AAI for mandatory authentication and proxy usage to allow internet access on public workstations of ETH-Bibliothek

Wolfgang Lierz, ETH-Bibliothek, IT Services
Cristian Tuduce, ETH Zürich, ID-Basisdienste

Outline

- The ETH proxy infrastructure

  Cristian
- The ETH-Bibliothek solution

  Wolfgang

The web-proxy

From appliance to Squid:

- Appliance end-of-life
- Many appliances use variations of Squid

Authenticating:

- Users connecting from outside ETH
- Selected IP ranges from inside ETH

Squid authentication problems

- RADIUS with basic authentication
- Clear-text channel between client and proxy
- Skinny authentication-helper interface

→Sniffing trivial

→Password guessing attacks

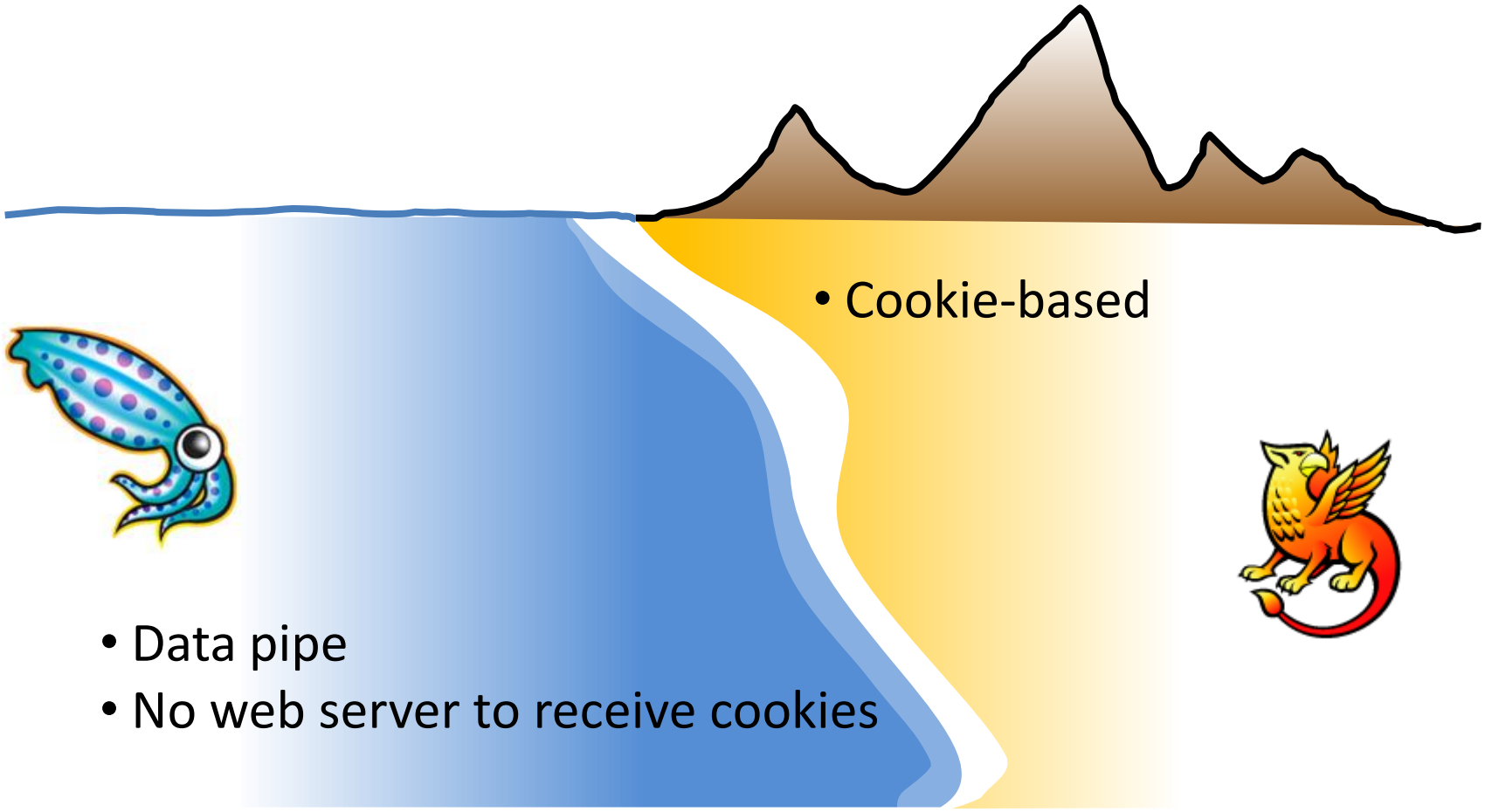
Solution: Squid with Shibboleth authentication!

