

# eduGAIN Access Check

Also a Topic of Interest for SWITCHaai?



# SWITCH

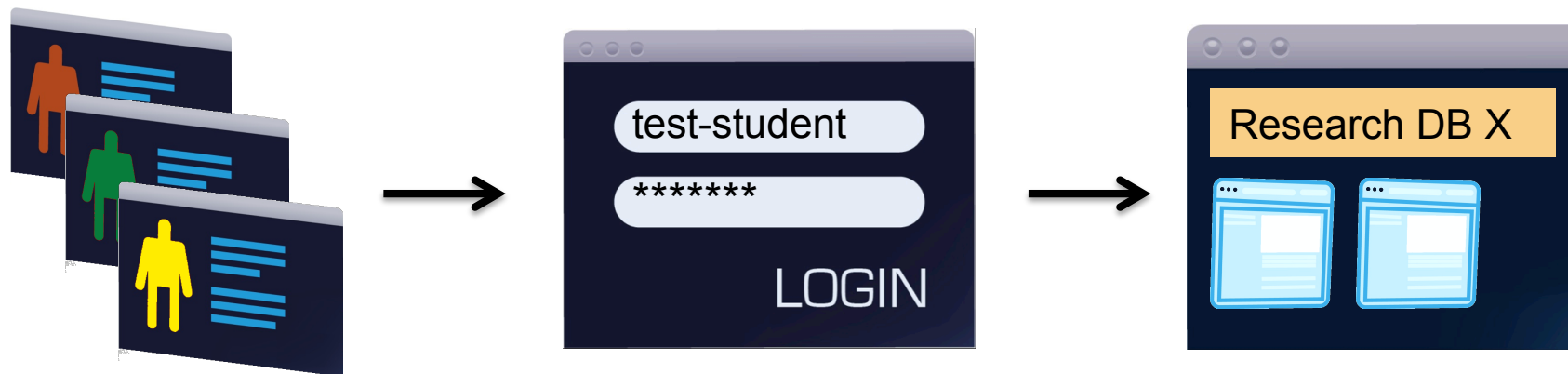
Lukas Hämmerle  
[lukas.haemmerle@switch.ch](mailto:lukas.haemmerle@switch.ch)

Bern, 13. August 2015

# What is this presentation about?

- SWITCH is sometimes asked by (commercial) SP admins:  
*"Can I get a test account in AAI to test my service?"*
- **Why do some SP admins need test accounts?**
  - To validate their SP's behavior also in production environment
- **What's the problem with this request?**
  - (Test) accounts which are not linked to real persons are not allowed in AAI
  - Organisations don't create test identities for people outside their organisation
  - VHO accounts are of limited use for tests and not easy to get
- **Even greater need in Interfederation/eduGAIN context**
  - Federation Partners and their suppliers, cloud providers and research communities often don't have AAI accounts (yet) to test AAI login on their own AAI services
  - GÉANT "Enabling Users" task (led by SWITCH) decided to build **eduGAIN Access Check** service to provide a solution

