

The Swiss Universities and FIM

The Past, the Present and the Future



SWITCH

Serving Swiss Universities



Lukas Hämmerle

lukas.haemmerle@switch.ch



FIM Infrastructures in Switzerland

Two major FIM infrastructures:

- **AAI** SWITCHaai + 
Get access to web services using your organisation identity
- **eduroam** 
Get network access using your organisation identity

The Past



A Long Time Ago...

The story of AAI as federated identity management infrastructure in Switzerland starts in last century.

In 1999 there was a paper published...

Application for a VCS Mandate

"Evaluation of an Authentication and Authorisation Infrastructure"

Alexander Gall, Christoph Graf and Thomas Lenggenhager
SWITCH, Limmatquai 138, 8001 Zürich

November 29, 1999

Abstract

Well co-ordinated access control is a crucial issue for the VCS project, requiring an Authentication/Authorisation Infrastructure (AAI). SWITCH proposes a one-year mandate to study and design an AAI that suits the needs of the VCS as well as further projects within universities and for collaborations with foreign institutions. The activities within the scope of this mandate will be funded by SWITCH. An AAI deployment will be proposed in follow-up mandates jointly with the universities.

First mention of the term "AAI"

The Use Case for AAI

- Swiss Virtual Campus (2000-2003 & 2004-2007)
- Subsidies for university projects with Principal Goal:
«develop teaching modules that will be used through the Internet in several regular study programs of the Swiss universities»
 - Users from multiple universities needed to be able to access any of the e-learning platforms
 - Authentication across security domains
 - All universities were involved

Early Roots of AAI

e-Academia / AAI Concept

SWITCH

The Swiss Education & Research Network

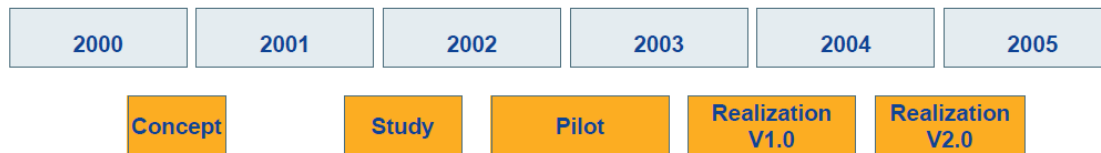
Vision of e-Academia

"We want a virtual community across our institutions in which all persons associated with the Swiss Higher Education System are able to gain access to its electronic resources, independent of the accrediting organization and independent of the place where they happen to be working."

AAI as the foundation of e-Academia

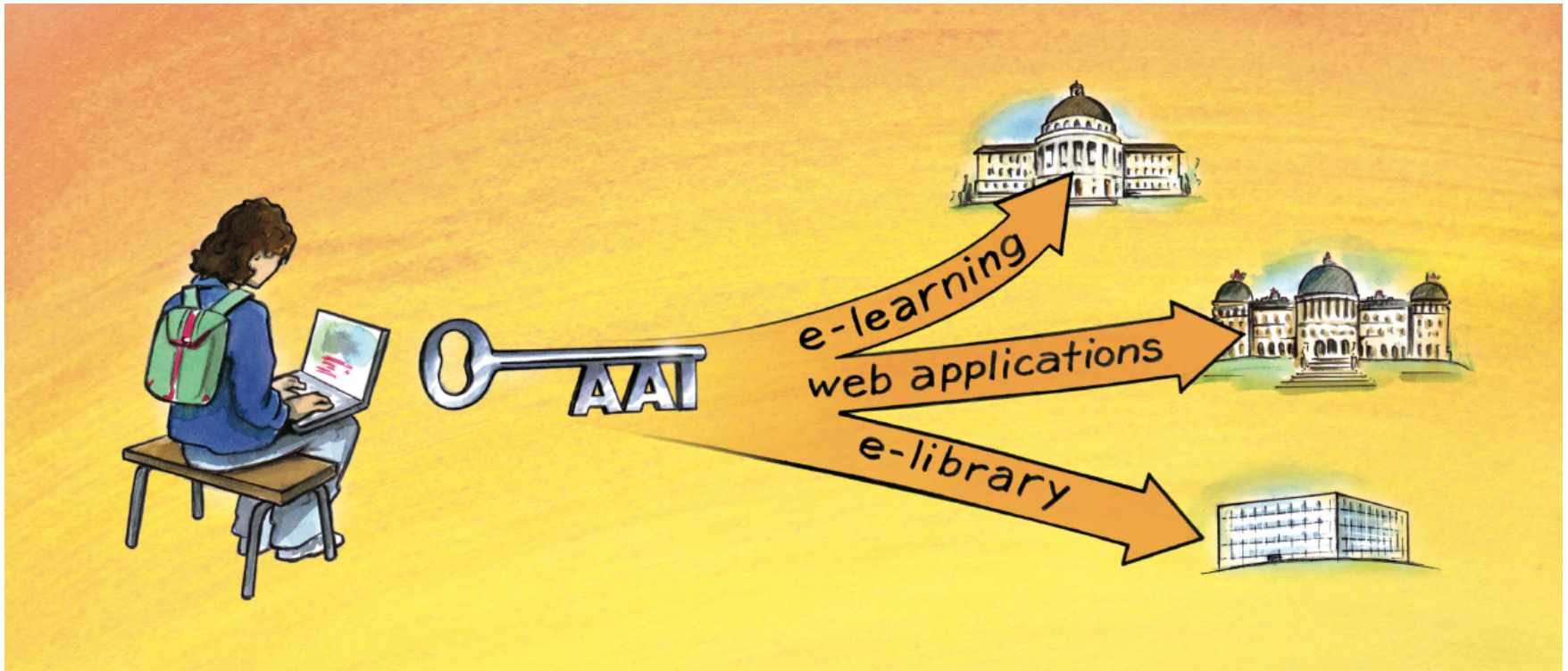
"... let's develop e-Academia, let us build the foundations in the form of a uniform authentication and authorization infrastructure (AAI) for the higher education system in Switzerland..."

