Embedded Discovery Service

Or how to save some clicks during AAI authentication.

Where Are You From?

SWITCH

Serving Swiss Universities

Lukas Hämmerle
lukas.haemmerle@switch.ch

Zurich, 5. May 2009

Raider is now Twix… and WAYF is now DS

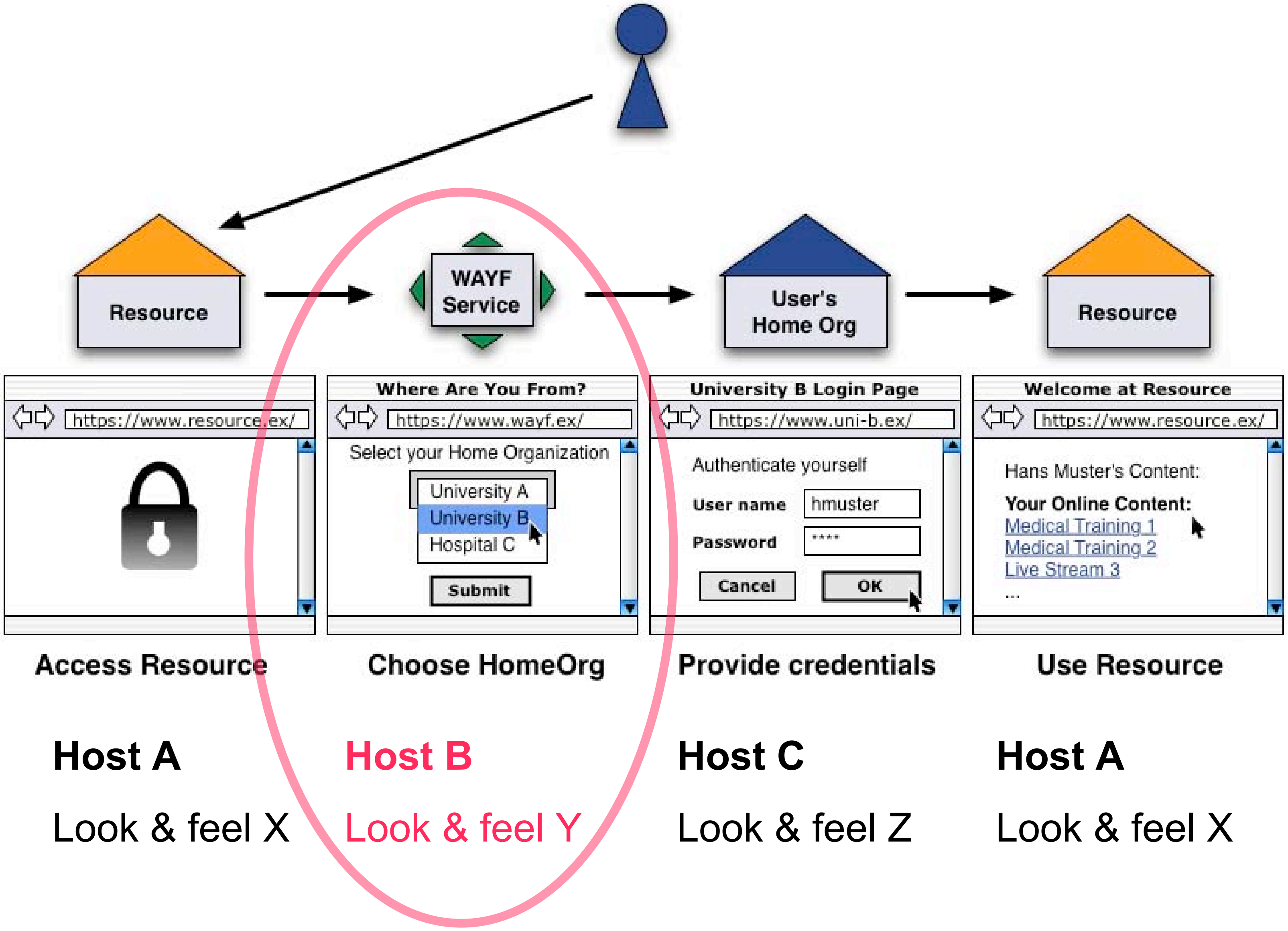
=

WAYF = **DS**

Where Are You From Service — Discovery Service

We (and others) still use both terms synonymously while DS is the technical correct term as defined in SAML specification.

The usual AAI login procedure



https://www.resource.ex/

Where Are You From?

https://www.wayf.ex/

Select your Home Organization

University A
University B
Hospital C

Submit

University B Login Page

https://www.uni-b.ex/

Authenticate yourself

User name: hmuster

Password: ****

Cancel OK

Welcome at Resource

https://www.resource.ex/

Hans Muster's Content:

Your Online Content:

Medical Training 1
Medical Training 2
Live Stream 3
...

