Attribute Availability & Release

Support of international attributes and uApprove

SWITCH

Serving Swiss Universities

Lukas Hämmerle
lukas.haemmerle@switch.ch

Berne, 1. March 2013

Overview

1. Supporting International Attributes
2. Data Protection and uApprove
3. Recommendations

1. Supporting International Attributes

- SWITCHaai was the first production federation in Europe
- Attributes used in SWITCHaai are sometimes specific for Switzerland due to swissEduPerson schema
- Internationally it is recommended to support alternative/other attributes than the swissEduPerson attributes

Recommended International Attributes

Attributes that should be additionally be supported:

- Scoped Affiliation ("staff@unibe.ch")
- Display Name ("Pierre Müller")
- Common Name ("Pierre Müller")
- SCHAC Home Organization ("unibe.ch")
- SCHAC Home Organization Type ("urn:schac:homeOrganizationType:ch:university")
- eduPersonPrincipalName ("sdc8932rhc@unibe.ch")

How to Support Int. Attributes

- User data is already available:
  - No modifications in user directory needed
  - Just the format and the name has to be configured
  - All values can be dynamically added by IdP

- Only a matter of IdP configuration
  - Attribute resolver configuration
  - Link: https://www.switch.ch/aai/docs/interfederation/international-attributes.html

Additional Benefits/Needs

- International Attributes are not only needed for Interfederation!
- Potential SWITCHaai Federation Partners require them too (e.g. scoped affiliation)
- Supporting International Attributes is important for future interoperability

SCHAC Attributes

- SCHAC = **SCH**ema for **AC**ademia
- Defines 21 Attributes for LDAP
- Some attributes similar to swissEduPersonSchema

- Link: http://www.terena.org/activities/tf-emc2/schac.html

SCHAC Example Definition

5.2.1 schacHomeOrganization

Name	**schacHomeOrganization**
Description	Specifies a person´s home organization using the domain name of the organization
Format	Domain name according to RFC 1035
# of values	Single
References	• **RFC 1035** – Domain names – implementation and specification
RFC 4517 definition	(schacAttributeType:9 NAME 'schacHomeOrganization' DESC 'Domain name of the home organization' EQUALITY caseIgnoreMatch SUBSTR caseIgnoreSubstringsMatch SINGLE-VALUE SYNTAX 1.3.6.1.4.1.1466.115.121.1.15)
Examples	• schacHomeOrganization = tut.fi

Data Protection and Privacy

Do you know of any data protection problems/law suits in your organisation regarding the release of user information?

Why Care About Data Protection?

- Most users don't care, so why should we?