Roadmap

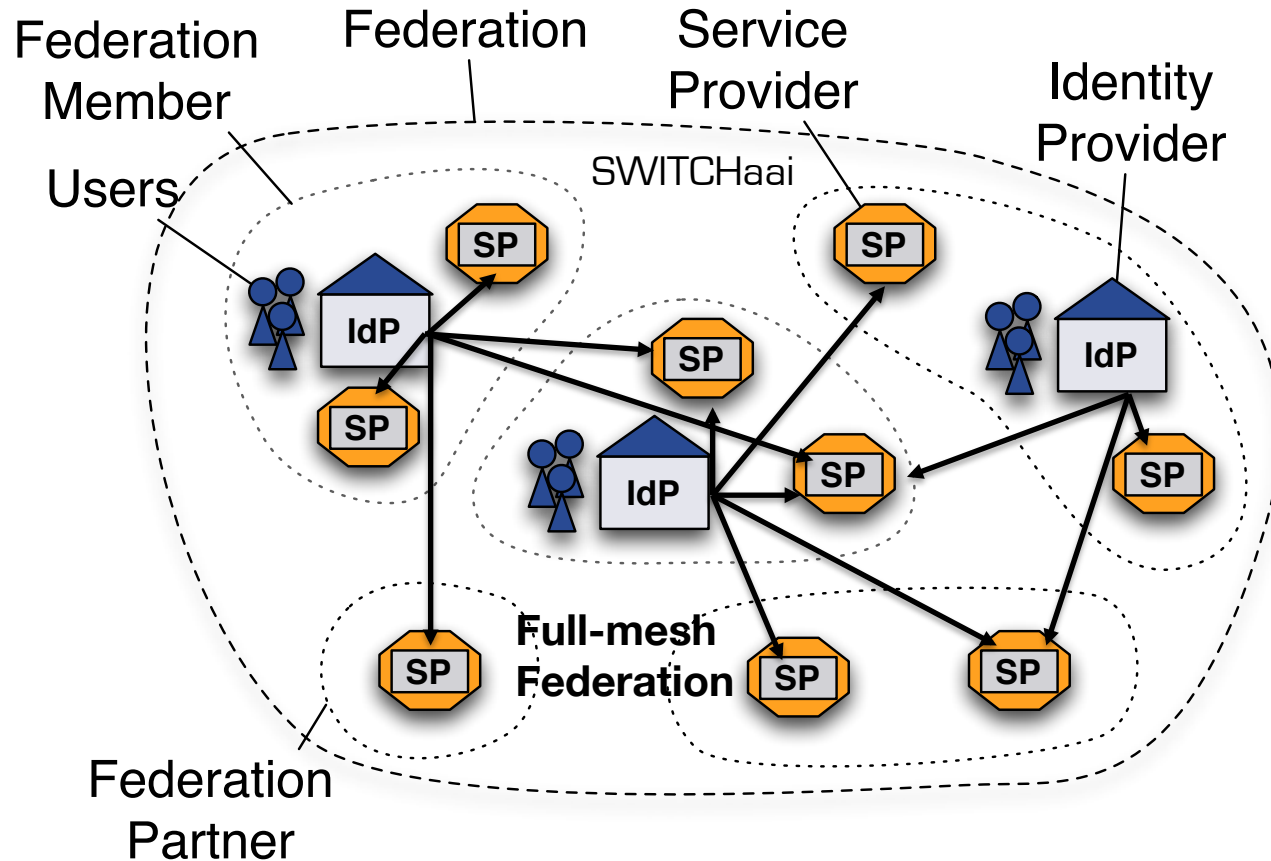


Proposed Solution: AAI

Authentication and Authorization Infrastructure
SAML-based identity federation in Switzerland