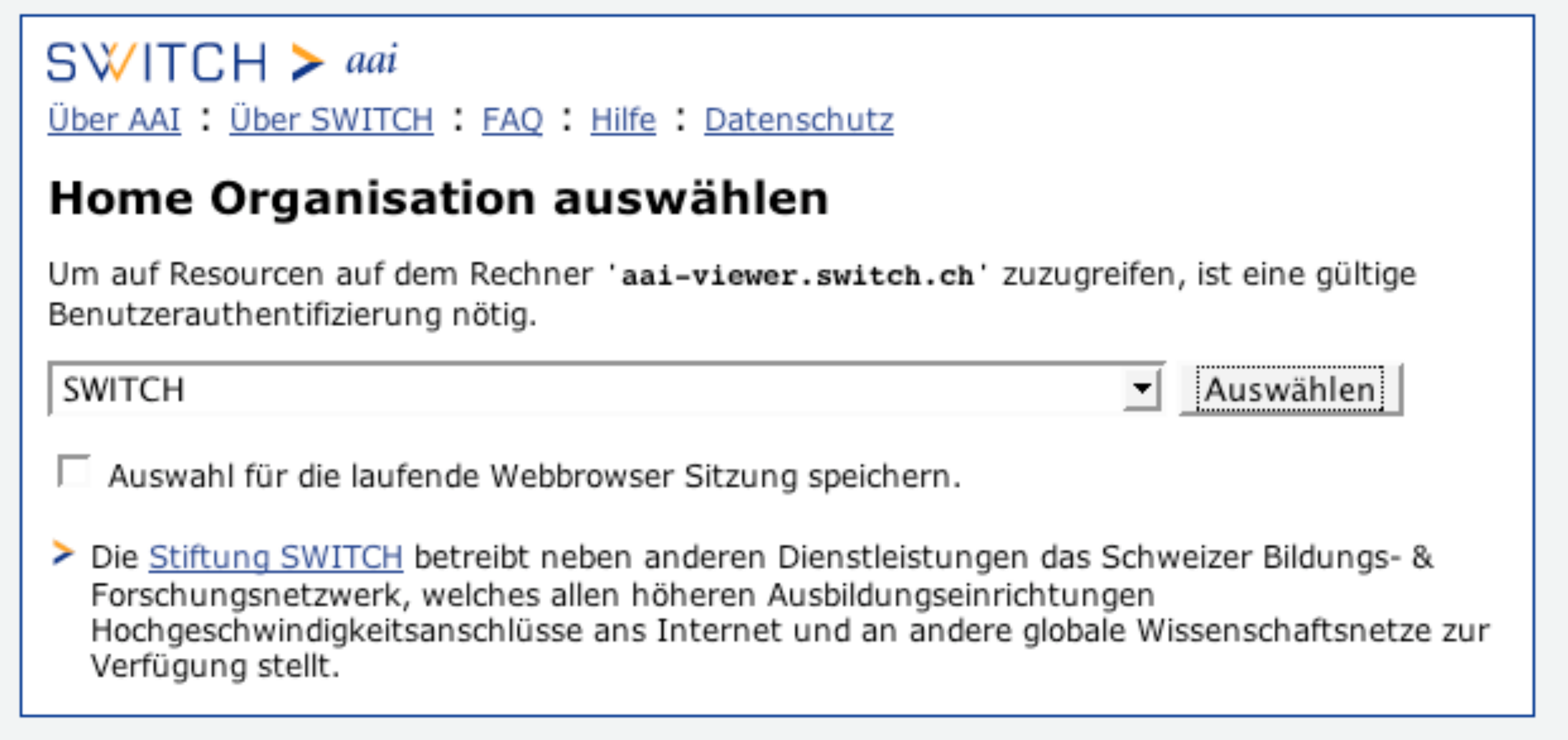
Access Resource	Choose HomeOrg	Provide credentials	Use Resource
Host A	**Host B**	**Host C**	**Host A**
Look & feel X	Look & feel Y	Look & feel Z	Look & feel X

History of the Discovery Service

- **Stone age: Central federation DS (see previous slide)**
  - Every federation operates some kind of a central WAYF/DS
  - E.g. wayf.switch.ch for SWITCHaai
  - Different domain, different look & feel, one more click for user
- **Bronze age: Self-Integrated DS**
  - Some applications have started using integrated WAYF
  - E.g. OLAT, ILIAS, Moodle
  - Has to be implemented and maintained by admin, cannot use cookie from central wayf to preselect Home Org, no statistics
- **Iron age: Embedded DS**
  - Embedded WAYF also allows other resources to easily integrate WAYF benefiting also from other features

Stone Age: Central DS

- For SWITCHaai: wayf.switch.ch
- Load-balanced and with high availability



Home Organisation auswählen

Um auf Resourcen auf dem Rechner '**aai-viewer.switch.ch**' zuzugreifen, ist eine gültige Benutzerauthentifizierung nötig.

