

uApprove formerly known as ArpViewer

TF-EMC2, 4. December 2008, Utrecht



SWITCH

Serving Swiss Universities

Thomas Lenggenhager
lenggenhager@switch.ch

Overview

- ① Introduction
- ② End user views
- ③ Concept and Design
- ④ Further information

Credits to Halm Reusser <halm.reusser@switch.ch>

What is it and what does it do?

- A plug-in for the Shibboleth Identity Provider
- For the end user
 - shows attributes, to be released
 - requires user consent
- For the IdP deployer
 - force end users to agree to terms of use
 - collect usage information on attribute release and resource access

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

Benefits

- Helps to implement data privacy protection, provides auditability.
- User controls 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 participating in SWITCHaai.

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

Overview

- ① Introduction
- ② End user views
- ③ Concept and Design
- ④ Further information

Terms of Use

A user accesses a resource for the first time

- Show Terms of Use (optional)
- User has to accept the Terms of Use
- Versioning support, as long as Terms of Use do not change, the user will not see them 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 Terms of Use, show the attributes to be released to the resource
- The user can accept or decline attribute release.
- If consent was given, the user will never be asked again as long as the set of attributes for this resource does not change.
- The user may give a global consent 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

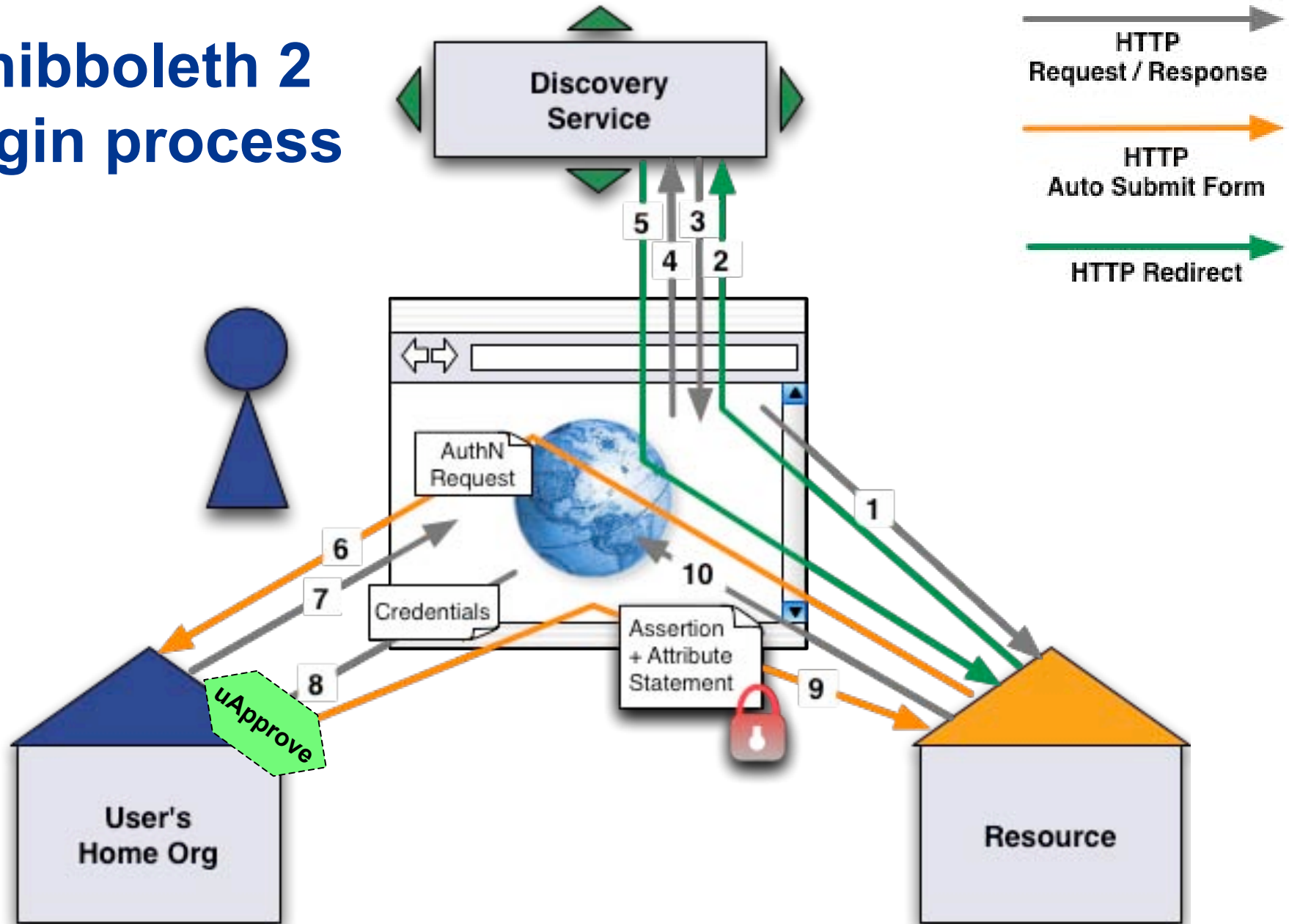
[About AAI](#) : [FAQ](#) : [Help](#) : [Privacy](#)