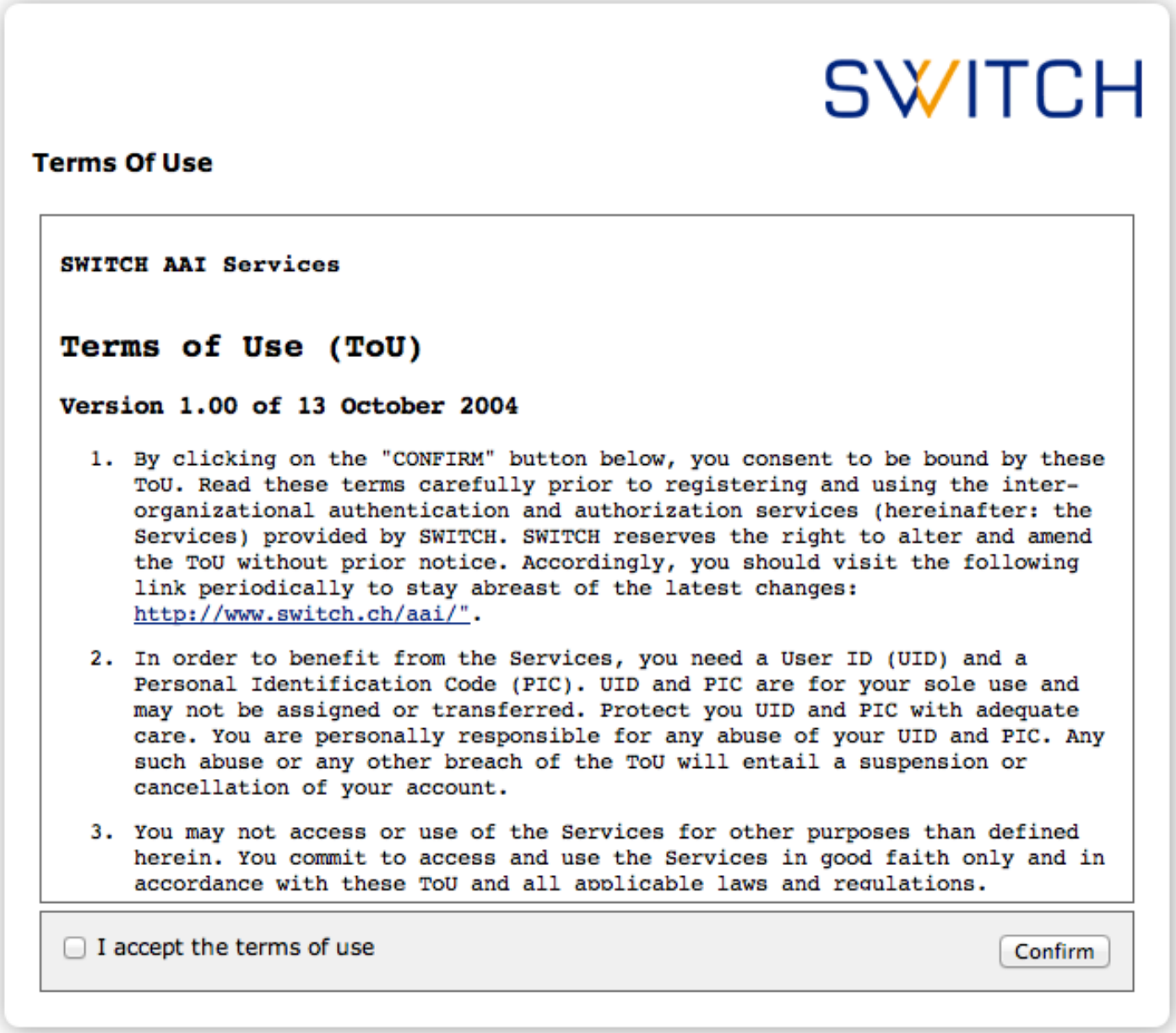
- **Why to care:**
  - With interfederation students and staff members access services operated in other jurisdictions
  - Organisation could be held liable
  - Reason why Facebook's reputation suffered