Why Shibboleth

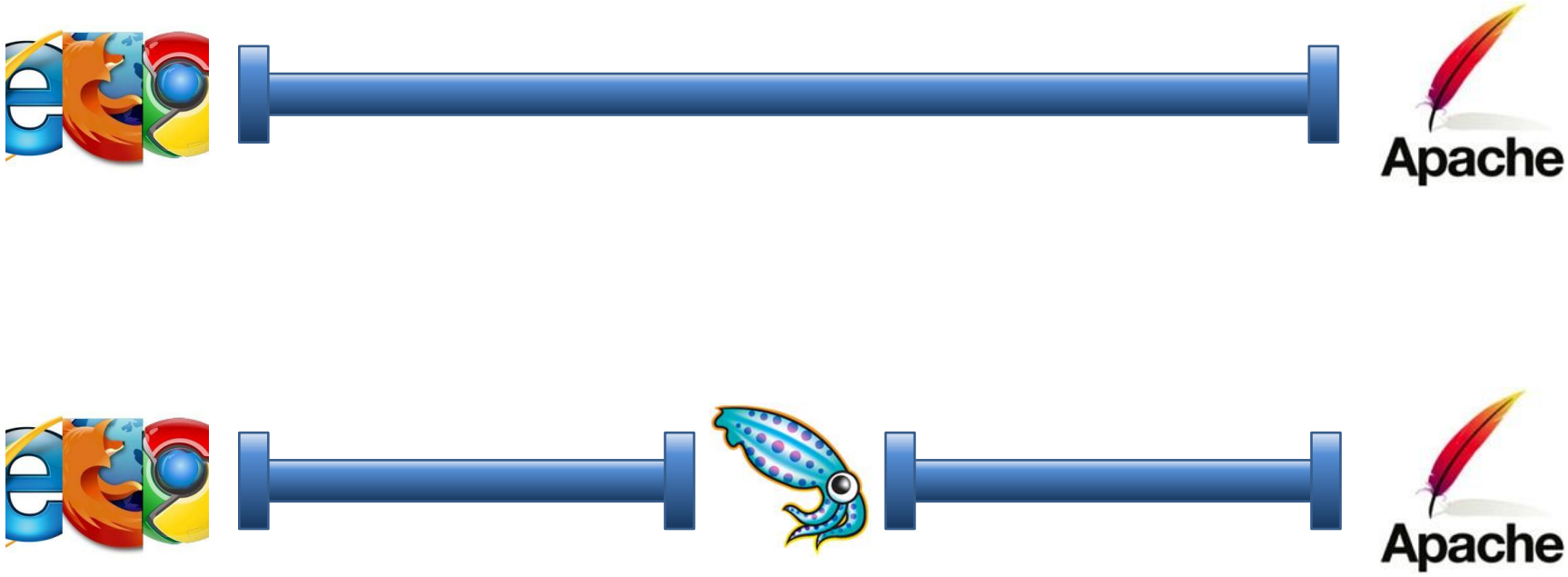
- No passwords floating around insecure
- Password guessing cumbersome
- [put favorite reason here]

- Interesting problem!

