eduGAIN Access Check

Also a Topic of Interest for SWITCHaai?

Lukas Hämmerle
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 acounts 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
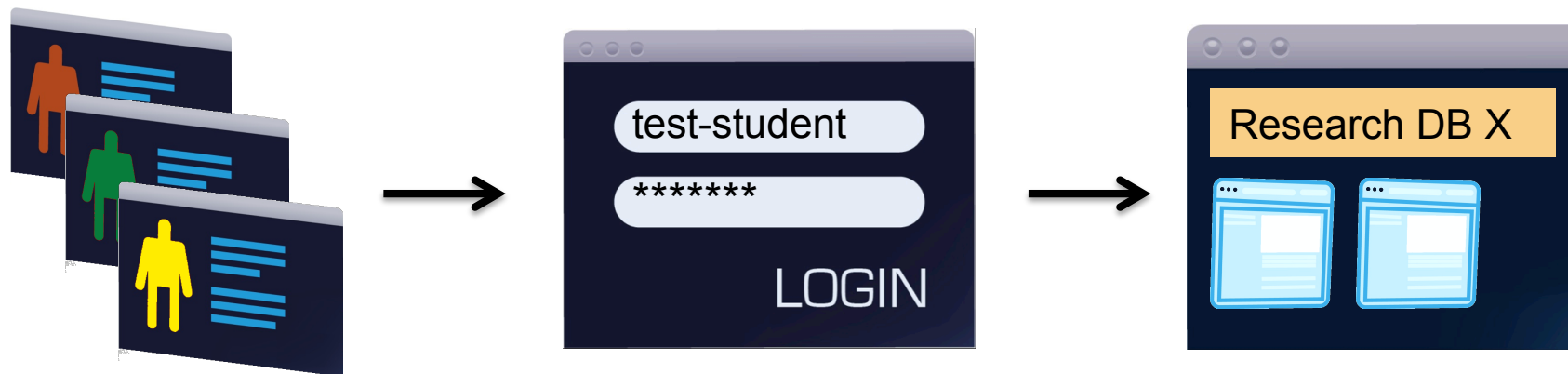
Create service-specific
test accounts with
different profiles
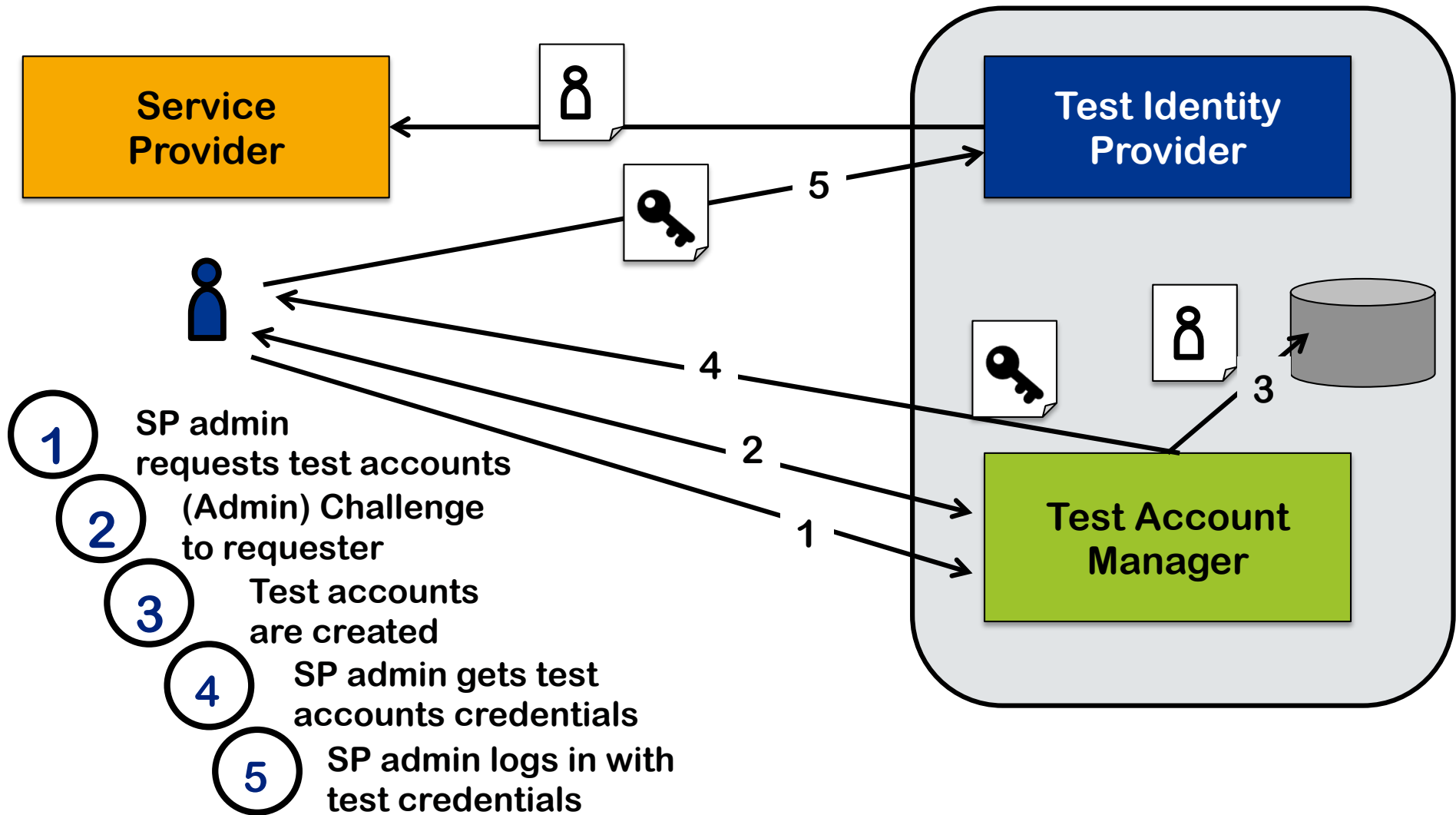
Use them
for login on
own service only

