



AAI & SAP SAML2 for Fiori / UI5

SAP NetWeaver Application Server ABAP as SAML service provider

Daniel Emch

University of Zurich



Trigger: new course catalog

University of Zurich COURSE CATALOGUE Fall Semester 2016 [Login](#) [Deutsch](#) [Help](#)

DIRECTORY SEARCH NOTED ITEMS CALENDAR

1198 Study Progr... 5109 Modules 4690 Courses 5003 Instructors

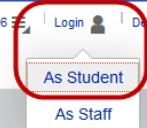
biology in All Remove all

4690 Course(s) found

↑↓No.	≡ Title	↑↓Abbreviation	Instructors	↑↓Category	↑↓Times	Room	Note
3476	Advanced Protein Engineering	BCH420 - English	Andreas Plückthun	Lecture with Practical Exercises	Mon 08:00-09:45		>
2830	Einführung in die Medienökonomie	251295.0 - German	Pascal Barro Isabelle Krebs	Course	Tue 08:00-09:45		>
3762	Land-Climate Interactions	GEO418.2 - English		Lecture with Practical Exercises	Tue 13:15-15:00		>
3809	Physics of Glaciers I	GEO855.1 - German		Lecture with Practical Exercises	to be announced		>
4736	Qualifikationsarbeit zum Seminar: Identität	160521 - German	Peter Schulthess	Seminar	as announced or arranged		>
3029	"Bass is the Place" - Forschungsfeld Hip Hop	721103a - German	Christof Thurnherr	Seminar	Fri 08:00-09:45		>
4824	"Bollywood and Beyond" - Eine Kulturgeschichte des indischen Kinos im 20. Jh.	600350 - German	Philosophische Fakultät N.N.-Dozent	Course	Mon 15:00-17:00		>
4236	"Ist mein Kind hochbegabt?" - Elterngespräche bei Schüler/innen mit auffälligen Lernprozessen	222IKh - German	Eva Susann Becker	Seminar	Tue 12:15-13:45		>

Search criteria:

[Create PDF](#)





Current Situation

The UZH is using the shibboleth service provider (mod_shib, shibd) to protect the SAP online services for students (www.students.uzh.ch/en.html)

All these UZH SAP online services (self-developed BSP-applications) will be replaced within the next two years



The login functionality for these UZH SAP online services is a self-developed BSP-application, which cannot be used without modification for Fiori authentication

The first self-developed UZH SAPUI5 application is the new course catalog (www.courses.uzh.ch), which is available since June 2016

The UZH plans to use the Fiori Launchpad to present the SAP UI5 online services to the students



Goals of the AAI authentication for Fiori / UI5



The authentication technology should be based on well known industry standards



The implementation should be possible without any modifications on SAP and IdP side



It has to be fully integrated in the AAI Federation & Resource Registry



Solution

1.

Configuration of the SAP NetWeaver Application Server ABAP to operate as a SAML service provider (SAP transaction SAML2)

2.

Create service provider in the AAI Resource Registry (<https://rr.aai.switch.ch/>)

3.

Set the logon procedure of the corresponding SAP service to «Alternative Logon Procedure» (SAP transaction SICF)



1. SAP SAML2 transaction

SAML-2.0-Konfiguration des ABAP-Systems: P22/001

Lokaler Provider Vertrauenswürdige Provider Richtlinien Namensbezeichnerverwaltung

Bearbeiten Sichern Abbrechen Deaktiv. Metadaten Konfiguration löschen Konfiguration exportieren

Provider-Name:

Betriebsart:

Status: Aktiviert

Allgemeine Einstellungen Authentifizierungskontexte Service-Provider-Einstellungen

Signatur und Verschlüsselung

Signierschlüsselpaar:

VerschlüsselSchlüsselpaar:

Zertifikat in Signatur aufnehmen

Metadaten signieren

Verschiedenes

Zeitversatztoleranz: Sekunden

SAML-2.0-Konfiguration des ABAP-Systems: P22/001

Lokaler Provider Vertrauenswürdige Provider Richtlinien Namensbezeichnerverwaltung

Liste vertrauenswürdiger Provider

Anzeigen:

Aktiv	Standard	Name	Alias
<input checked="" type="checkbox"/>	<input checked="" type="radio"/>	https://aai-idp.uzh.ch/idp/shibboleth	IdP
<input type="checkbox"/>	<input type="radio"/>		
<input type="checkbox"/>	<input type="radio"/>		
<input type="checkbox"/>	<input type="radio"/>		

Details d.Identity-Provider "https://aai-idp.uzh.ch/idp/shibboleth"

Endpunkte Identitätsföderation Signatur und Verschlüsselung Authentifizierungsanforderungen

Anzeigen:

Standard	Bindung	Orts-URL
<input checked="" type="radio"/>	HTTP Redirect	https://aai-idp.uzh.ch/idp/profile/SAML2/Redirect/SSO
<input type="radio"/>	HTTP POST	https://aai-idp.uzh.ch/idp/profile/SAML2/POST/SSO



2. AAI Resource Registry

Basic Resource Information	
Federation	SWITCHaai Federation
Home Organization	uzh.ch (SWITCHaai)
EntityID	https://idsapp22.lan.bap.uzh.ch/
Relying Party	Default
Interfederation Enabled	Interfederation support not enabled
GÉANT Data Protection Code of Conduct	Not committed to GÉANT Data Protection Code of Conduct
REFEDS R&S Category	Service not compliant with REFEDS R&S .
Home URL	https://studentservices.uzh.ch/
Helpdesk URL	
Valid from	27 April 2016
Valid until	Valid forever.
Public	Yes If the Resource is marked as public, it will be visible in public Resource listings.
Embedded Certificates	
Certificate	/ C=CH / ST=Zuerich / L=Zuerich / O=Universitaet Zuerich / OU=Business Applications / OU=Zentrale Informatik / CN=idsapp22.lan.bap.uzh.ch Issuer: / C=BM / O=QuoVadis Limited / CN=QuoVadis Global SSL ICA G2 SHA1 Fingerprint: 20:E4:07:64:4D:DD:5C:98:54:49:83:29:C0:82:87:37:4F:98:FD:AB Expiration Date: Apr 8 15:02:54 2019 GMT
Service Locations	
Assertion Consumer Service	https://studentservices.uzh.ch/sap/saml2/sp/acs/001 Binding: urn:oasis:names:tc:SAML:2.0:bindings:PAOS
Assertion Consumer Service	https://studentservices.uzh.ch/sap/saml2/sp/acs/001 Binding: urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Artifact
Assertion Consumer Service	https://studentservices.uzh.ch/sap/saml2/sp/acs/001 Binding: urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST



3. Alternative Logon Procedure (SAP transaction SICF)

The screenshot shows the SAP SICF configuration interface for the 'Alternative Logon Procedure'. The 'Procedure' dropdown is set to 'Alternative Logon Procedure' and is circled in red. Below this, the 'Logon Data' section includes fields for Client, User, Language, and Password Status (set to 'Initial'). The 'Security Requirement' section has 'SSL' selected. The 'Authentication' section has 'Standard SAP User' selected. The 'Reauthentication' section has 'Deactivated system-wide' set to 'No'. At the bottom, the 'Logon Procedure List (in Order of Execution)' is shown, with '2 SAML Logon' circled in red.

Logon Procedure List (in Order of Execution)	
N..	Logon Procedure
1	Logon Through HTTP Fields
2	SAML Logon
3	Logon Through SSL Certificate
4	SAP Logon/Assertion Ticket
5	SAP Assertion Ticket