# The eduGAIN Access Check Basics



Create service-specific **test accounts** with different profiles

Use them for login on **own service only**

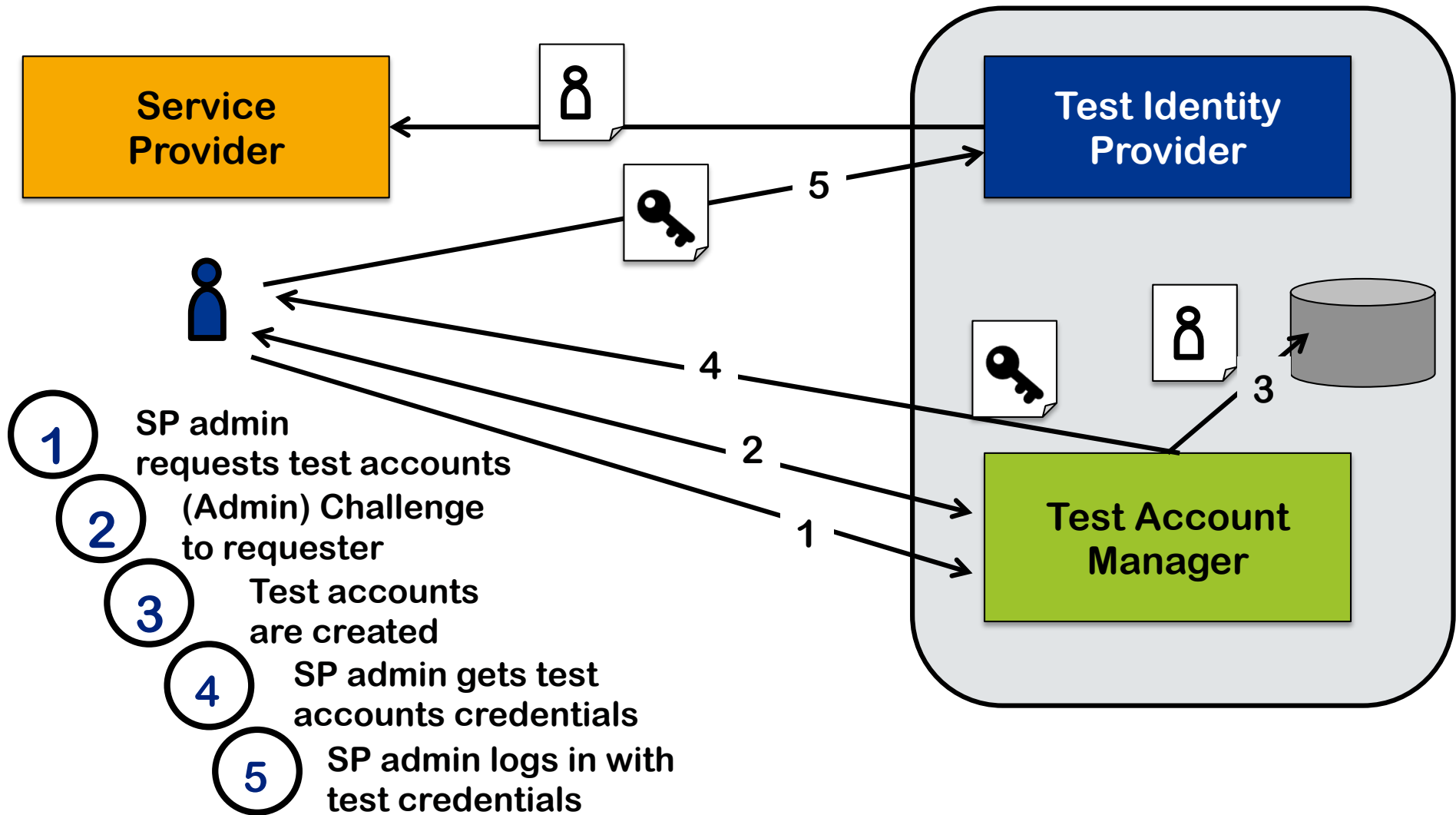
**Check** if access works and attributes are available

- **eduGAIN Access Check acts as Identity Provider** in eduGAIN
- Mainly useful for service operators without an own AAI/federated login (e.g. commercial cloud providers) but generally for AAI SP admins

# Purpose of eduGAIN Access Check

- **A self-service test account provider within eduGAIN to help test access/attribute release to an own federated service**
- **Multiple test accounts with varying attribute sets**
  - with different profiles to simulate real users (incl. non-ascii characters)
  - with different release policies to simulate different IdP behaviors (R&S/CoCo support, missing attributes, all attributes)
- **Restricted use**
  - Validated SP admins can use test accounts to access own service only
  - Test account credentials (currently) expire after a few days
  - Attribute set is fixed and values cannot be changed
  - Identities are clearly marked as test identities

# How does Access Check work?



# Access Check Screenshots



## eduGAIN Access Check

### eduGAIN Access Check?

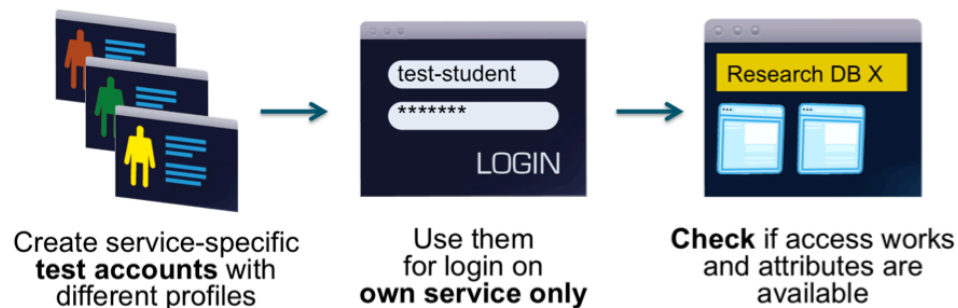
eduGAIN Access Check allows administrators of a Service Provider (SP) registered in [eduGAIN](#) to create test accounts with different profiles to validate the behaviour and test federated login. The test accounts can only be used to access own services. [Learn more about this service...](#)