Check if access works
and attributes are
available

(Research DB X)
(test-student)
(LOGIN)

- **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 <u>to access own service only</u>
  - 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?

Service Provider

Test Identity Provider

5

4

2

1

Test Account Manager

3

1 SP admin requests test accounts

2 (Admin) Challenge to requester

3 Test accounts are created

4 SP admin gets test accounts credentials

5 SP admin logs in with test credentials

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

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

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

Check if access works and attributes are available

https://access-check.edugain.org/
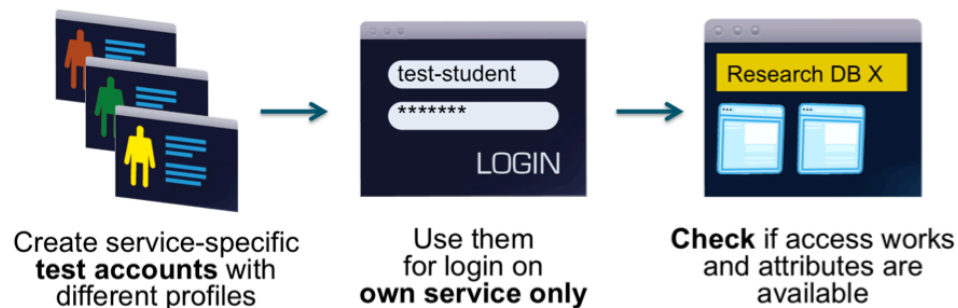
Step 1: Select an AAI Service

Step 2a: Send (Admin) Challenge

© 2015 SWITCH

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.
The address 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 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 proof that you are administrator of this service.