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

Overview

- ① Introduction
- ② End user views
- ③ Concept and Design
- ④ Further information

Shibboleth 2 login process



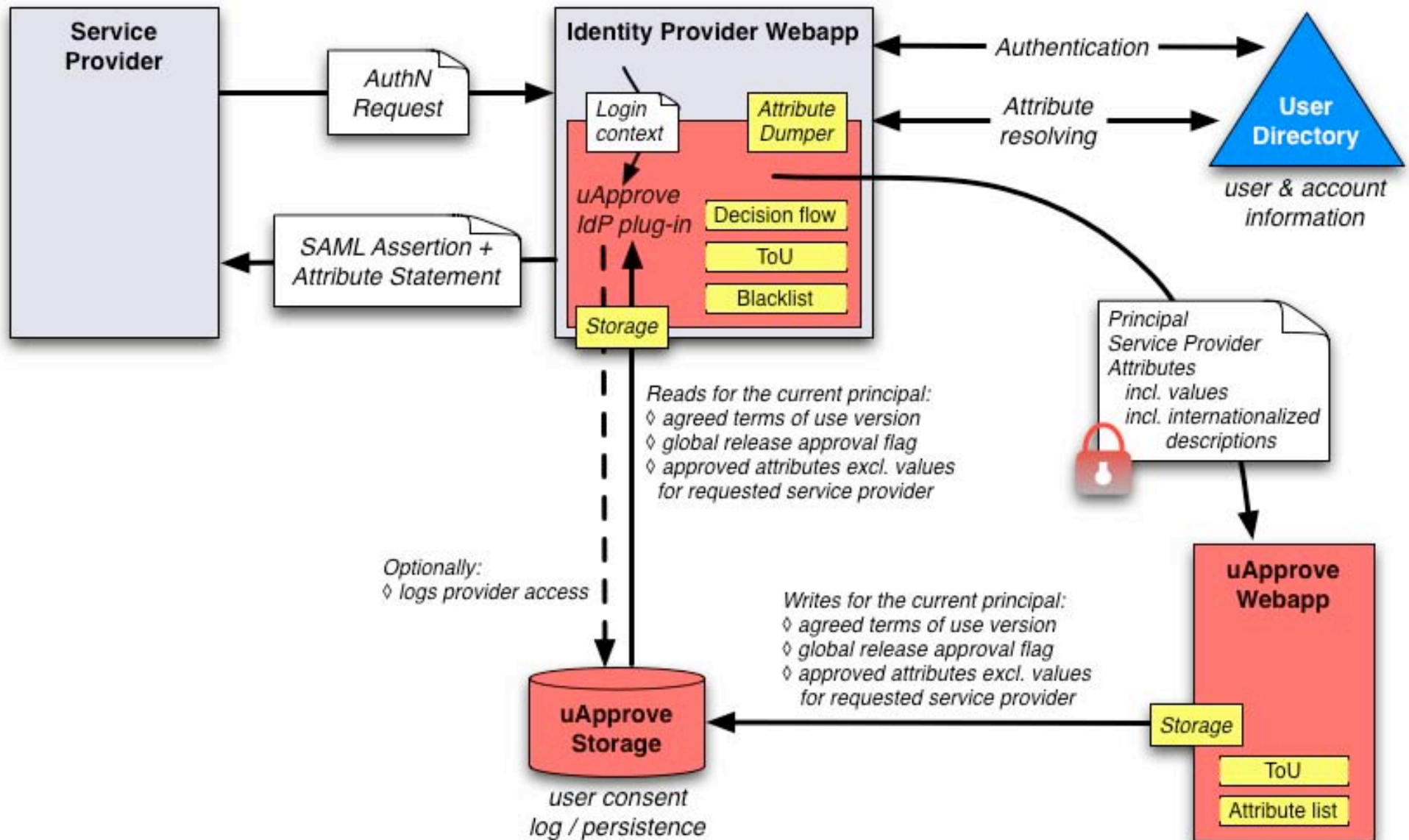
<http://www.switch.ch/aai/demo/>

How it works - 3 Components

uApprove is a Java application,
with three components:

