User Consent for the Shibboleth Identity Provider

AAI Operations Committee

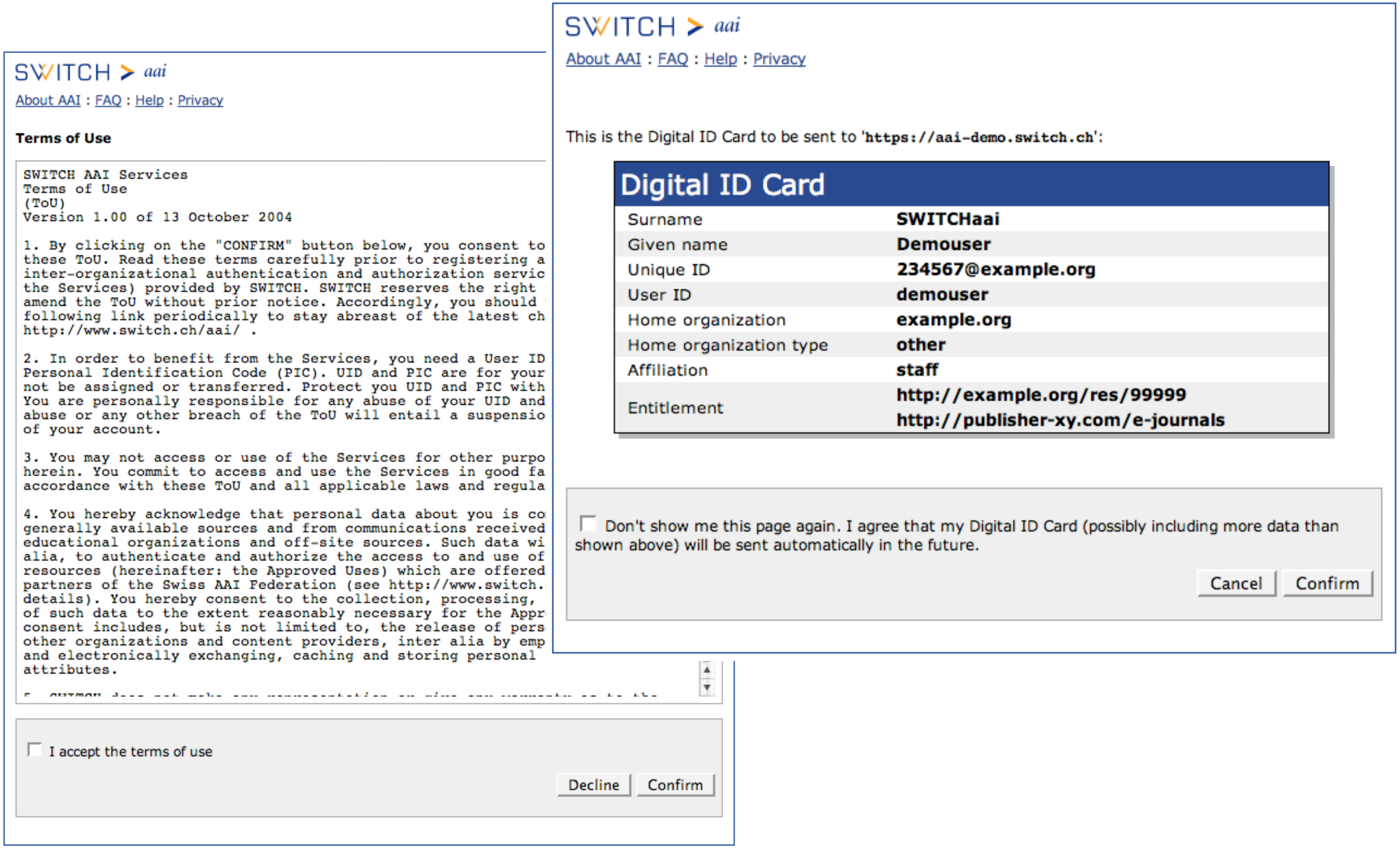
SWITCH

Serving Swiss Universities

Halm Reusser
halm.reusser@switch.ch

Berne, 15. June 2010

Terms of Use & Attribute Release Consent



Terms of Use

```
SWITCH AAI Services
Terms of Use
(ToU)
Version 1.00 of 13 October 2004

1. By clicking on the "CONFIRM" button below, you consent to
these ToU. Read these terms carefully prior to registering a
inter-organizational authentication and authorization servic
the Services) provided by SWITCH. SWITCH reserves the right
amend the ToU without prior notice. Accordingly, you should
following link periodically to stay abreast of the latest ch
http://www.switch.ch/aai/ .

2. In order to benefit from the Services, you need a User ID
Personal Identification Code (PIC). UID and PIC are for your
not be assigned or transferred. Protect you UID and PIC with
You are personally responsible for any abuse of your UID and
abuse or any other breach of the ToU will entail a suspensio
of your account.

3. You may not access or use of the Services for other purpo
herein. You commit to access and use the Services in good fa
accordance with these ToU and all applicable laws and regula

4. You hereby acknowledge that personal data about you is co
generally available sources and from communications received
educational organizations and off-site sources. Such data wi
alia, to authenticate and authorize the access to and use of
resources (hereinafter: the Approved Uses) which are offered
partners of the Swiss AAI Federation (see http://www.switch.
details). You hereby consent to the collection, processing,
of such data to the extent reasonably necessary for the Appr
consent includes, but is not limited to, the release of pers
other organizations and content providers, inter alia by emp
and electronically exchanging, caching and storing personal
attributes.

5. SWITCH does not make any representation or give any warranty as to the
```

□ I accept the terms of use

This is the Digital ID Card to be sent to 'https://aai-demo.switch.ch':

Digital ID Card

Surname	**SWITCHaai**
Given name	**Demouser**
Unique ID	**234567@example.org**
User ID	**demouser**
Home organization	**example.org**
Home organization type	**other**
Affiliation	**staff**
Entitlement	**http://example.org/res/99999** **http://publisher-xy.com/e-journals**

□ Don't show me this page again. I agree that my Digital ID Card (possibly including more data than shown above) will be sent automatically in the future.

