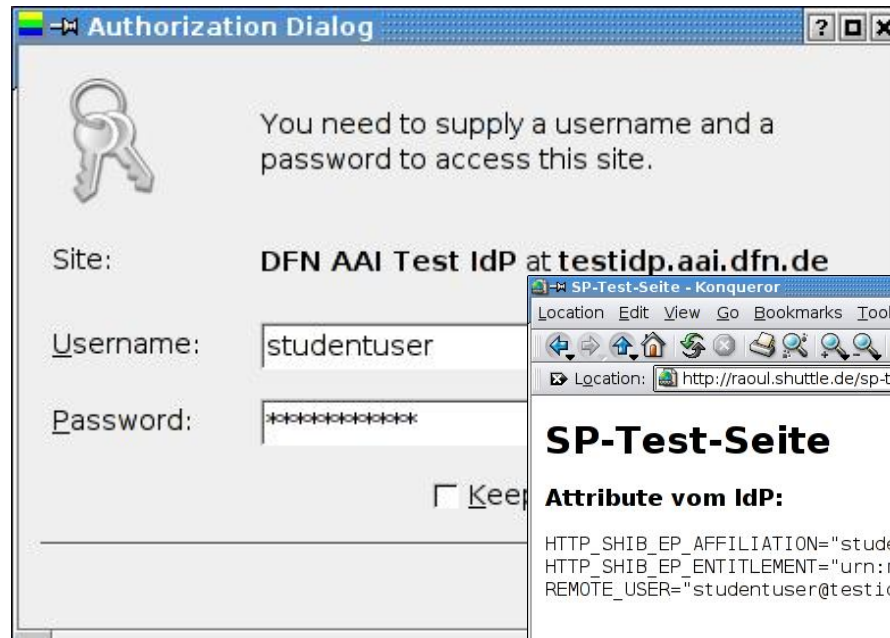
Beim Zugriff auf Ihre SP-Seite findet eine Weiterleitung auf unseren WAYF statt:

Am WAYF wählen Sie
DFN-Test-IdP
aus

The screenshot displays two browser windows. The left window, titled 'raoul.shuttle.de - Konqueror', shows a page with the heading 'SP-Test'. The right window, titled 'DFN-AAI-Test: Home Organization Selection - Konqueror', shows the 'WAYF der DFN-AAI-Testföderation' page. This page features the DFN logo and the text 'WAYF - Where Are You From'. Below this, it explains that this is the localization service for DFN-Test-AAI and that users must authenticate themselves. A section titled 'DFN-AAI-Test: Select your Home Organization' contains a dropdown menu with the following options: Alfred-Wegener-Institut für Polar- und Meeresforschung, Badische Landesbibliothek, C3 Grid DKRZ Hamburg, C3 Grid Projekt am PIK, DAASI IdP, DEMOaar IdP 2, DFN Berlin IdP, **DFN Test-IdP**, and DFN-CERT Services GmbH. A 'Select' button is visible to the right of the dropdown.

Wie benutze ich die Testumgebung?