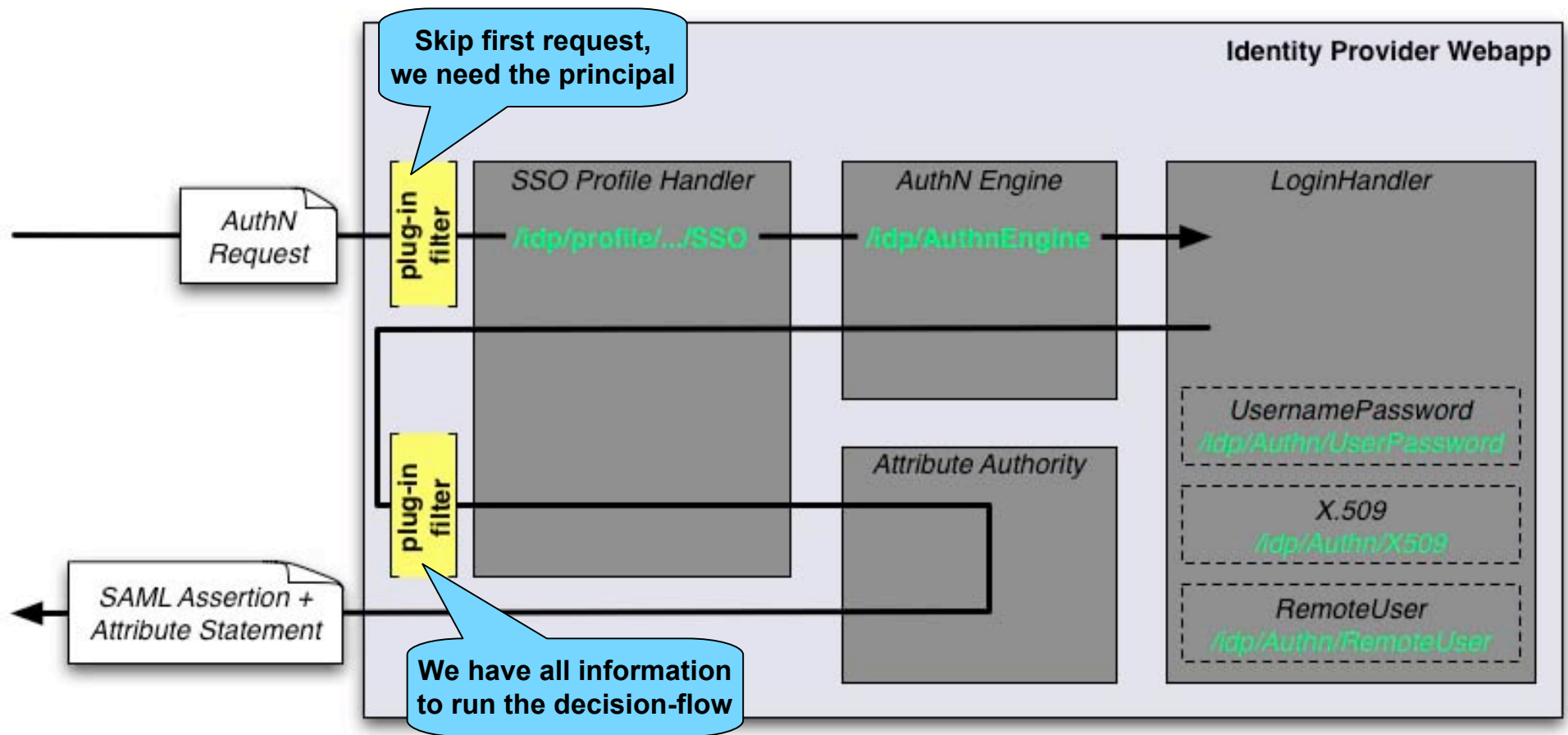
1. An **IdP plug-in**, to determine whether to invoke uApprove
2. An **application**, which presents the views (Terms of Use, attribute set, reset form) and interacts with the user.
3. Persistent **information store**, either a SQL database or a XML flat file