AAI as a Federation

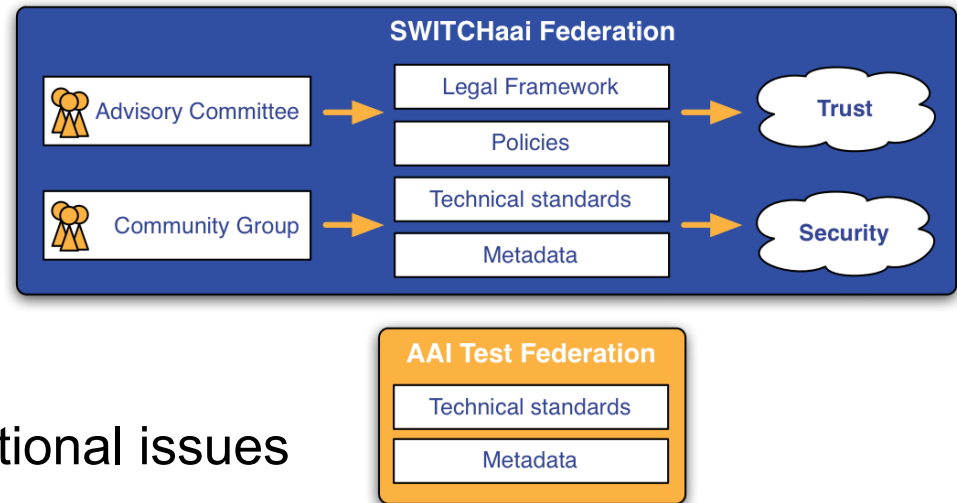


Federation: Common trust, standards and policies

SWITCHaai Federation

SWITCH consults with two bodies:

- **Advisory Committee** deals with policies and legal framework
- **Community Group** deals with technical/operational issues



Two categories of SWITCHaai Participants:

- **SWITCH Community**
Organization fits the definition from the SWITCH Service Regulations. E.g. Universities, research institutions
- **Federation Partner**
Organization sponsored by a SWITCHaai Participant from the SWITCH Community. E.g. Microsoft, Elsevier

SWITCHaai: Services Provided

- Rules, policies and agreements
- Documentation: installation/migration guides, How-Tos
- Call-in helpdesk and support mailing list
- Centralized Services
 - Discovery Service, Attribute Viewer
 - Resource Registry (metadata management)
 - Virtual Home Organization (VHO), Guest Login (for homeless)
 - Group Management Tool, Toolbox (solution for VOs)
- Shibboleth IdP plugins: uApprove, x.509 login, kerberos login
- Test federation
- Some application integration support
- Training (hands-on workshops)
- **Identity Provider Hosting**

Early roots of eduroam

Projektplan

SWITCH
The Swiss Education & Research Network

Deployment eduroam	2006			2007			
Nat. RADIUS Hierarchie/Service	Q2	Q3	Q4	Q1	Q2	Q3	Q4
Aufbau RADIUS-Infrastruktur							
Tests - Lokal (institution level), Global (TDL)							
Transition in produktive Umgebung TLD.ch und switch.ch RadSec							
Vorbereitung: eduroam als Service							
Dokumentation eduroam Technische Doku / Service Doku							



Eduroam als Service eingeführt!