### Start testing your eduGAIN service

To start testing your own eduGAIN service, start by selecting the Service Provider you are administrator for.

[Go on testing the service](#)

### eduGAIN Access Check basics



<https://access-check.edugain.org/>

# Step 1: Select an AAI Service



## eduGAIN Access Check

1. Select your Service Provider

2. Send email challenge

3. Complete Email Challenge

4. Test Accounts

### Select your Service Provider

Please search and select the Service Provider that you want to test in the list below. You must be an administrator of that Service Provider to continue afterwards.

**Type the SP name or entityID to search for it.**

Note that only Service Providers are in the list which are included in the eduGAIN metadata.

- AAI Attributes Viewer (<https://attribute-viewer.aai.switch.ch/shibboleth>)
- AAI Viewer Interfederation Test (<https://attribute-viewer.aai.switch.ch/interfederation-test/shibboleth>)
- Haka Attribute Test Service (<https://rr.funet.fi/attribute-test>)
- Lifestyles of the Attribute Rich and Privacy Preserved (LARPP) Calendar Server (<https://calendar.larpp.internet2.edu/shibboleth>)
- Lifestyles of the Attribute Rich and Privacy Preserved (LARPP) List Manager (<https://list-manager.larpp.internet2.edu/shibboleth>)
- Lifestyles of the Attribute Rich and Privacy Preserved (LARPP) Registry (<https://registry.larpp.internet2.edu/shibboleth>)
- Lifestyles of the Attribute Rich and Privacy Preserved (LARPP) Wiki (<https://wiki.larpp.internet2.edu/shibboleth>)

# Step 2a: Send (Admin) Challenge

## eduGAIN Access Check

1. Select your Service Provider

2. Send email challenge

3. Complete Email Challenge

4. Test Accounts

### Send email challenge

Before you can create test accounts at this Identity Provider, we need to ensure you are a legitimate administrator of "AAI Attributes Viewer".

#### Select your email address

The email addresses below have been extracted from your SP SAML metadata.

Please select the email address where an email challenge can be sent to validate your identity

aai@switch.ch

Previous

Next



# Step 2b: Email Challenge

From eduGAIN Access Check <edugain-access-check@geant.net> ☆  
Subject eduGAIN Access Check - Test accounts request 15:55  
To SWITCHaai Support ☆

This is an email challenge automatically sent to you by eduGAIN Access Check.  
[viewer.aai.switch.ch/shibboleth](http://viewer.aai.switch.ch/shibboleth).  
The address [aai@switch.ch](mailto:aai@switch.ch) is mentioned in the eduGAIN metadata as a contact f  
To complete the creation of test accounts, paste the following validation tok

Validation token: 3515c026f6752e8711b3

eduGAIN Access Check: <https://access-check.edugain.org/accountmanager>

If the creation of test accounts was not initiated by you or a fellow adminis  
[integration@geant.net](mailto:integration@geant.net) to inform them about a potential abuse of the eduGAIN A

Best Regards  
eduGAIN Access Check Bot

# Step 2c: Enter Challenge One Time Token



## eduGAIN Access Check

1. Select your Service Provider

2. Send email challenge

3. Complete Email Challenge

4. Test Accounts

### Complete Email Challenge

An email challenge including a validation token has been emailed to you at aai@switch.ch. Please copy and paste the validation token in the form below to prove that you are administrator of this service.