Der WAYF leitet Sie weiter zum Test-IdP



Authorization Dialog

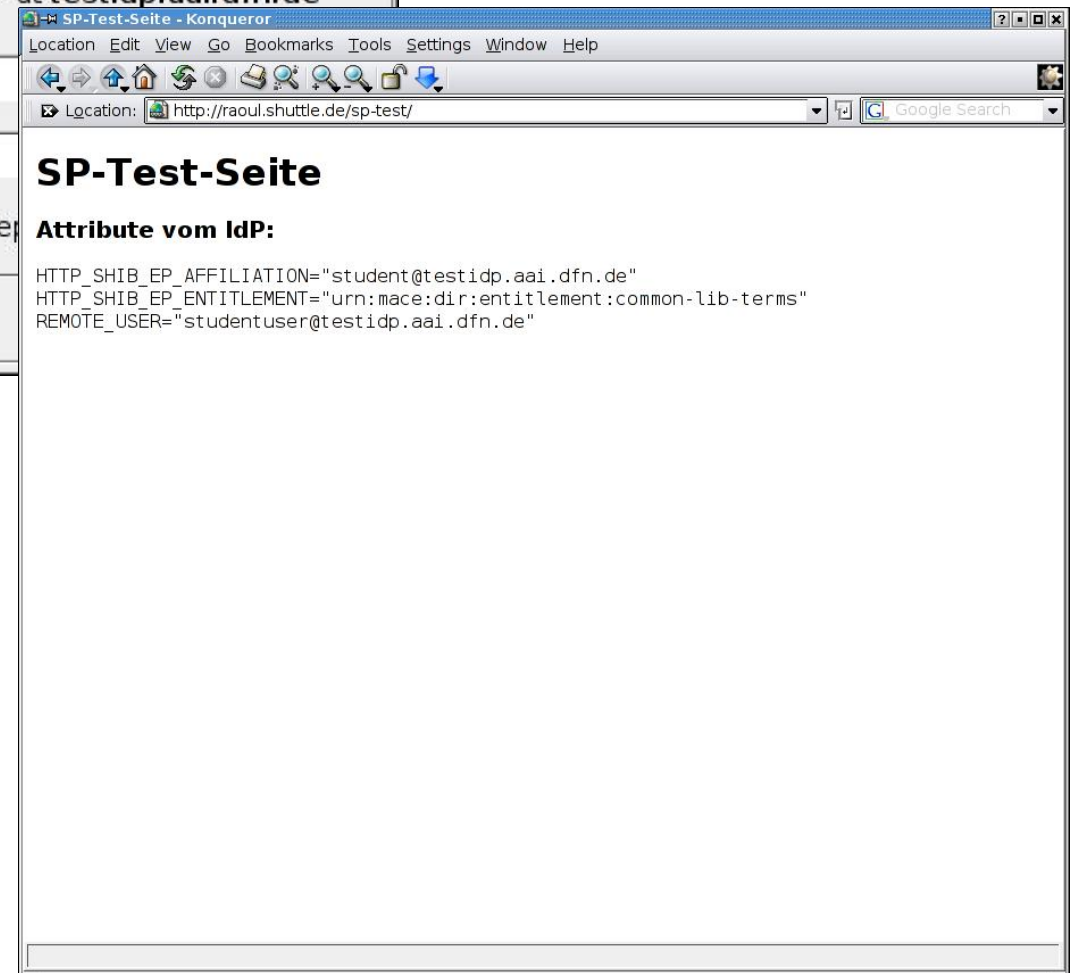
You need to supply a username and a password to access this site.

Site: DFN AAI Test IdP at testidp.aai.dfn.de

Username: studentuser

Password: *****

Keep



SP-Test-Seite - Konqueror

Location Edit View Go Bookmarks Tools Settings Window Help

Location: http://raoul.shuttle.de/sp-test/

SP-Test-Seite

Attribute vom IdP:

```
HTTP_SHIB_EP_AFFILIATION="student@testidp.aai.dfn.de"
HTTP_SHIB_EP_ENTITLEMENT="urn:mace:dir:entitlement:common-lib-terms"
REMOTE_USER="studentuser@testidp.aai.dfn.de"
```

Nach erfolgreicher Authentifizierung sollten Sie zur geschützten SP-Seite zurückgeleitet werden.

Analog können Sie Ihren IdP gegen unseren Test-SP testen!

Vorraussetzungen:

- unterschriebener Teilnehmergevertrag und damit Verpflichtung zur Einhaltung der Föderations-Policy
- gültige anerkannte Zertifikate (möglichst DFN-PKI, andere nach Prüfung durch DFN-PKI-Abteilung)
- Attributschema der DFN-AAI muss unterstützt werden
- erfolgreicher Test in der Testföderation
- Produktionsföderation in der Metadatenverwaltung anklicken ;-)

- DFN-AAI-Team prüft ob die Voraussetzungen erfüllt sind und schaltet den betreffenden Provider ggfs. für die Produktivumgebung frei
- der Technical und Administrative Contact bekommen darüber eine Informationsmail
- Sie müssen nur Ihre Provider geringfügig umkonfigurieren:

SP (shibboleth.xml):

```
<SessionInitiator...  
  wayfURL="https://wayf.aai.dfn.de/DFN-AAI-Test/wayf/"  
</SessionInitiator>
```

```
<SessionInitiator...  
  wayfURL="https://wayf.aai.dfn.de/DFN-AAI/wayf/"  
</SessionInitiator>
```