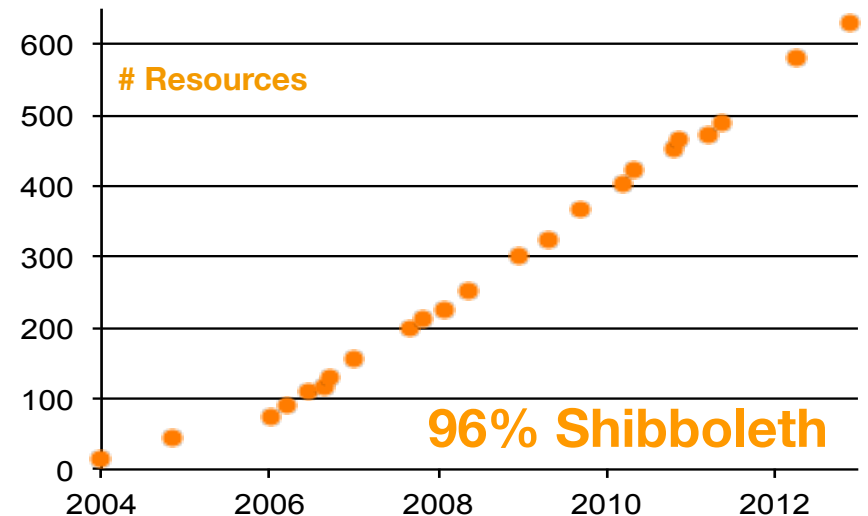
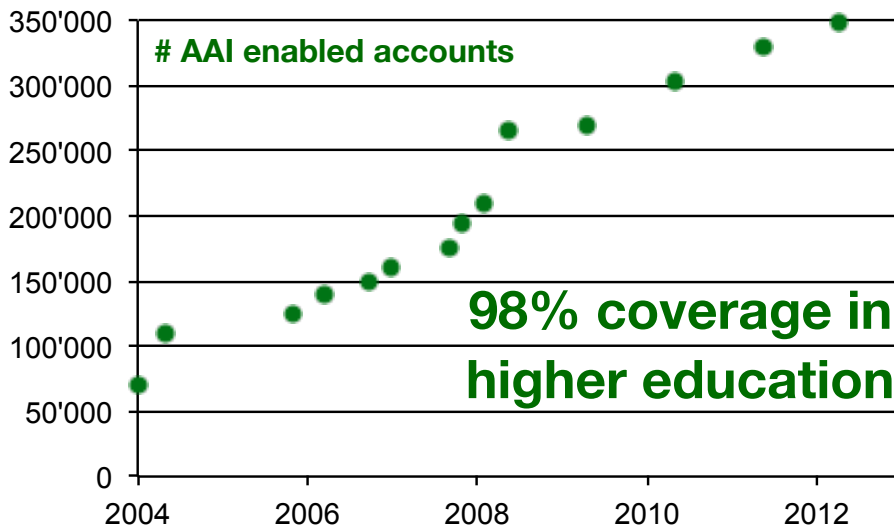
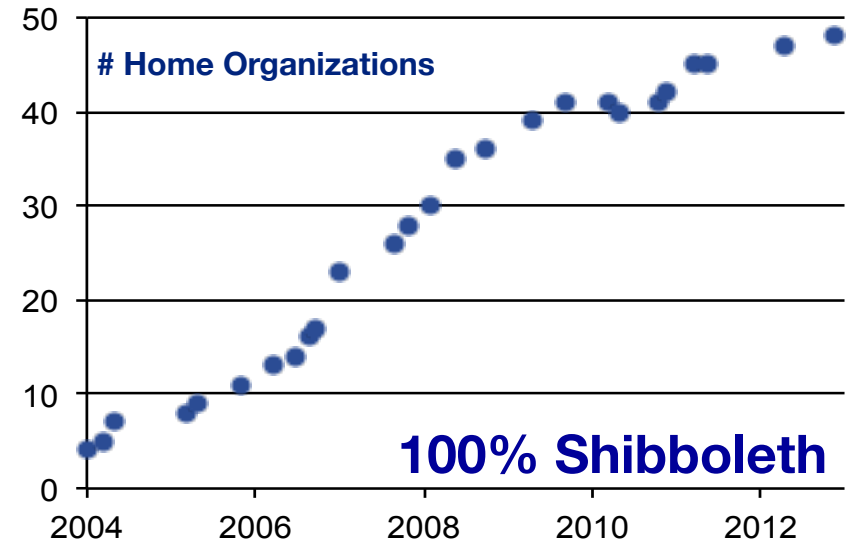
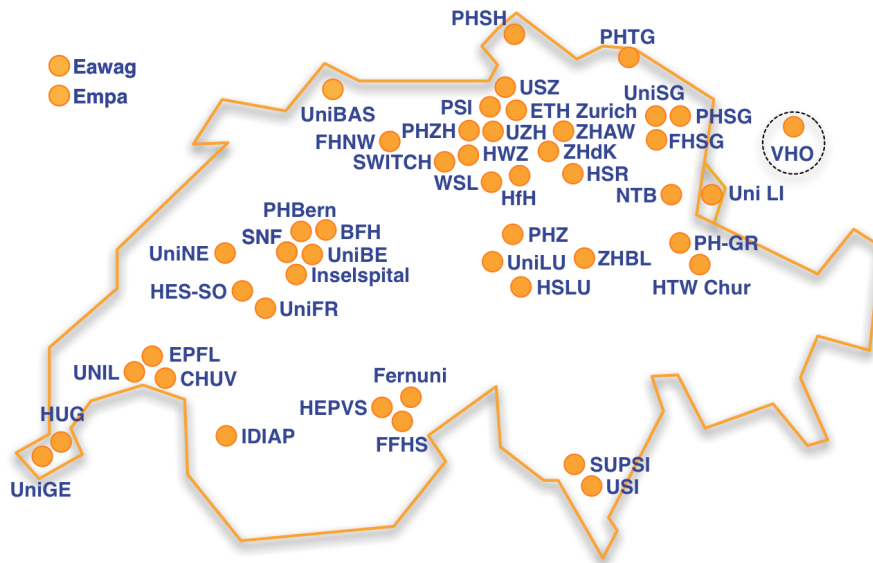
eduroam