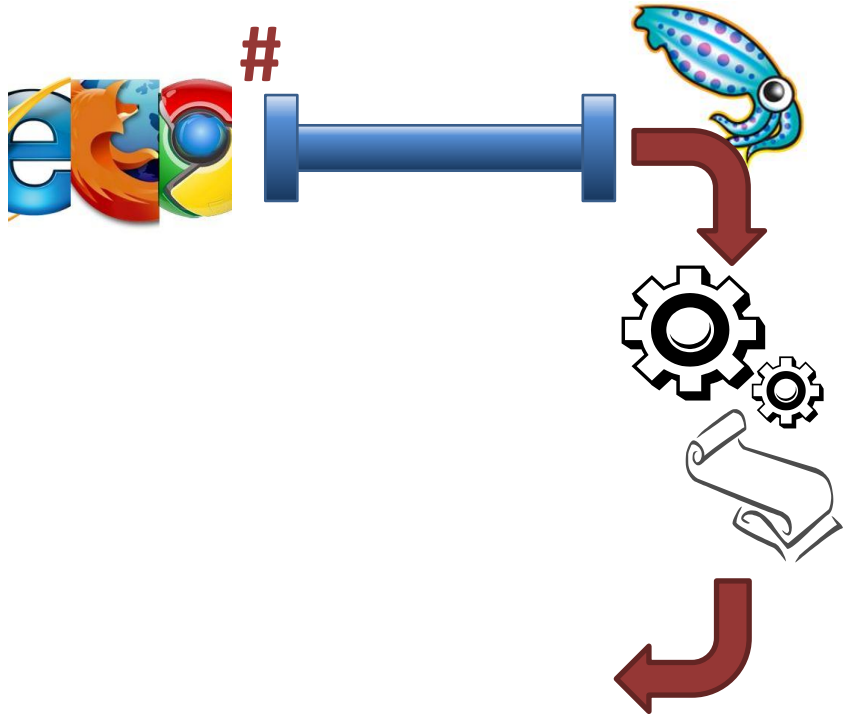
The challenge: different worlds



The proxy principle

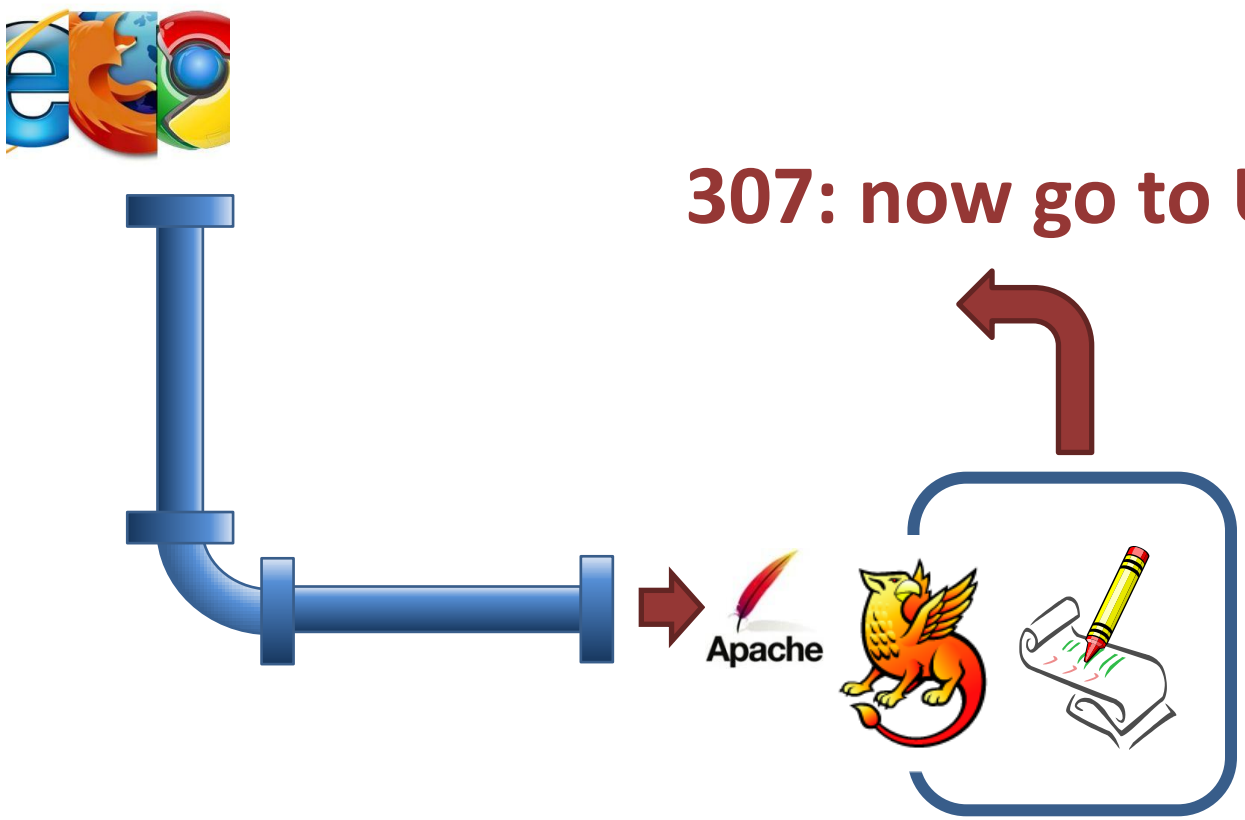