#### Validation Token

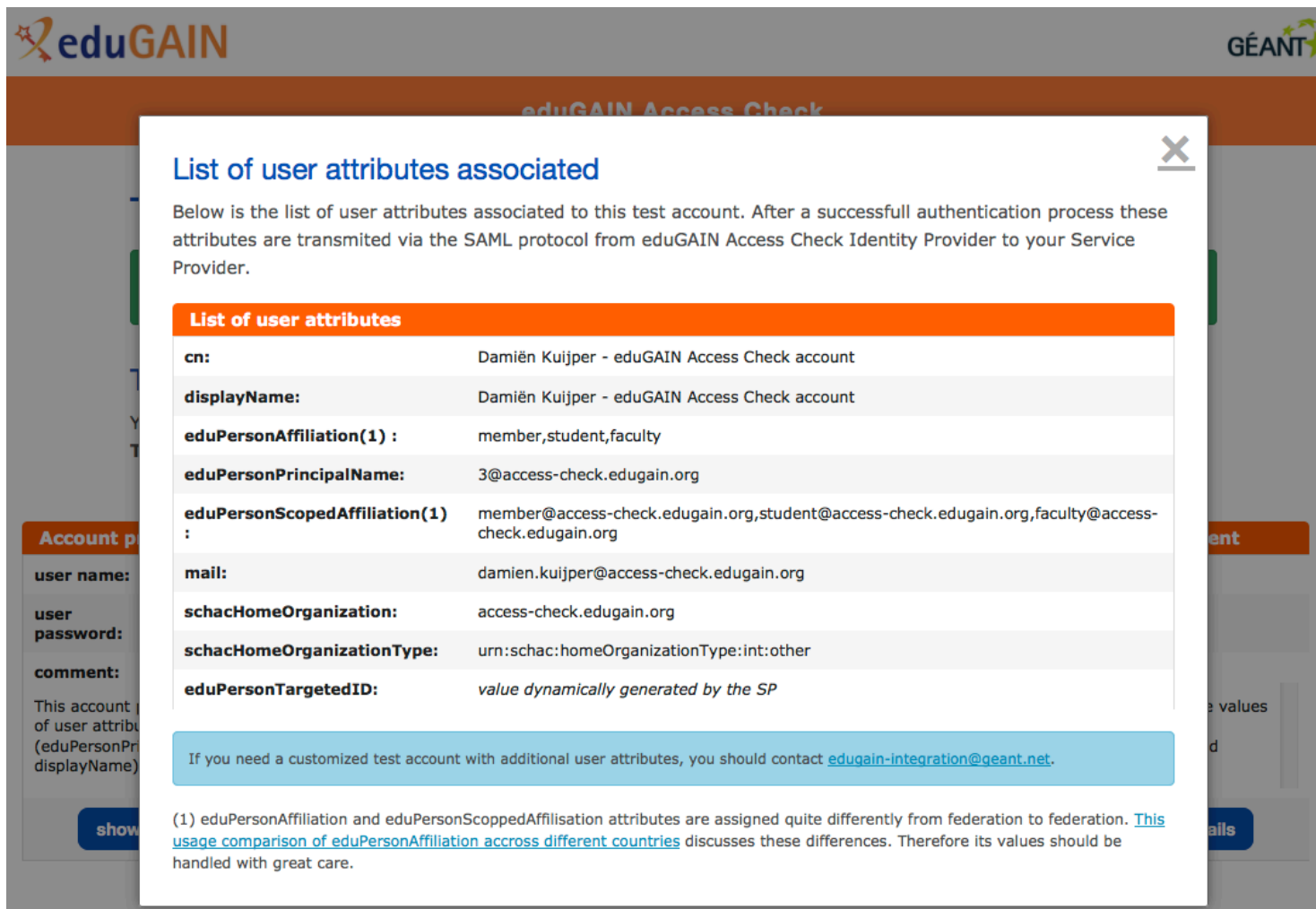
Please provide the validation token here:

3515c026f6752e8711b3

Previous

Next

# Step 3: Inspect Test Account Profiles



The screenshot shows the eduGAIN Access Check interface. A modal window titled "List of user attributes associated" is displayed. The modal contains a list of user attributes and a note about a customized test account.