- Was internationally driven from the start
 - Developed by GEANT
- eduroam is about authentication only
 - No user attributes available
- Hierarchical Radius architecture

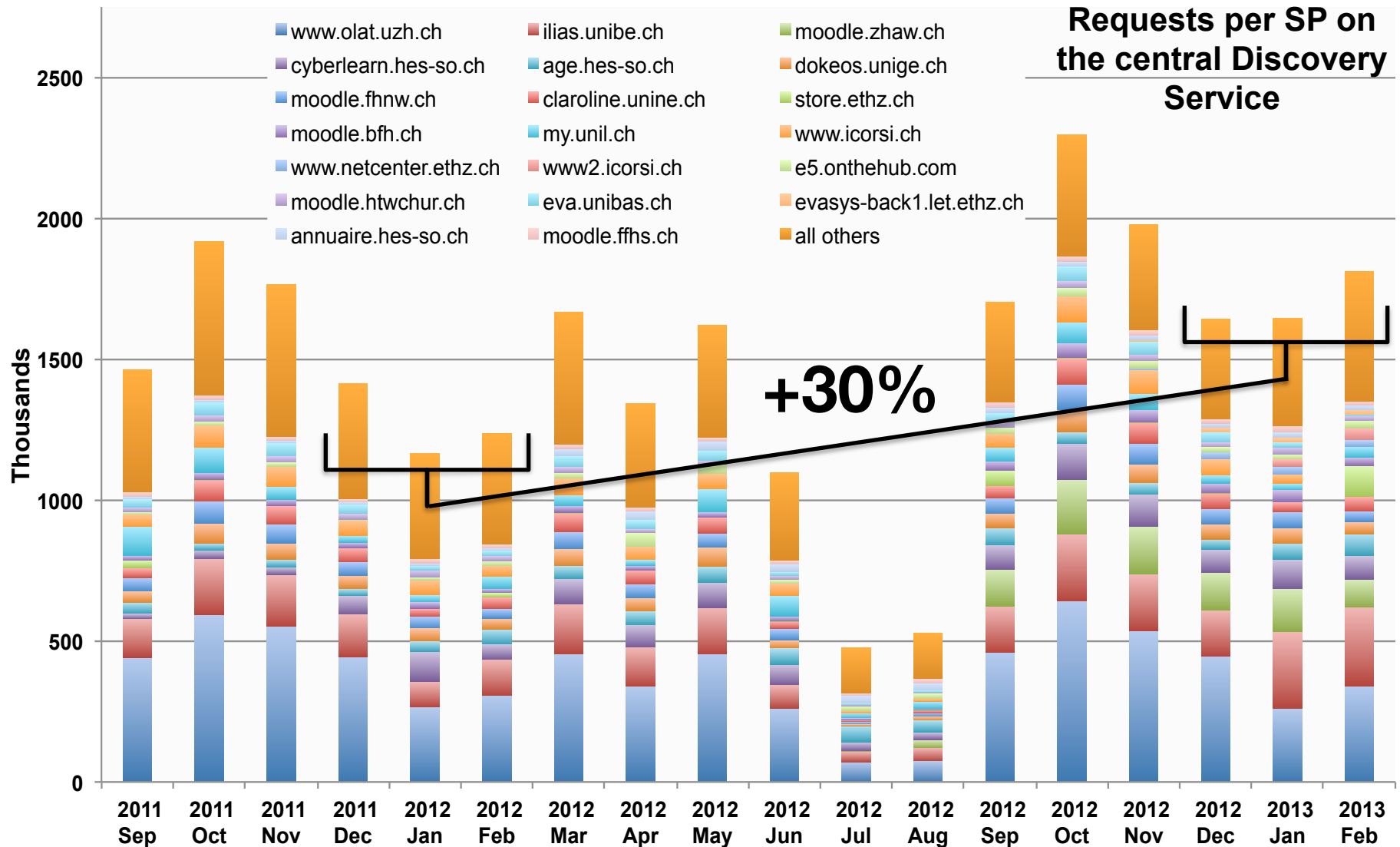
The Present



AAI today



(Minimum) AAI Authentication Requests



SWITCHaai Attribute Release

- Completely automated attribute release:
 - Attribute release is managed via Resource Registry web interface by IdP administrators
 - Default rules are applied to new SPs
 - IdPs download attribute release rules hourly
 - Administrators get automatically informed of changes and can create specific rules
- Attribute release issues are very rare!

SWITCHaai Success Factors

- Virtual Campus Switzerland funding
 - Subsidies required cooperation
- Acceptance due to Involvement
 - Close collaboration with universities during development of AAI