Embedded within the Shibboleth components



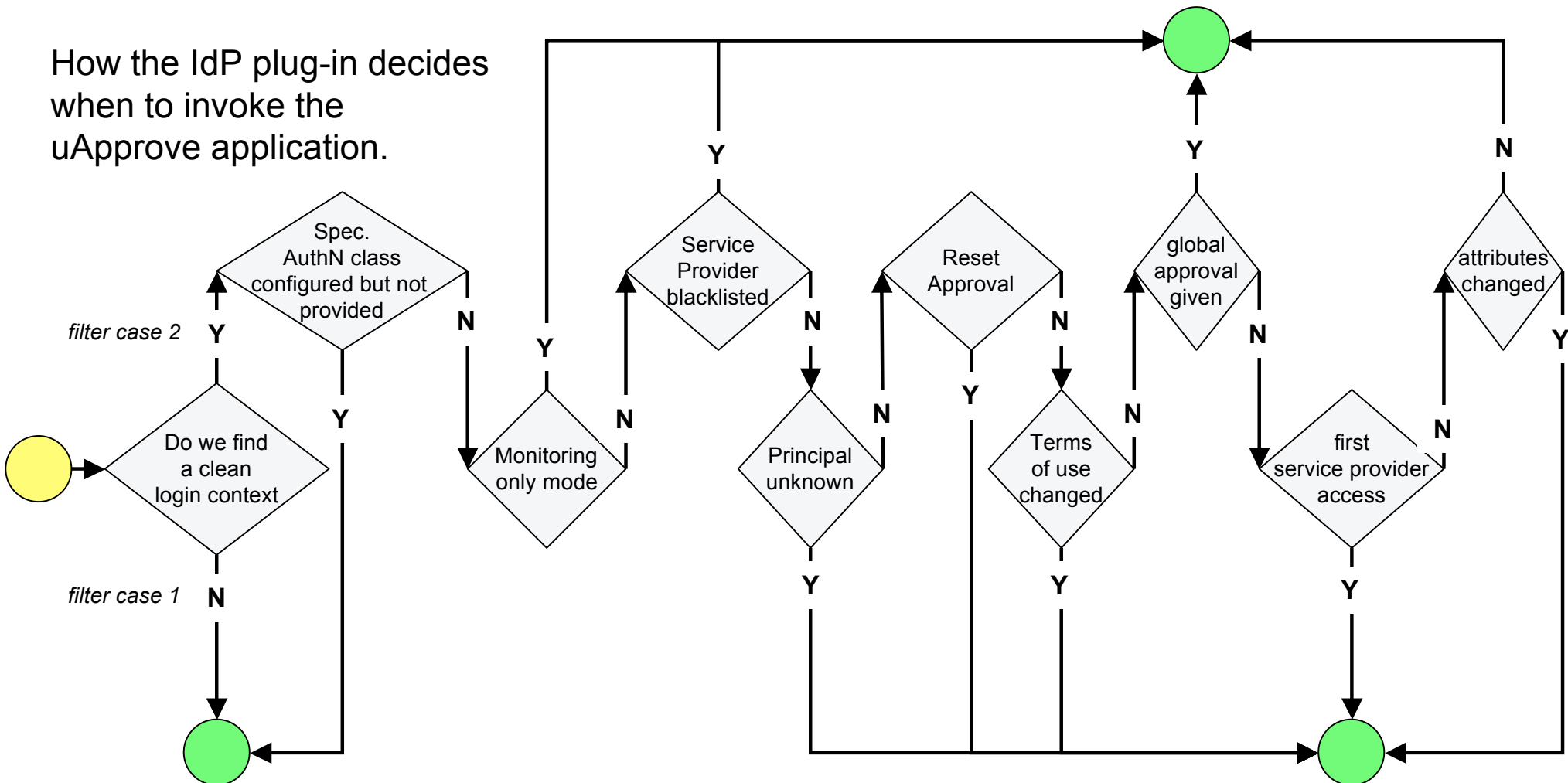
IdP integration

- The uApprove IdP plug-in implements the javax.servlet.Filter interface
- It is triggered on http requests and forwards to /idp/profile/*



Decision flow

How the IdP plug-in decides when to invoke the uApprove application.



Skip plug-in

- Start state
- End state
- ◇ Decision state

Continue IdP flow

- fetch the principal if not yet known
- log provider access if configured
- return control to IdP

Post data to uApprove application

- put login context to the session
- handle isPassive rules
- post form with encrypted data:
 - principal
 - service provider
 - attributes incl. values

Information persistence and maintenance

- Users
 - Principal
 - Last accepted version of the ToU
 - First access, last access