**List of user attributes associated**

Below is the list of user attributes associated to this test account. After a successful authentication process these attributes are transmitted via the SAML protocol from eduGAIN Access Check Identity Provider to your Service Provider.

| List of user attributes                |   |
|--|---|
| <b>cn:</b>                             | Damiën Kuijper - eduGAIN Access Check account   |
| <b>displayName:</b>                    | Damiën Kuijper - eduGAIN Access Check account   |
| <b>eduPersonAffiliation(1) :</b>       | member,student,faculty  |
| <b>eduPersonPrincipalName:</b>         | 3@access-check.edugain.org  |
| <b>eduPersonScopedAffiliation(1) :</b> | member@access-check.edugain.org,student@access-check.edugain.org,faculty@access-check.edugain.org |
| <b>mail:</b>                           | damien.kuijper@access-check.edugain.org   |
| <b>schacHomeOrganization:</b>          | access-check.edugain.org  |
| <b>schacHomeOrganizationType:</b>      | urn:schac:homeOrganizationType:int:other  |
| <b>eduPersonTargetedID:</b>            | <i>value dynamically generated by the SP</i>  |

If you need a customized test account with additional user attributes, you should contact [edugain-integration@geant.net](mailto:edugain-integration@geant.net).

(1) eduPersonAffiliation and eduPersonScopedAffiliation attributes are assigned quite differently from federation to federation. [This usage comparison of eduPersonAffiliation across different countries](#) discusses these differences. Therefore its values should be handled with great care.

# Step 4: Initiate Login to Your Service


## AAI Attribute Viewer SWITCH

---

The AAI Attribute Viewer displays all attributes that are available about an AAI user. All user information is stored 10 days in a log file before it is automatically deleted.

Please select your Home Organization and log in to see the [AAI attributes](#)  that are available for you.

Login with: > AAI

 eduGAIN Access Check ▼

Remember selection for this web browser session. Login

Alternatively, log in [using an AAI Test Home Organisation](#) or the [Shibboleth Embedded Discovery Service](#).

Use the links below to display the Embedded WAYF in another language.

Display the Embedded WAYF on this page in:  
[In English](#) | [In French](#) | [In German](#) | [In Italian](#)

Test central WAYF:  
[In English](#) | [In French](#) | [In German](#) | [In Italian](#)

# Step 5: Login with Test Account



## eduGAIN Access Check

[English](#) | [Bokmål](#) | [Nynorsk](#) | [Sámegiella](#) | [Dansk](#) | [Deutsch](#) | [Svenska](#) | [Suomeksi](#) | [Español](#) | [Français](#) | [Italiano](#) | [Nederlands](#) | [Lëtzebuergesch](#) | [Čeština](#) | [Slovenščina](#) | [Lietuvių kalba](#) | [Hrvatski](#) | [Magyar](#) | [Język polski](#) | [Português](#) | [Português brasileiro](#) | [Türkçe](#) | [日本語](#) | [简体中文](#) | [繁體中文](#) | [русский язык](#) | [eesti keel](#) | [עברית](#) | [Bahasa Indonesia](#) | [Srpski](#) | [Latviešu](#) | [Românește](#) | [Euskara](#)

### Enter your username and password

A service has requested you to authenticate yourself. Please enter your username and password in the form below.

The login form is enclosed in a red rounded rectangle. It features a light orange background. On the left side, there is a yellow key icon. The 'Username' field contains the text 'user1'. The 'Password' field is filled with ten black dots. Below the fields is a blue button with the text 'Login' in white.

### Help! I don't remember my password.

Too bad! - Without your username and password you cannot authenticate yourself for access to the service. There may be someone that can help you. Consult the help desk at your organization!

eduGAIN Access Check open Beta 1 - [contact us](#)

# Test Account Profiles

- eduGAIN Test IdP creates sets of test accounts with:
  - different user profiles (faculty, student, staff),
  - varying set of attributes and values (including non-ascii chars)
- eduGAIN Test IdP will behave like an average IdP regarding attribute release (CoCo, R&S)
- Test accounts profile customization
  - requester should have the ability to customize attribute values
  - planned for phase II of the service

# Access Check also for SWITCHaai?

- Currently eduGAIN Access Check can only be used by SWITCHaai services that enabled Interfederation/eduGAIN support
- **Should localized version of Access Check also be included in SWITCHaai?**
  - Access Check IdP metadata would be in SWITCHaai metadata
  - Would not be shown in WAYF/Discovery Service by default due to standardized "Hide-from-Discovery" entity category in metadata. Manually enable in Embedded WAYF or use login link.
  - Would provide SWITCHaai-specific attributes (e.g. uniqueID)