Before authentication

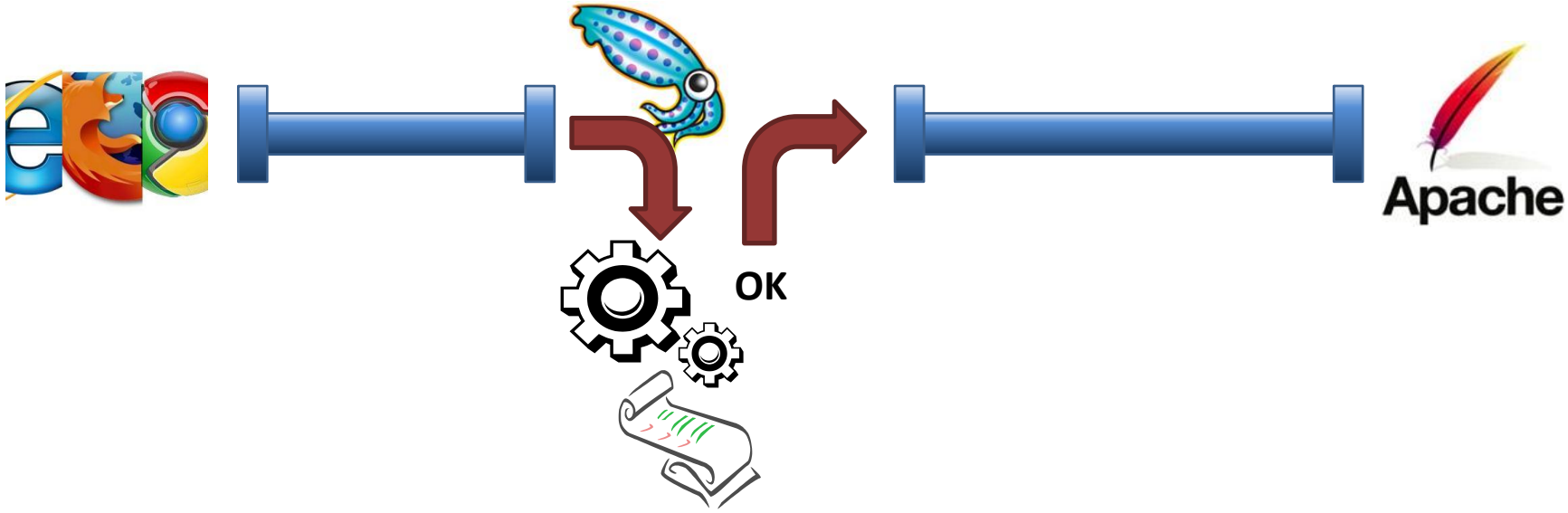


307: go authenticate (then #)!