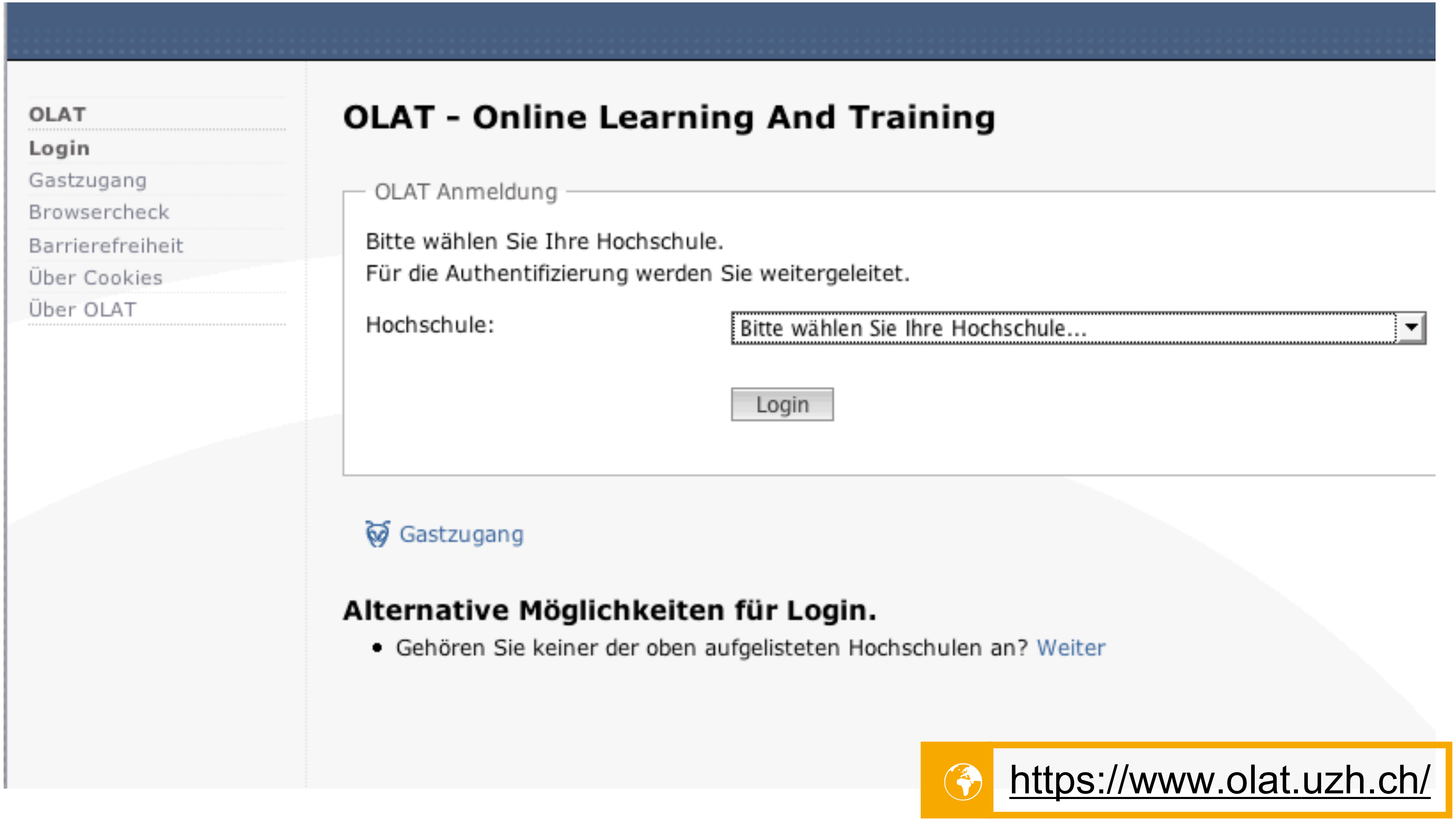
SWITCH ▾ Auswählen

□ Auswahl für die laufende Webbrowser Sitzung speichern.

> Die Stiftung SWITCH betreibt neben anderen Dienstleistungen das Schweizer Bildungs- & Forschungsnetzwerk, welches allen höheren Ausbildungseinrichtungen Hochgeschwindigkeitsanschlüsse ans Internet und an andere globale Wissenschaftsnetze zur Verfügung stellt.

Bronze Age: Self-Integrated DS

Was first and still is used by OLAT. Custom implementation



OLAT - Online Learning And Training

OLAT Anmeldung

Bitte wählen Sie Ihre Hochschule.
Für die Authentifizierung werden Sie weitergeleitet.

Hochschule: Bitte wählen Sie Ihre Hochschule...