- Critical Mass
 - Participation of large universities accelerated adoption rate
 - AAI became a self-runner

Status of eduroam

From 46 Swiss Higher Education Organisations:

- 32 (69%) support eduroam
- 5 planned or in progress
- 9 no plans not planned

Hochschule für Technik Rapperswil (HSR)	Running
Hochschule Luzern (HSLU)	Running
HTW Chur	Running
IDIAP Research Institute	Running
Kanton Zug (Sekundarstufe II)	Running
Pädagogische Hochschule Bern	Running
Pädagogische Hochschule Graubünden	Running
Pädagogische Hochschule Luzern	Planned

Development of eduroam in Switzerland compared to AAI

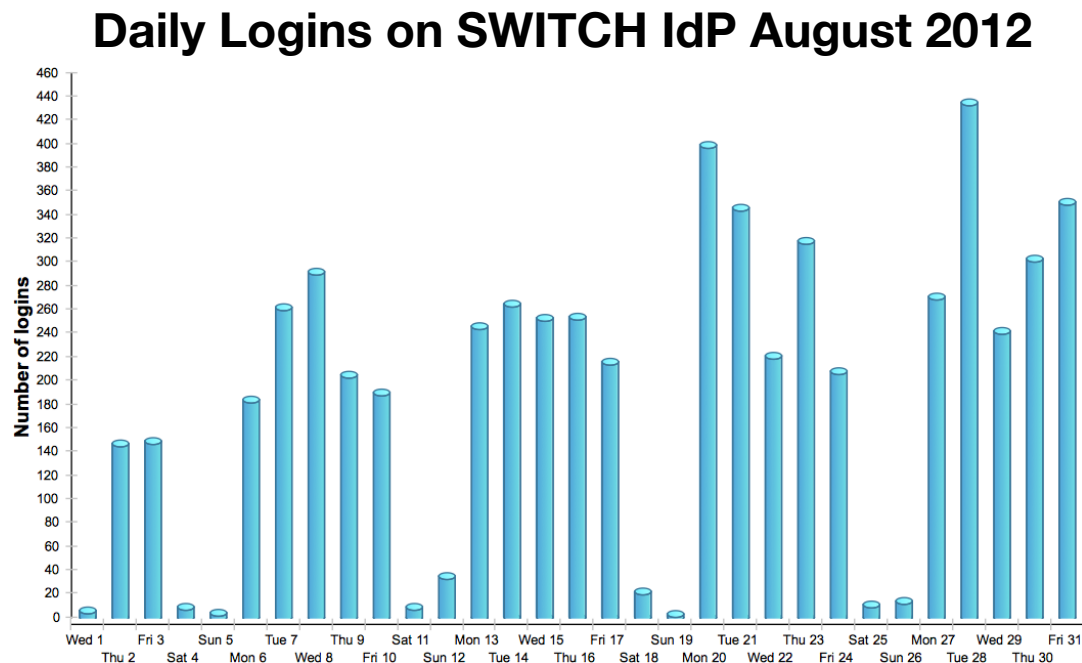
- Smaller coverage and slower adoption in Switzerland compared to AAI
- Partly due to alternatives:
 - Universities mutually allow access to their VPN concentrators
 - open Wifi (like here at PSI)

