

# uApprove



**SWITCH**  
Serving Swiss Universities

## Agenda

- ① Introduction
- ② End user views
- ③ Concept and Design
- ④ Further information, Q&A

## What is it and what does it do?

- A plug-in for the Shibboleth Identity Provider

- For the end user
  - shows the attributes, which are released
  - retrieve user consent

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

- For the IdP deployer
  - force the end users to agree to the terms of use
  - collect information about attribute releases and resource accesses

## Benefits

- Helps in implementing data privacy protection and provides auditability.
- Users control attribute release → improves user acceptance
- Provides Kim Cameron's 1st Law of Identity [1]:
  - User Control and Consent:  
*"Technical identity systems must only reveal information identifying a user with the user consent."*
- It was a requirement for some Swiss universities for the SWITCHaai rollout.

[1] <http://www.identityblog.com/stories/2005/05/13/TheLawsOfIdentity.pdf>

# Agenda

- ① Introduction
- ② End user views
- ③ Concept and Design
- ④ Further information, Q&A

## Terms of use

A user accesses a resource for the first time

- Terms of use are shown (optionally)
- The user has to accept the ToU
- As long as the ToU do not change, the user never will see those again

SWITCH > aai  
[About AAI](#) : [FAQ](#) : [Help](#) : [Privacy](#)

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

I accept the terms of use

Decline Confirm

## Attribute release

After the user accepted the ToU or they were previously accepted, the attributes - which will be released to the resource - are shown

- The user can accept/decline the attribute release.
- If a consent was given, the user will not be asked again as long as the set of attributes for this resource do not change.
- The user may give a global approval for all subsequent attribute releases.

SWITCH > aai  
[About AAI](#) : [FAQ](#) : [Help](#) : [Privacy](#)

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.

Cancel Confirm

## Reset approvals

- The user has the possibility to reset already given attribute release consent or to disable the *global release approval* flag.

SWITCH > aai  
[About AAI](#) : [FAQ](#) : [Help](#) : [Privacy](#)

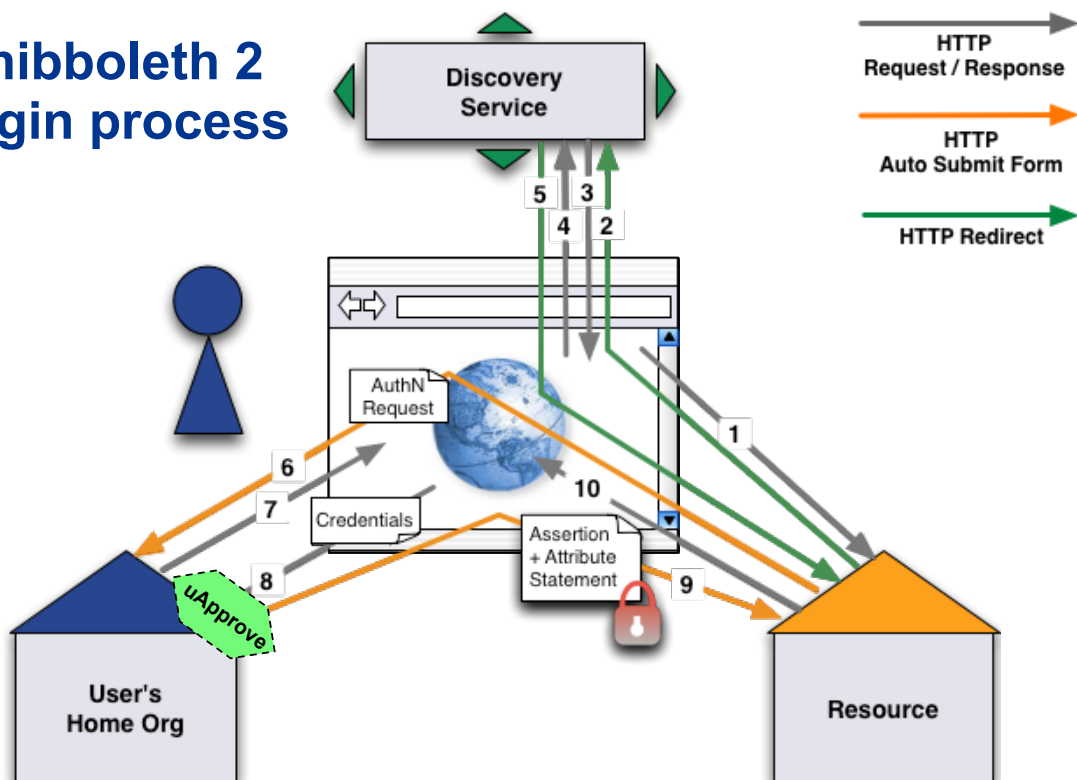
Reset my login preferences: This will show my Digital ID Card each time I access a web resource for the first time.