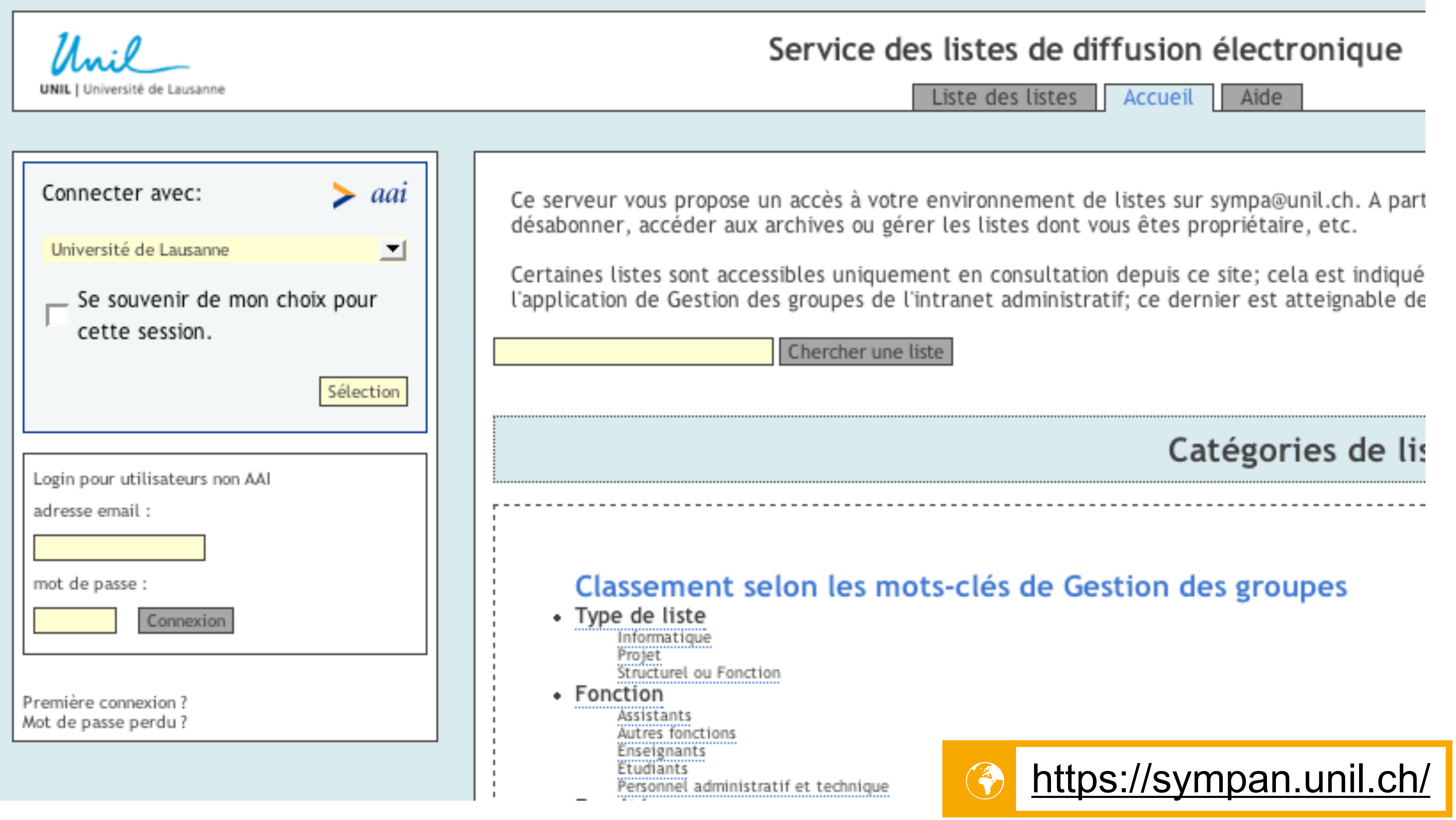
Alternative Möglichkeiten für Login.

- Gehören Sie keiner der oben aufgelisteten Hochschulen an? Weiter

https://www.olat.uzh.ch/

Iron Age: Embedded DS

Already used by half a dozen sites



UNIL | Université de Lausanne

Service des listes de diffusion électronique

Connecter avec: aai

Université de Lausanne

□ Se souvenir de mon choix pour cette session.

Login pour utilisateurs non AAI

adresse email :

mot de passe :

Première connexion ?
Mot de passe perdu ?

Ce serveur vous propose un accès à votre environnement de listes sur sympa@unil.ch. A part
désabonner, accéder aux archives ou gérer les listes dont vous êtes propriétaire, etc.