The authentication process



After authentication

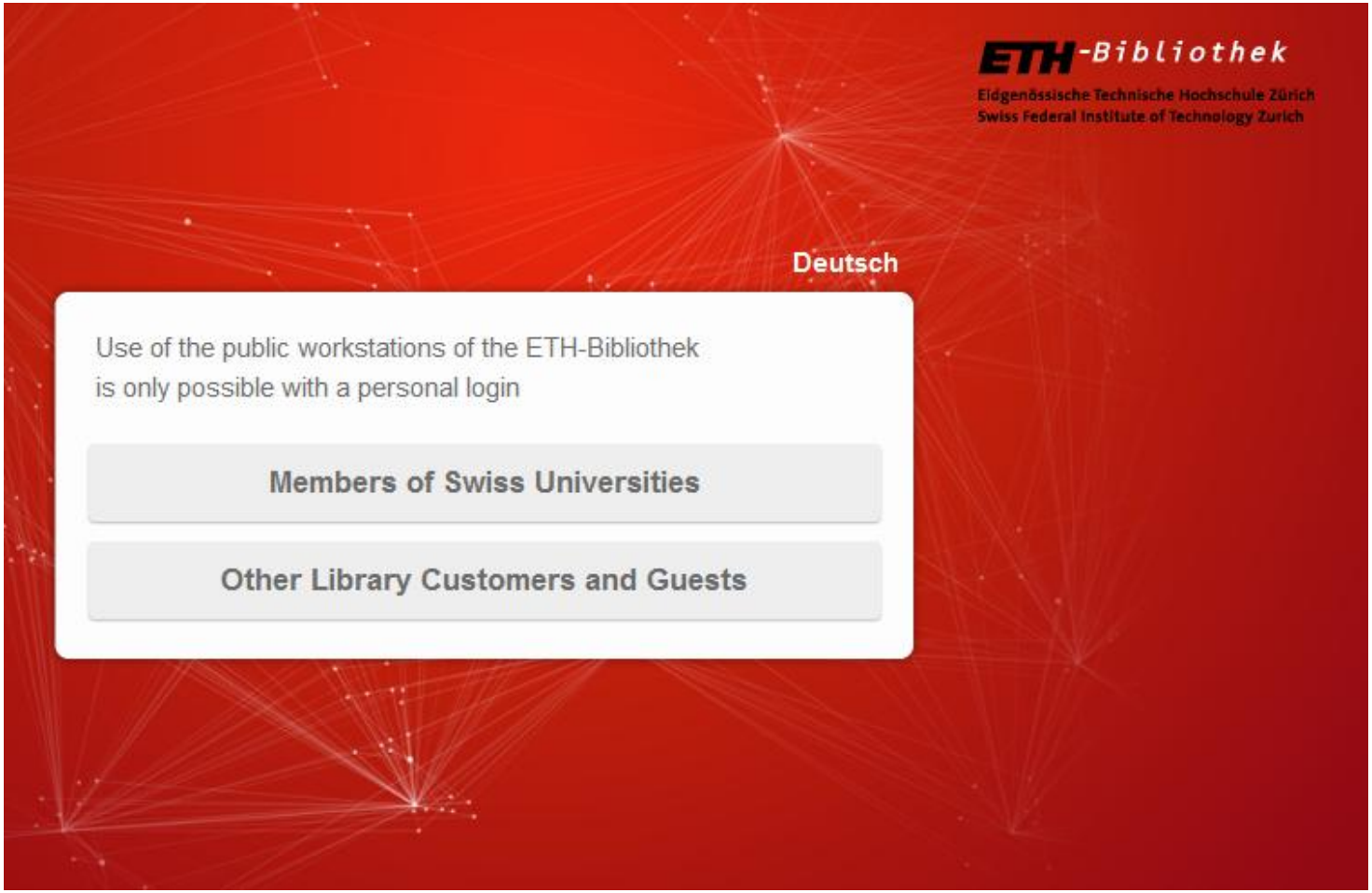


The building block

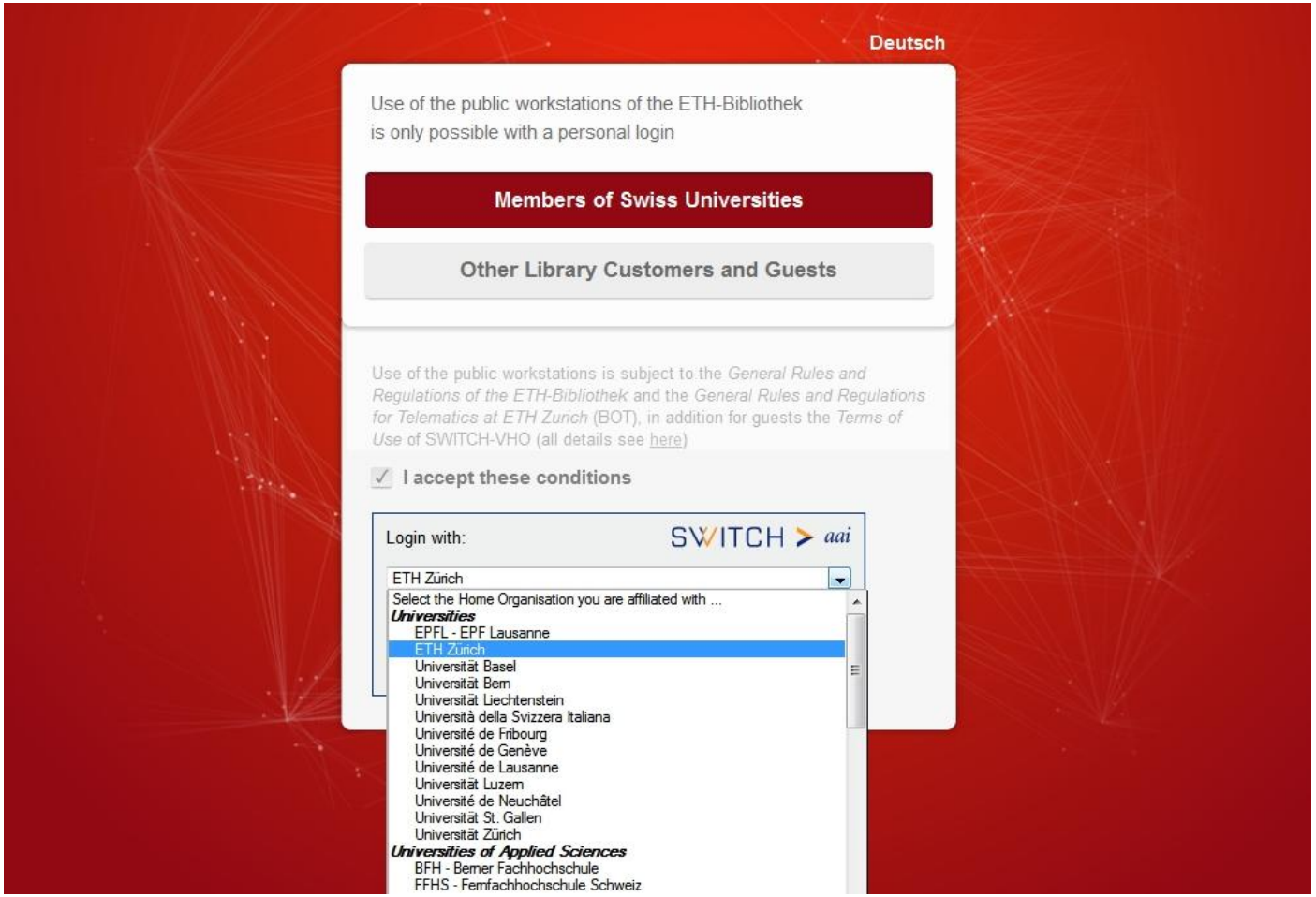
AAI-enabling public workstations of ETH-Bibliothek: requirements

- authentication itself is the service!
- AAI for customers outside SWITCHaai scope
- (time-limited) internet access via AAI-enabled proxy
- modifications on proxy.ethz.ch