The Future



Monitoring with AMAAIS

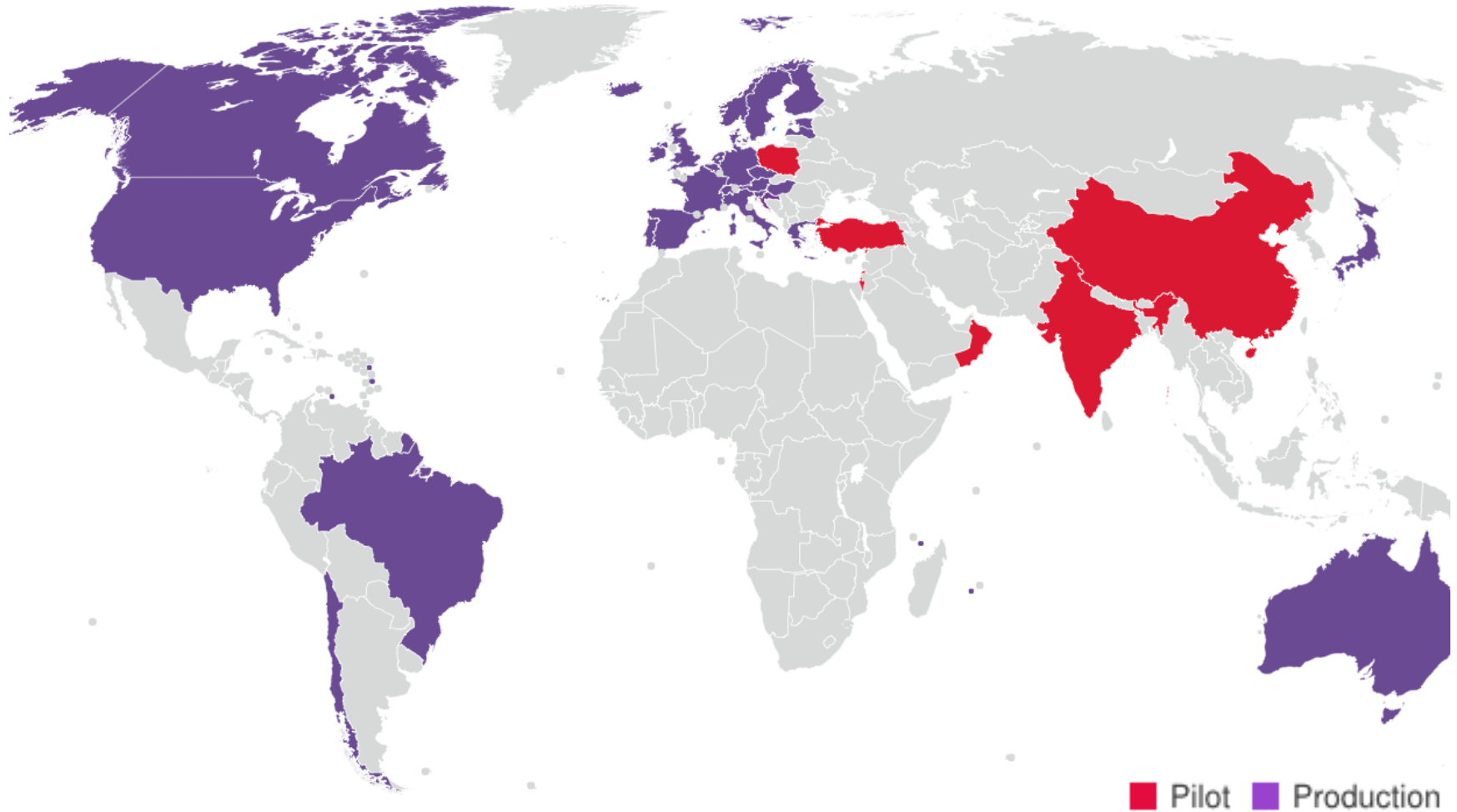
- No accurate user statistics currently in a meshed federation like SWITCHaai
- Only IdPs have accurate statistics



Growth on National Level

- Coverage in Higher Education is 98%
- Upper secondary students are the future university students
- Swiss Cantons can join AAI for Upper Secondary as Federation Partner
- Requires an Identity Management for Upper Secondary users
- Specific interest known from 5 of 26 cantons

Countries with an AAI



Growth on International Level

- Most AAls use/also support SAML2
 - Policies and architectures slightly differ
- Some university services are already part of other federations/bilaterally configured