Validation Token
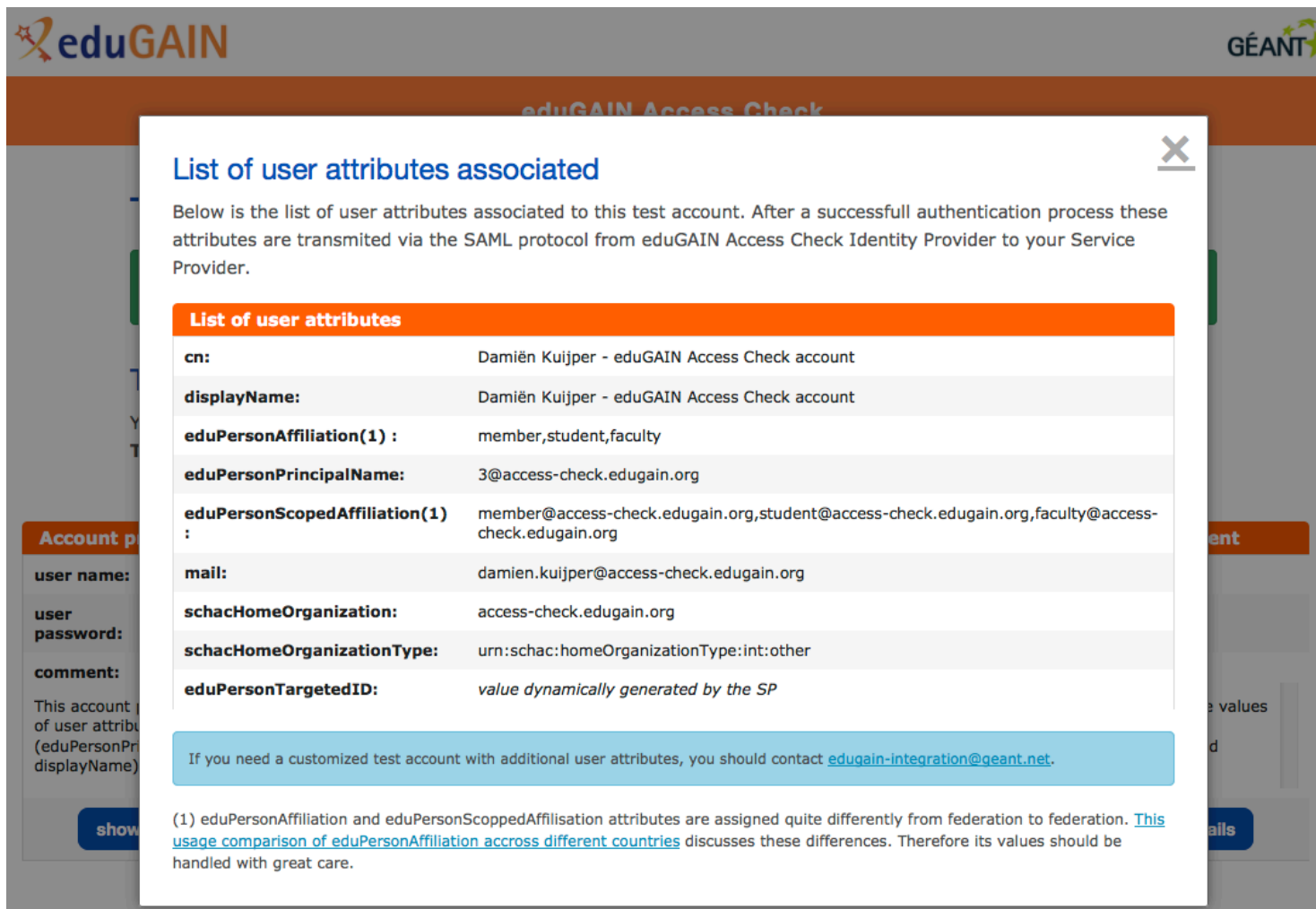
Please provide the validation token here:

3515c026f6752e8711b3

Previous   Next

Step 3: Inspect Test Account Profiles

© 2015 SWITCH

Step 4: Initiate Login to Your Service

Step 5: Login with Test Account

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)