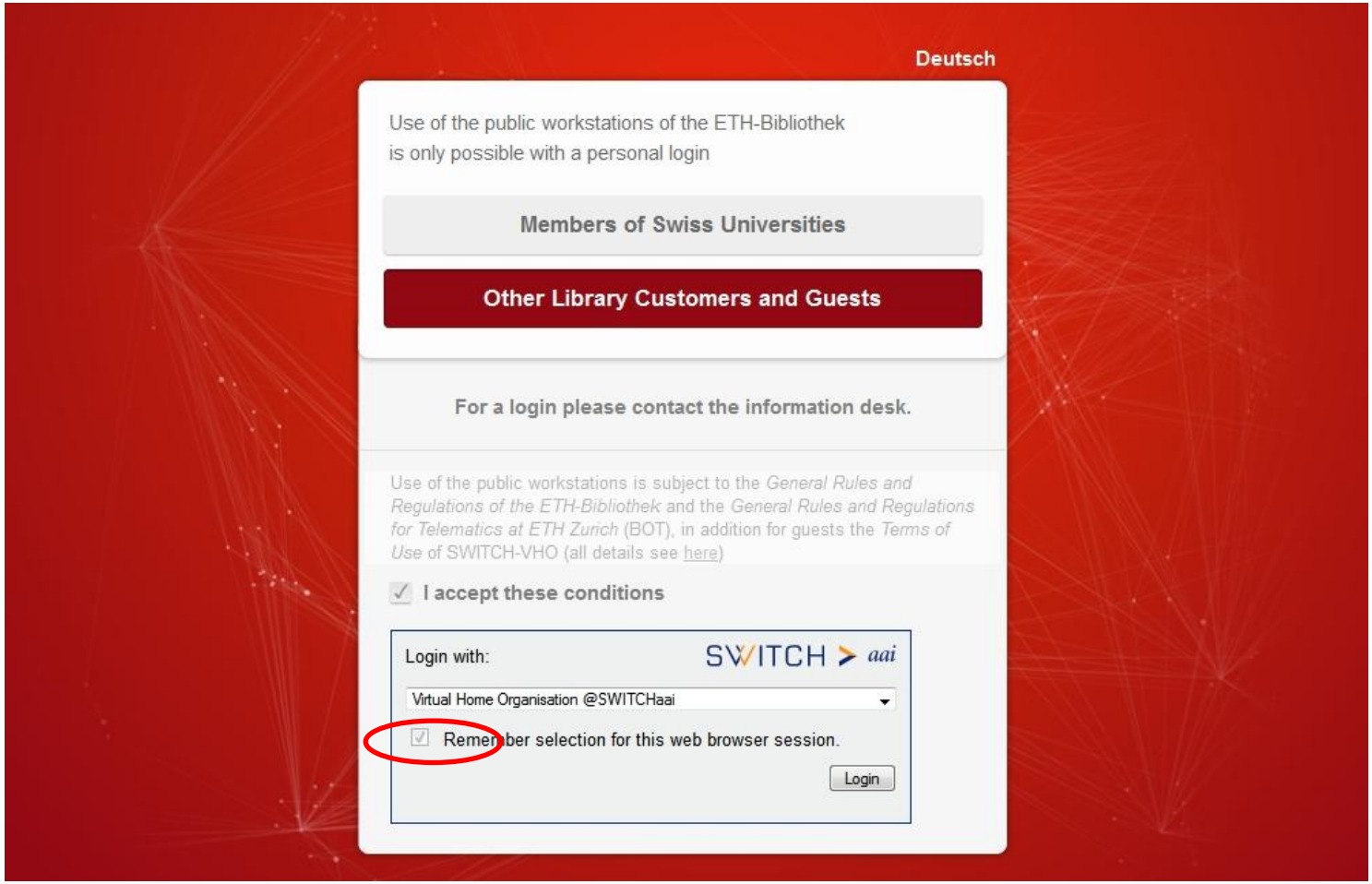
Authentication itself as service



AAI for Swiss university members



AAI for other library customers



Modifications on SWITCH embedded WAYF

- `wayf_force_remember_for_session = true;`
- `wayf_show_remember_checkbox = true;`