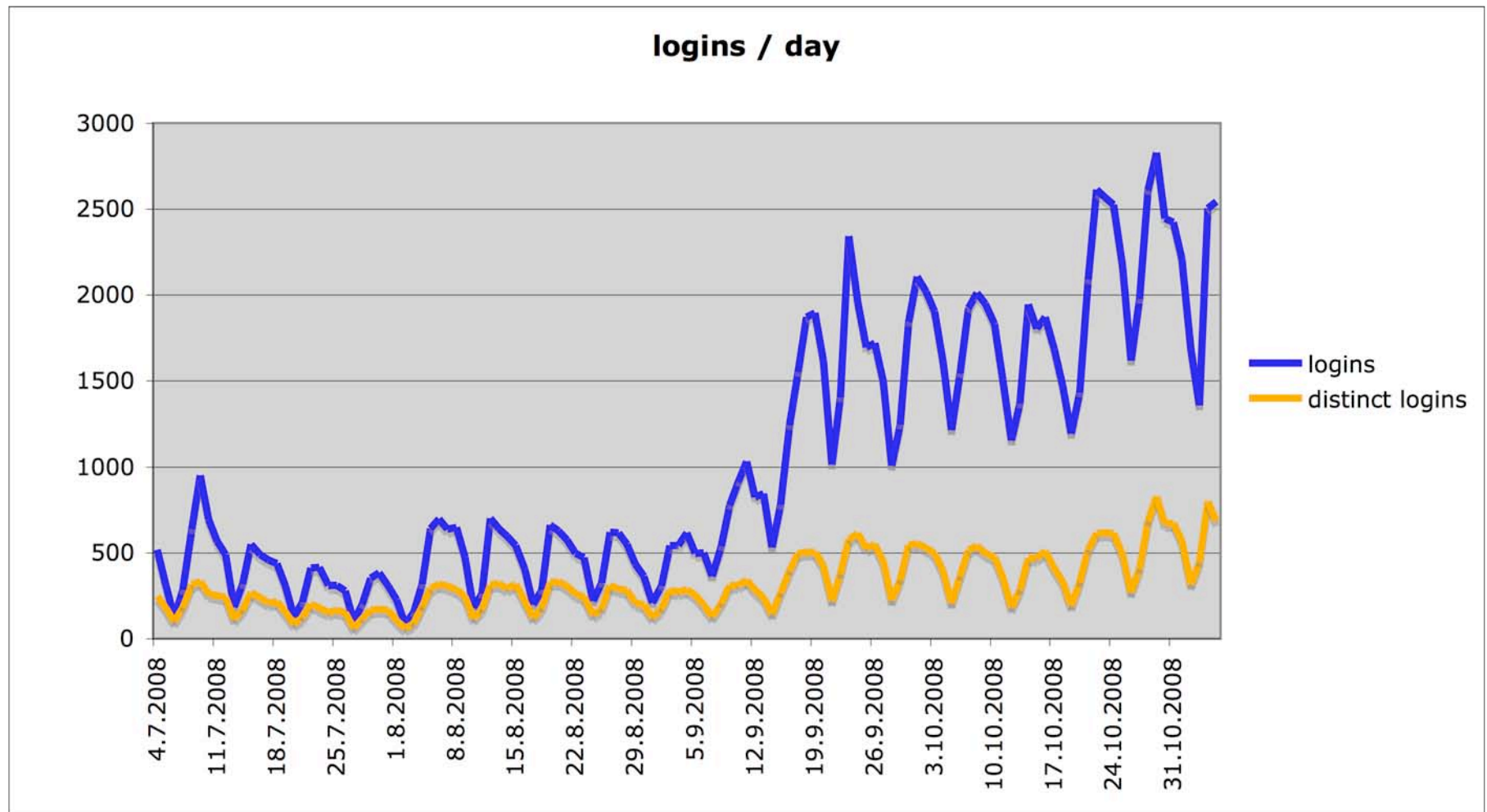
 - Attribute release approvals
 - User
 - Service Provider or global approval
 - Date and time
 - ToU version
 - Attributes **excl. values**
- User may delete his entry (*reset approvals*)
- Provider Access (optionally)
 - Same information as *attribute release approvals*, but users cannot remove it

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

Example usage statistics with provider access log

SWITCH Virtual Home Organization, last months



Overview

- ① Introduction
- ② End user views
- ③ Concept and Design
- ④ Further information

Users & interested parties of uApprove

In Switzerland

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

International

- 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
- Other European Countries
 - University of Cambridge, UK
 - Technical University Prague, Czech Republic
- USA
 - Brown University, Rhode Island
 - The Ohio State University

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>

Advertisement: Shibboleth 2 Install Fest

- Three successful Shibboleth Install Fests
 - June and July in Zürich
 - August in Lausanne
- A further IdP & SP Install Fest
 - Wed 21. - Fri 23. January 2008 in Zürich
 - Registration at
<http://www.switch.ch/aai/events/installfest-2009/>