Certaines listes sont accessibles uniquement en consultation depuis ce site; cela est indiqué
l'application de Gestion des groupes de l'intranet administratif; ce dernier est atteignable de

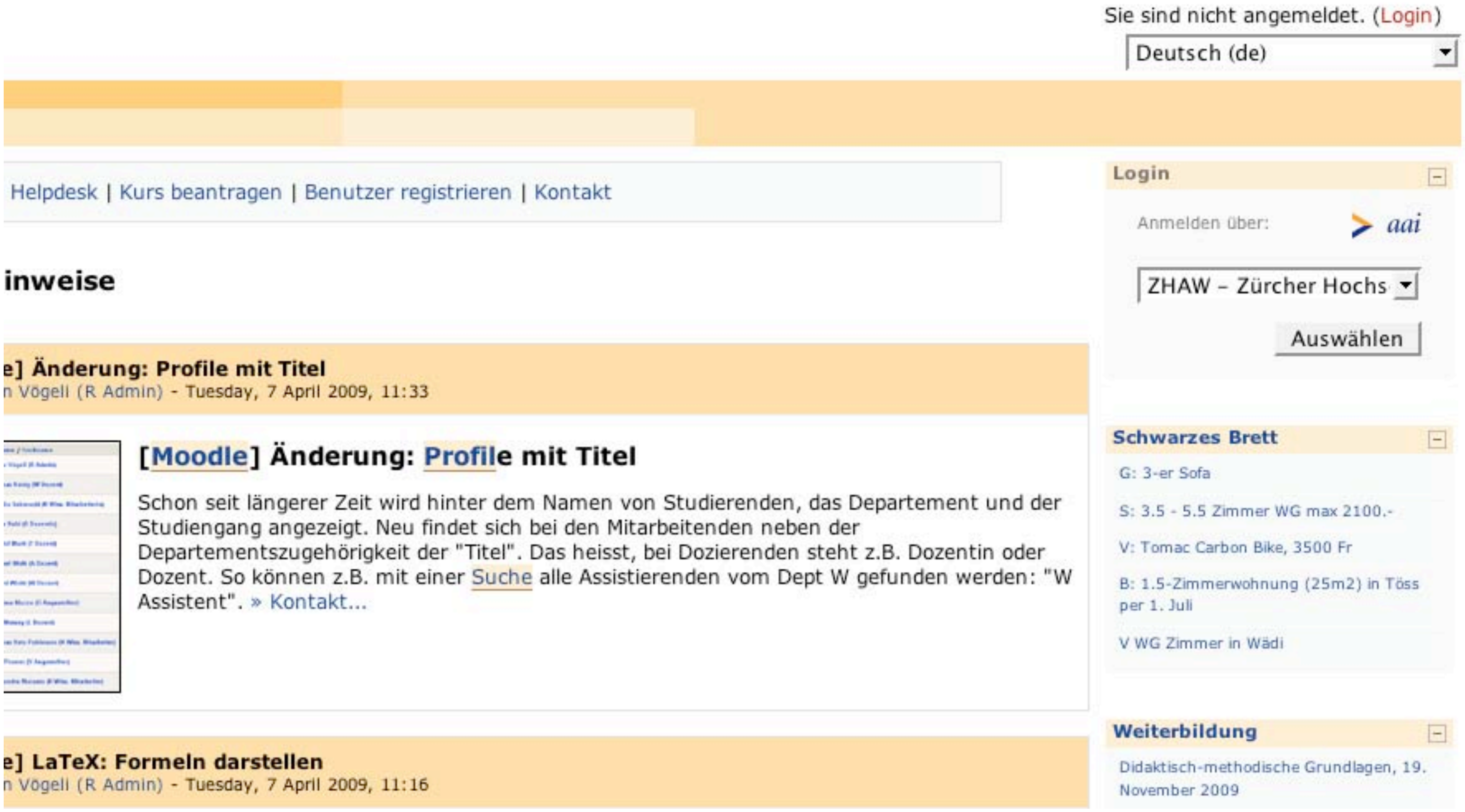
Catégories de lis

Classement selon les mots-clés de Gestion des groupes

- Type de liste
  - Informatique
  - Projet
  - Structurel ou Fonction
- Fonction
  - Assistants
  - Autres fonctions
  - Enseignants
  - Etudiants
  - Personnel administratif et technique

https://sympan.unil.ch/

Another example



Sie sind nicht angemeldet. (Login)

Deutsch (de)

Helpdesk | Kurs beantragen | Benutzer registrieren | Kontakt

inweise

e] Änderung: Profile mit Titel

n Vögeli (R Admin) - Tuesday, 7 April 2009, 11:33

[Moodle] Änderung: Profile mit Titel

Schon seit längerer Zeit wird hinter dem Namen von Studierenden, das Departement und der Studiengang angezeigt. Neu findet sich bei den Mitarbeitenden neben der Departementszugehörigkeit der "Titel". Das heisst, bei Dozierenden steht z.B. Dozentin oder Dozent. So können z.B. mit einer Suche alle Assistierenden vom Dept W gefunden werden: "W Assistent". » Kontakt...