Cancel Confirm

# Agenda

- ① Introduction
- ② End user views
- ③ Concept and Design
- ④ Further information, Q&A

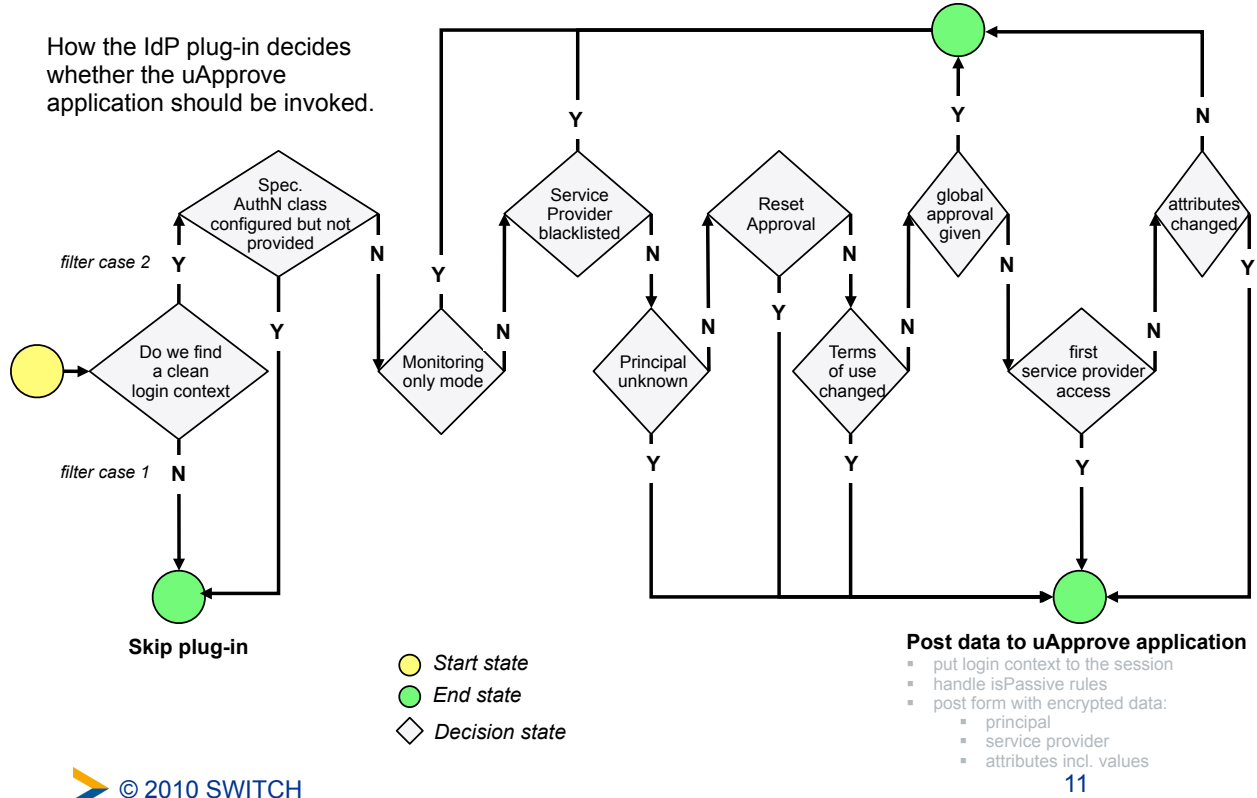
## Shibboleth 2 login process



<http://www.switch.ch/aai/demo/>

# Decision flow

How the IdP plug-in decides whether the uApprove application should be invoked.



# Features

- **General**
  - Independent of authentication mechanism
- **Deployment configuration**
  - Optional terms of use
  - Optional global release approval flag
  - Service Provider blacklisting
- **Attribute release information**
  - Names and description in local language
  - Hide specific attributes
- **Audit log**
  - Provider access log provides usable usage statistics.
  - Monitoring mode only

# Agenda

- ① Introduction
- ② End user views
- ③ Concept and Design
- ④ Further information, Q&A

# Users & interested parties of uApprove I

## In Switzerland

- SWITCH incl. Virtual Home Organization
- University of Lausanne
- University of Fribourg
- University of St. Gallen
- Berner Fachhochschule

# Users & interested parties of uApprove II

## Abroad

- Germany
  - Stiftung Alfred-Wegener-Institut für Polar- und Meeresforschung, Bremerhaven
  - University of Freiburg
  - Bavarian State Library
  - Leibniz-Rechenzentrum der Bayerischen Akademie der Wissenschaften, Munich
  - University of Tuebingen
  - GWDG
- Other Europeans
  - University of Cambridge, UK
  - Technical University Prague, Czech Republic
  - Helsinki University, CSC IT Center of Science , Aalto University School of Science and Technology, Finland
  - Fundação para a Computação Científica Nacional, Reitoria da Universidade do Porto, Portugal
  - and many more
- USA
  - Brown University, Rhode Island
  - The Ohio State University
  - University of California
  - Virginia Tech
  - University of North Carolina
  - and many more
- Other World
  - Hyro, New Zealand
  - University of South Australia

## Summary

- Valuable Shibboleth Identity Provider plug-in
- Retrieves user consent about attribute release
- Straight forward to use



## Try it out

- Online demonstration
  - <https://aai-demo.switch.ch/secure-uApprove/>
  - Username(s): demo[1..50]
  - Password: demo
  
- Website & Download
  - <http://www.switch.ch/aai/uApprove>