Current state and roadmap

- uApprove for Shibboleth Identity Provider 2.x available

- In preparation as integrated module in Shibboleth IdP 3.0
  - Part of the IdP release plan and issue tracking

  - Current development/integration ongoing, 80% done
  - Roadmap

2010/Q3:	Testing and integration
later:	Release with Shibboleth IdP 3.0

Main benefits of the integration into the IdP

- Zero effort installation (out of the box)
  - IdP installer script deploys a working instance

- Simplified integration
  - Integrated within the IdP configuration
  - Integrated within IdP error handling and logging (audit log)

- Simpler to customize the template based views

Components

- Terms Of Use
  - Enable/Disable by configuration
  - Fingerprint of approved version/text and agree date is stored NEW
- Relying party black list
  - Disable terms of use and user consent for specific SPs (regex based)
- Attribute list
  - Configuration of the attribute listing order
  - Possibility to blacklist several attributes (e.g., targetedID, …)
    - Blacklisted attributes were not treated as agreed NEW

Attribute release consent (1)

- User consent consist of:
  - Attribute incl. hash of value(s) NEW
  - Date of last agreement (in case of value change) NEW
- Allow global consent for all Service Providers and all attributes
  - Enable/Disable by configuration

Attribute release consent (2)

- User has to re-approve, if:
  - Attribute set has changed
  - The hash of attribute value(s) has changed NEW
- Reset attribute release consent NEW
  - Clear all attribute release consents for the SP to access
  - If global consent set ➔ reset global consent

Persistence

- JDBC storage
  - Standard SQL
  - Out of the box setup for HSQLDB
    provides a file based option, no server needed
  - Allows usage of other SQL databases
- Infinispan storage NEW http://www.jboss.org/infinispan/
  - Extremely scalable, highly available distributed cache
  - IdP 3.0 choice of persistence
- Principal identification NEW
  - An arbitrary configured attribute is used as principal identification
    (e.g., persistentID, swissEduPersonUniqueID).
    This attribute must be released, but can be blacklisted.

Internationalisation

- Locale selection may be enforced by the deployer, else the user agent locale is taken with a default fallback.
- Views are multilingual thanks to message bundles.
- Attribute display name and descriptions are used as defined in the attribute resolver, if available.

NEW

- Relying party (SP) display names and descriptions are taken from the metadata, if available.