e] LaTeX: Formeln darstellen

n Vögeli (R Admin) - Tuesday, 7 April 2009, 11:16

Login

Anmelden über: aai

ZHAW – Zürcher Hochs

Schwarzes Brett

G: 3-er Sofa

S: 3.5 - 5.5 Zimmer WG max 2100.-

V: Tomac Carbon Bike, 3500 Fr

B: 1.5-Zimmerwohnung (25m2) in Töss per 1. Juli

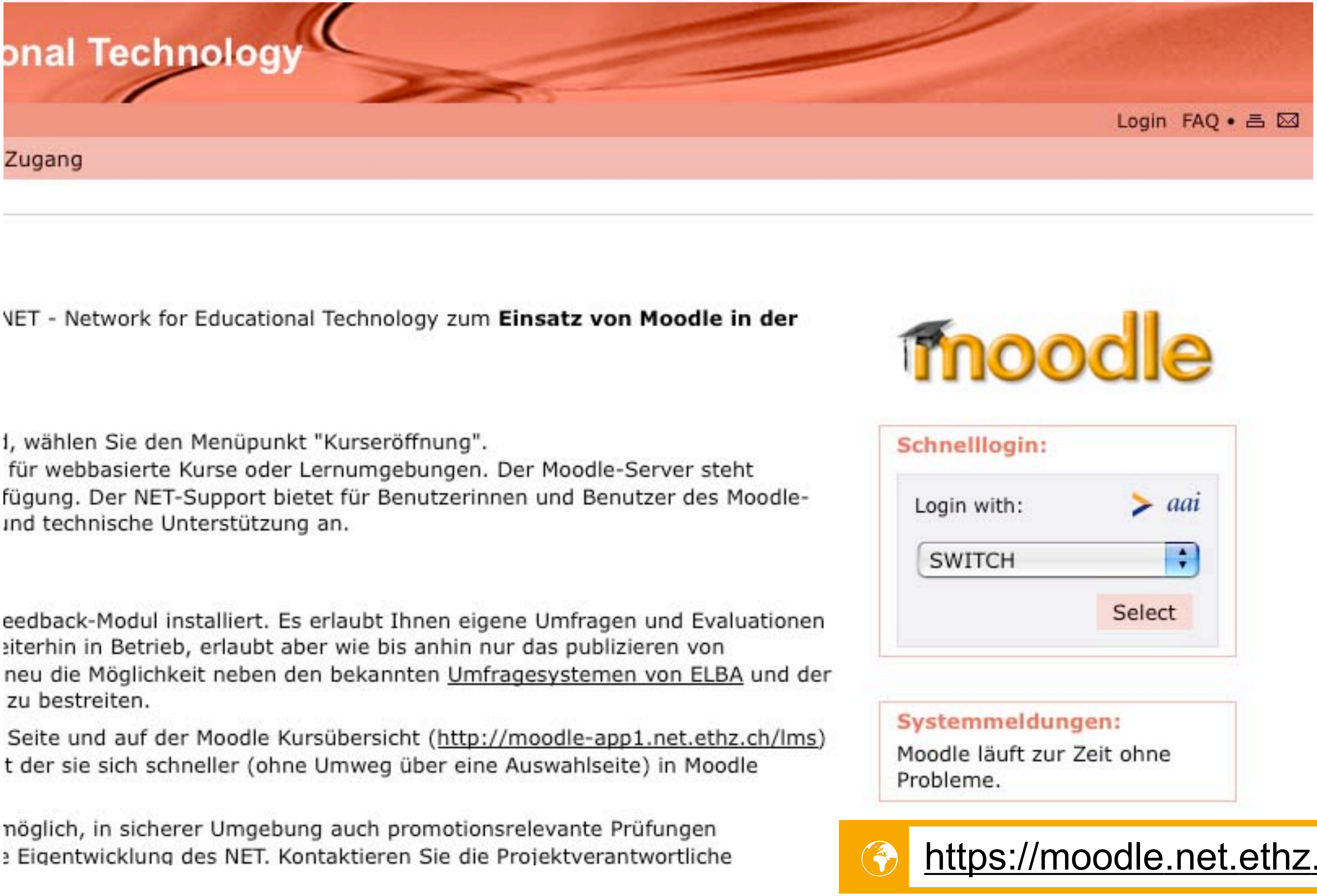
V WG Zimmer in Wädi

Weiterbildung

Didaktisch-methodische Grundlagen, 19. November 2009

https://elearning.zhaw.ch/

… and another one



onal Technology

Login FAQ •

Zugang

NET - Network for Educational Technology zum **Einsatz von Moodle in der**

d, wählen Sie den Menüpunkt "Kurseröffnung". für webbasierte Kurse oder Lernumgebungen. Der Moodle-Server steht fügung. Der NET-Support bietet für Benutzerinnen und Benutzer des Moodle- und technische Unterstützung an.

eedback-Modul installiert. Es erlaubt Ihnen eigene Umfragen und Evaluationen eiterhin in Betrieb, erlaubt aber wie bis anhin nur das publizieren von neu die Möglichkeit neben den bekannten Umfragesystemen von ELBA und der zu bestreiten.