IdP (idp.xml):

```
<IdPConfig...  
defaultRelyingParty="https://www.aai.dfn.de/DFN-AAI-Test">  
  <RelyingParty...  
    name="https://www.aai.dfn.de/DFN-AAI-Test">  
  </RelyingParty>  
</IdPConfig>
```

```
<IdPConfig...  
defaultRelyingParty="https://www.aai.dfn.de/DFN-AAI">  
  <RelyingParty...  
    name="https://www.aai.dfn.de/DFN-AAI">  
  </RelyingParty>  
</IdPConfig>
```

und natürlich nicht vergessen die Metadaten der Produktionsumgebung zu benutzen!

“Zertifikats-Hürde”

Testumgebung: akzeptiert **beliebige Zertifikate** (self-signed, Versign-Trial, etc.)

Produktivumgebung: akzeptiert nur **im Sinne der DFN-PKI-Policy gültige Zertifikate!**

Vorteil: testen ohne “Zertifikats-Hürde”

Nachteil: mehr Arbeit beim Umstieg in die Produktivföderation!

Unsere Empfehlung:

nehmen Sie zum Testen schon im Sinne der DFN-PKI-Policy gültige Zertifikate welche beim Umstieg in die Produktivumgebung weiter verwendet werden können!

Wie wird in die Produktiv-Föderation gewechselt?

“Zertifikats-Hürde”

Unsere Metadatenverwaltung unterstützt Sie bei der Beurteilung der Zertifikate:

Location Edit View Go Bookmarks Tools Settings Window Help

Location: <https://www.aai.dfn.de/verwaltung/metadaten/zertifikate/> Google Search

Location: [https://www.aai.dfn.de/verwaltung/metadaten/zertifikate/](#)

Zertifikate akzeptiert, für die Übernahme in die Betriebsföderation werden jedoch bestimmte Anforderungen gestellt. Unter der [DFN-PKI FAQ](#) finden sie die jeweils aktuellen Kriterien, die die Zertifikate erfüllen müssen. Aus der [DFN-Hierarchie](#) stammende Zertifikate werden sofort freigeschaltet. Bei Zertifikaten anderer Aussteller werden zuerst deren Policies von uns auf Vereinbarkeit mit der [DFN-AAI-Policy](#) geprüft und die Zertifikate dann gegebenenfalls freigeschaltet oder abgelehnt. Diese Prüfung kann mehrere Werktage dauern.

Um ein ablaufendes Zertifikat innerhalb eines Providers zu ersetzen können sie das neue Zertifikat parallel zum alten eintragen, es werden beide in die Metadaten aufgenommen. Dadurch wird ein Übergang ohne Betriebsunterbrechung ermöglicht.

[neues Zertifikat eintragen](#)

Nr	CommonName	Ablaufdatum	Status	Kommentar	Provider			
39	sgs.dfn.de	2014-05-08 16:36:24	freigeschaltet	found in whitelist		Details	Ändern	Löschen
129	t1	2008-02-07 13:40:31	abgelehnt	certificate not valid: self signed certificate	test-idp	Details	Ändern	Löschen
30	testidp.aai.dfn.de	2012-04-03 11:30:37	freigeschaltet		IdP der DFN Testumgebung	Details	Ändern	Löschen
31	testsp.aai.dfn.de	2012-04-03 11:30:40	freigeschaltet		SP der DFN Testumgebung	Details	Ändern	Löschen
40	www0.shuttle.de	2013-04-17 17:15:07	freigeschaltet		zzz internal Test-IDP (do not use)	Details	Ändern	Löschen

Bitte beachten Sie dass es bis zu einer Stunde dauert, bis Ihre Änderungen oder Ergänzungen in den Metadaten aufgenommen worden sind. Im Moment werden die Metadaten zu jeder vollen Stunde neu generiert.

IdPs geben als nächstes bitte den [Scope](#) ihrer Einrichtung an,
SPs gehen bitte gleich weiter zu den [Attributen](#).

Für alle technischen Fragen rund um die DFN-AAI:

E-Mail: hotline@aai.dfn.de

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