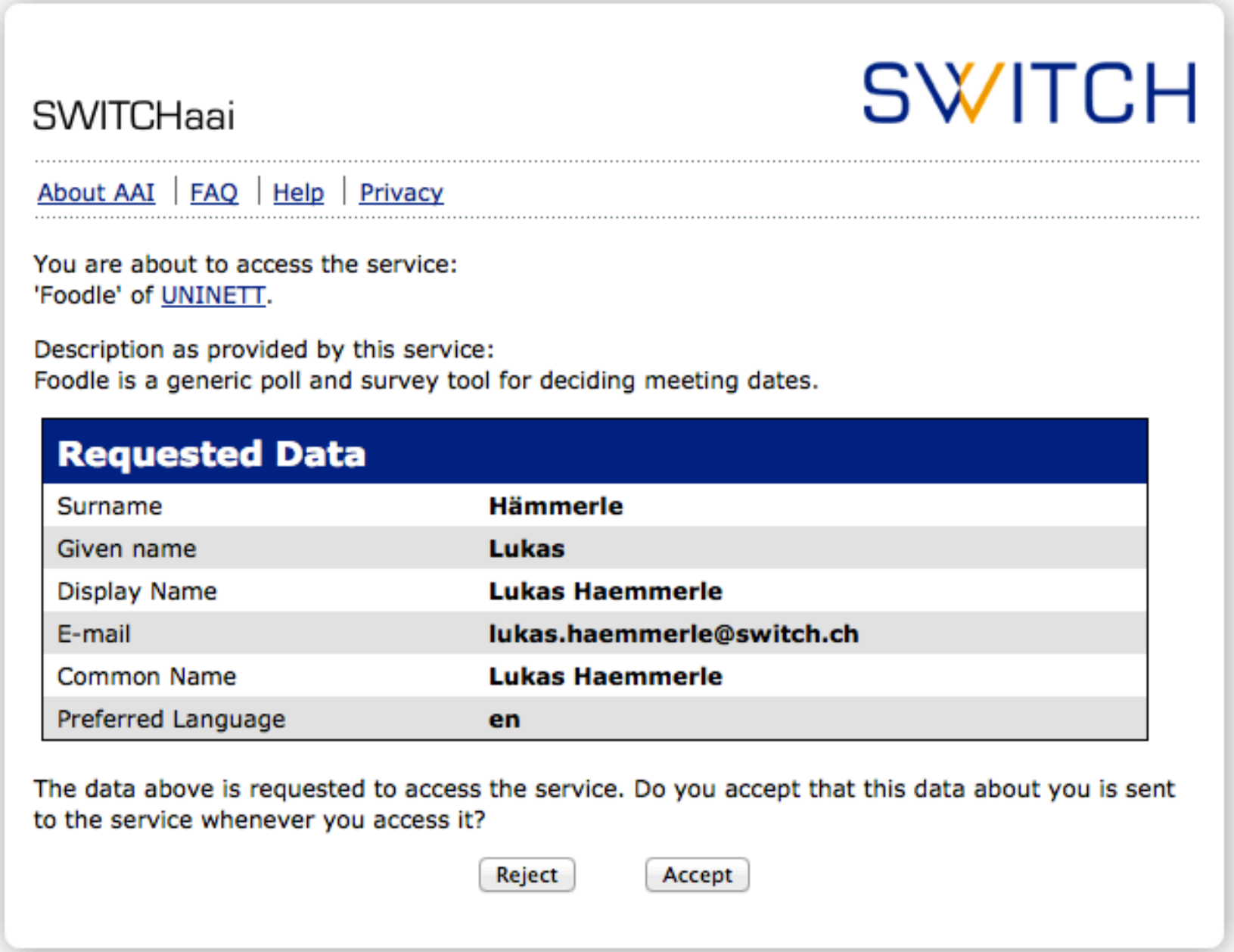
2. Data Protection and uApprove

- Attributes are personal data of enduser
- Home Organisation is responsible and liable for personal data/attributes
  - Release may infringe users privacy when he accesses services outside organisation
- User should agree/consent to attribute release
  - Formally with Terms of Use and/or technically
- Discussions with Swiss Data Protection Officer:
  -> User Consent is strongly recommended

Getting User's Consent with uApprove

- uApprove = Plug-In for the Shibboleth IdP
- Asks user to:
  - accept IdP terms of use once (optional)
  - allow attribute release on first access of service or if attributes changed
- Developed by SWITCH as Open Source
- Used internationally
- Link: http://www.switch.ch/aai/uapprove


SWITCH
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 be bound by these ToU. Read these terms carefully prior to registering and using the inter-organizational authentication and authorization services (hereinafter: the Services) provided by SWITCH. SWITCH reserves the right to alter and amend the ToU without prior notice. Accordingly, you should visit the following link periodically to stay abreast of the latest changes: http://www.switch.ch/aai/".
2. In order to benefit from the Services, you need a User ID (UID) and a Personal Identification Code (PIC). UID and PIC are for your sole use and may not be assigned or transferred. Protect you UID and PIC with adequate care. You are personally responsible for any abuse of your UID and PIC. Any such abuse or any other breach of the ToU will entail a suspension or cancellation of your account.
3. You may not access or use of the Services for other purposes than defined herein. You commit to access and use the Services in good faith only and in accordance with these ToU and all applicable laws and regulations.
I accept the terms of use
Confirm


SWITCHaai
SWITCH
About AAI | FAQ | Help | Privacy
You are about to access the service:
'Foodle' of UNINETT.
Description as provided by this service:
Foodle is a generic poll and survey tool for deciding meeting dates.
Requested Data
Surname Hämmerle
Given name Lukas
Display Name Lukas Haemmerle
E-mail lukas.haemmerle@switch.ch
Common Name Lukas Haemmerle
Preferred Language en
The data above is requested to access the service. Do you accept that this data about you is sent to the service whenever you access it?
Reject
Accept

uApprove Deployment

- Requires a MySQL database
  - Already deployed by all SWITCHaai IdPs
- Easy to deploy
- Templates can and should be adapted

- Example terms and configurations: http://www.switch.ch/aai/legaltemplates (SWITCH legal approved)

Recommendations

- Support International Attributes even without interfederation participation
  - It's easy to support them
  - Publishers may require some of them in the future

- SWITCH strongly recommends deploying uApprove for interfederation support
  - Transparent for users regarding data release
  - Organisation should be on the safe side
  - Not very invasive if blacklisting is used