Seite und auf der Moodle Kursübersicht (http://moodle-app1.net.ethz.ch/lms) t der sie sich schneller (ohne Umweg über eine Auswahlseite) in Moodle

nöglich, in sicherer Umgebung auch promotionsrelevante Prüfungen e Eigentwicklung des NET. Kontaktieren Sie die Projektverantwortliche

moodle

Schnelllogin:

Login with: aai

SWITCH

Select

Systemmeldungen:

Moodle läuft zur Zeit ohne Probleme.

https://moodle.net.ethz.ch/

How it works

- Embed 2 JavaScripts and a <NOSCRIPT> element for fallback:
  - https://wayf.switch.ch/SWITCHaai/WAYF/embedded-wayf.js/snippet.html

1. **Configuration script**
   - Influences look and feel (colors, size, etc.)
   - Can be used to exclude IdPs from list or add from other federations
   - Configures some of the logic (e.g. to show “Remember” checkbox or not)

2. **Logic script**
   - Generated by and loaded from central SWITCHaai WAYF
   - Custom tailored based on cookies available to central WAYF
     - ❑ This allows IdP preselection or direct redirection

3. **Non-Javascript Fallback**
   - For those people who live outside of Web 2.0 land

All you need is love… ahm, or some code :-)

Example code (configuration for aai-viewer.switch.ch)

```
<!-- 1. Configuration script -->
<script type="text/javascript"><!--
wayf_use_discovery_service = false;
wayf_sp_entityID = "https://aai-viewer.switch.ch/shibboleth";
wayf_sp_handlerURL = "https://aai-viewer.switch.ch/Shibboleth.sso";
wayf_sp_samlDSURL = "https://aai-viewer.switch.ch/Shibboleth.sso/DS";
wayf_URL = "https://wayf.switch.ch/SWITCHaai/WAYF";
wayf_return_url = "https://aai-viewer.switch.ch/aai/";
</script>
<!-- 2. Logic script loaded from central WAYF -->
<script type="text/javascript"
  src="https://wayf.switch.ch/SWITCHaai/WAYF/embedded-wayf.js"></script>
<!-- 3. Fallback for non-JavaScript users -->
<noscript>
  <p><strong>Login:</strong> Since Javascript is not activated or not available in
  your web browser, you have to
  <a href="https://aai-viewer.switch.ch/aai/">proceed manually</a>.</p>
</noscript>
```

Behind the scenes

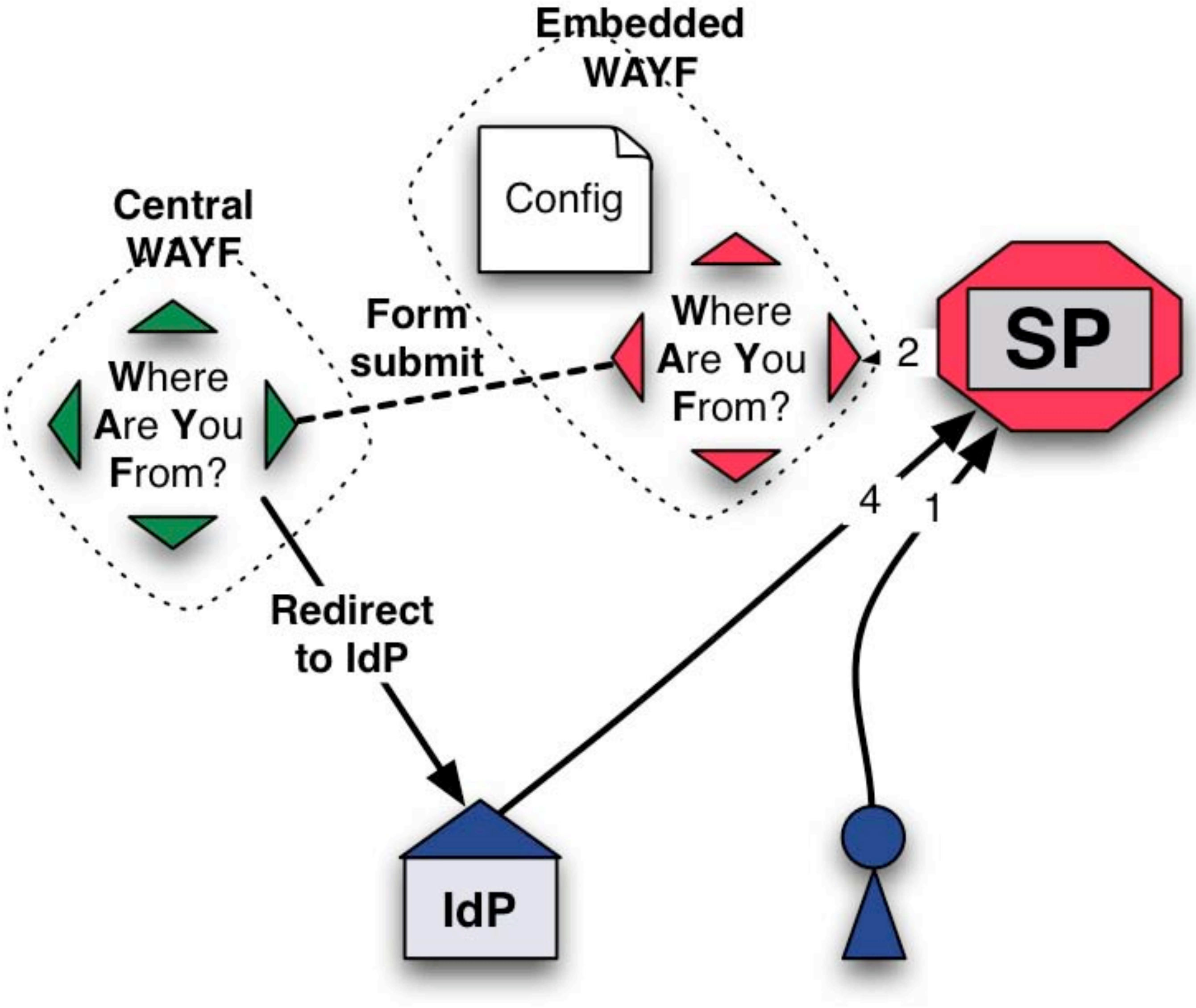
Works like Google Ads but won't display ads :-)