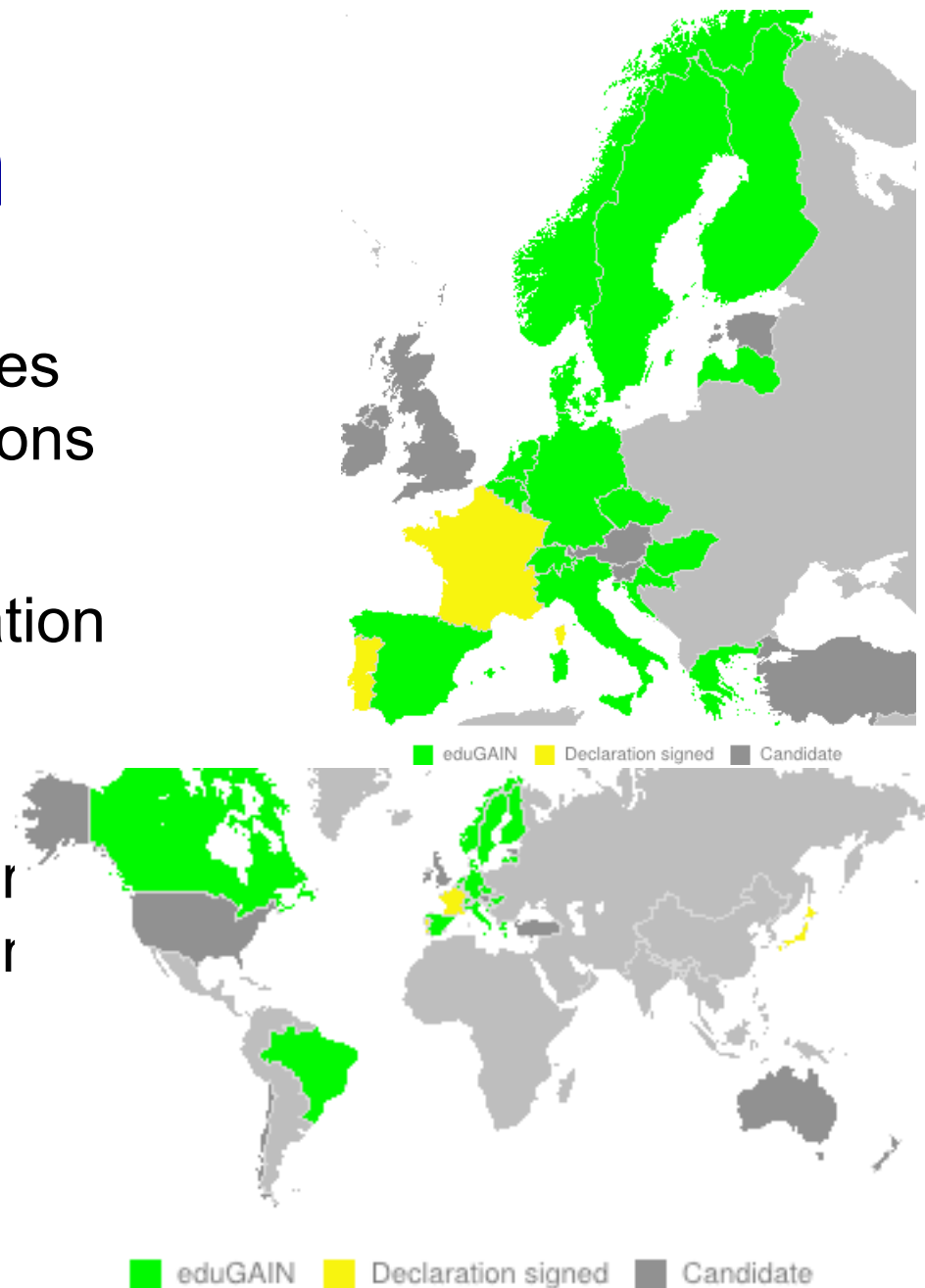
There is a natural move and a need for Interfederation

Interfederation

- Users get access to services registered in other federations
- eduGAIN is the interfederation service of GÉANT
- Rules and Guidelines regarding international data protection are still under debate

<http://edugain.org>

<http://switch.ch/aai/interfederation>



European Countries with eduroam

eduroam also available
in countries:

- North America
- South America
- APAN



Moonshot = eduroam + AAI

- Completely new technology consisting of already known technologies (SAML, Radius, EAP, GSS-API, SASL,...)
- Potential solution for non-browser apps
 - Take the best from eduroam (non-browser support) + AAI (attributes)
- Moonshot pilot starts in April

Summary

- Involving the universities helped AAI to get accepted and become successful faster
- International research projects face similar issues like Virtual Campus Switzerland 10 years ago
- AAI in Switzerland needed about 3 years to reach critical mass