1. Logic script is loaded from central SWITCHaai WAYF
   - By loading the JS, the browser also sends cookies to wayf.switch.ch containing the last used IdP
   - Central WAYF custom-tailors JS using cookie information

2. It then inserts the WAYF HTML form using options from configuration script
   - E.g. document.write(‘<form action=“https://wayf.switch.ch”>’)

3. Central WAYF handles input after submit and transparently redirects user to selected IdP

Resulting Login Flow



What you as Resource admin benefit

- **Easy to integrate and no maintenance**
  - Only 5 mandatory settings
  - Integrated in less than 1 minute
  - Automatically updated, e.g. when new IdPs join SWITCHaai

- **Comprehensive controls over look and feel**
  - 18 optional settings for size, colors, behavior, etc.
  - Even more customizable using local CSS styles
  - Translated in en, fr, it, de, pt

- **Adapt IdPs in drop-down list**
  - Hide certain IdPs or categories that cannot access Resource
  - E.g. only universities and the VHO

What your users benefit

- **More consistent look & feel**
  - Embedded DS takes over layout of your site
  - Transparent (not noticeable) redirect to central WAYF (wayf.switch.ch)
- **Saves at minimum one click**
  - No click required anymore to get to the WAYF
  - **Zero Click Login**: If user already is logged in on another Resource that uses central/embedded WAYF and if “Remember selection” checkbox was checked, user can be logged in automatically
- **IdP Pre-selection for all embedded WAYFs**
  - Works even if you are the first time on a Resource
  - Still won’t work on other sites that have their built-in WAYF implementation like OLAT, ILIAS or Moodle

How to use embedded WAYF

- **Step 1:**
  - Go to https://rr.aai.switch.ch/gen_embedding_code.php
- **Step 2:**
  - Using the entityID of your resource, select your resource from list The script will use information from the Resource Registry to generate the embedded WAYF configuration code.
- **Step 3:**
  - Copy and paste the resulting HTML code to any web page. This page can also be on a host where Shibboleth is not installed.
- **Step 4** (optional)**:**
  - Customize optional settings like size, colors, IdPs to show etc.

Features and Configuration Options

- Set:
  - size of WAYF box
  - font size and color
  - background color
  - border color
  - large or small AAI logo to use
- Whether to show “Remember selection” checkbox
- Disable Zero-Click login
- Hide certain IdPs or categories of IdPs
- Set a default IdP to preselect if user has never been on central WAYF
- Customize “Already logged in ”message
- Add IdPs from other federations

Limitations and Considerations

- **Users need JavaScript to be turned on**
  - As is the case for Google Ads, Facebook and all Web 2.0 sites
  - But there is a fall back included in the HTML snippet of the embedded WAYF using the <NOSCRIPT> element, points to central WAYF
- **Central WAYF must be highly available and reliable**
  - wayf.switch.ch uses high availability solution. Hasn't had any downtime for years
  - Risk comes more from unnoticed logic errors in the code of new versions
- **Embedded WAYF cannot always know when user is logged in or out**
  - Depends on the cookies that can be read by the embedded WAYF
  - Depends on where code is embedded (cookies are set for hosts)
- **Loading remote JavaScript opens door to your web site**
  - Same for GoogleAds or any JavaScript loaded from remote sites
  - In case the SWITCHaai WAYF gets compromised, attacker could change anything on sites that use embedded WAYF
  - SWITCHaai WAYF is protected and monitored with IDS

Summary

The Embedded WAYF

- Allows **easy integration** of a WAYF into your web page
- Is maintained and **updated automatically**
- Can be **custom-tailored** in look & feel
- At minimum **one click is saved**

See it in action/more information: 🌐 https://aai-viewer.switch.ch/

🌐 http://www.switch.ch/aai/support/serviceproviders/sp-embedded-wayf.html

Many thanks for the valuable feedback from the ETHZ NET and the ZHAW e-learning team for the many suggestions.