- `wayf_hide_categories = new Array("library","vho","upcoming");`

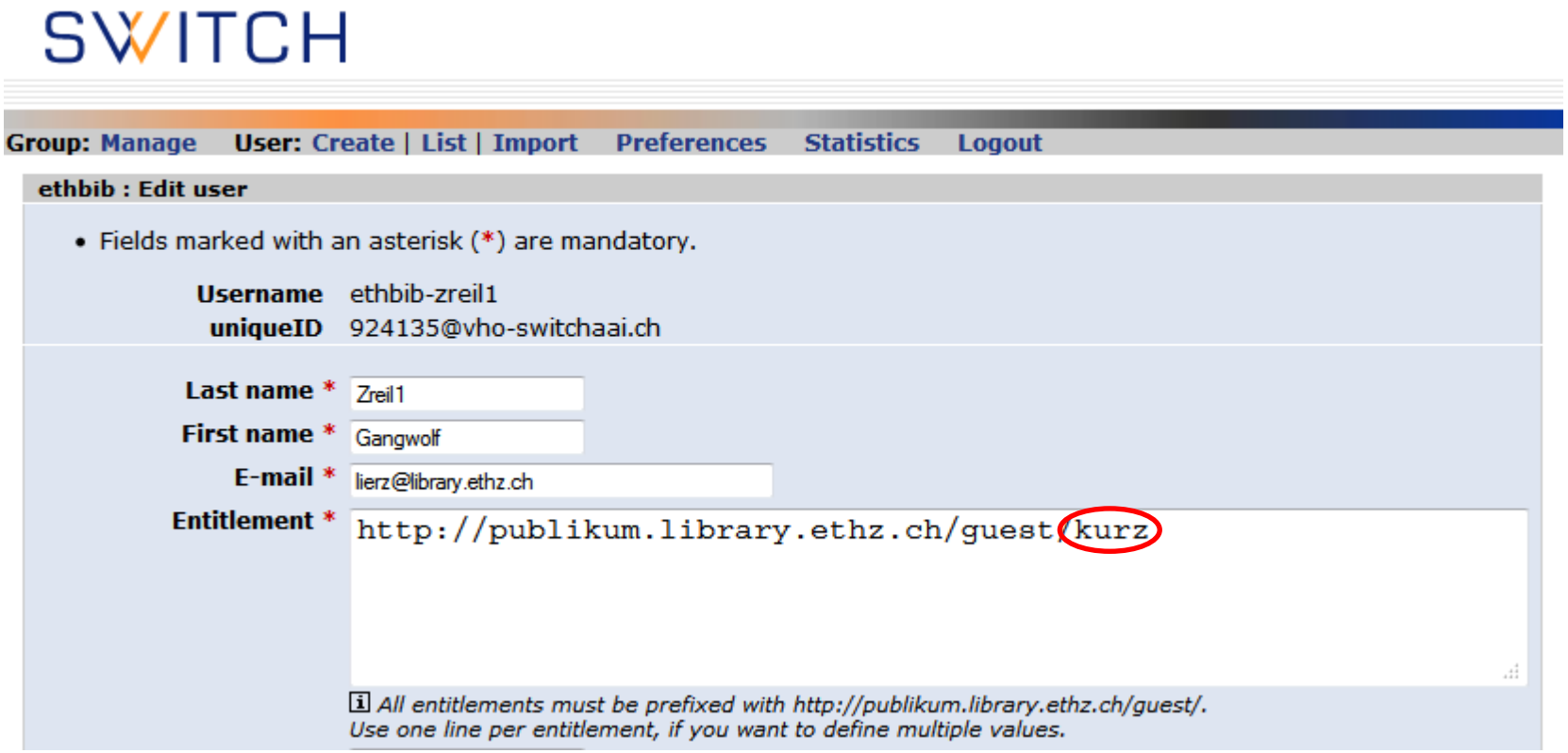
- `wayf_hide_categories = new Array("all");`
- `wayf_unhide_idps = new Array("https://aai-logon.vho-switchaai.ch/idp/shibboleth");`

- **`wayf_return_url`** = `"https://publikum.library.ethz.ch/login/aai/`**`pinlogin.php`**`";`

AAI-enabled service: login+redirect

- `https://publikum.library.ethz.ch/login/aai/pinlogin.php`
- `$hosts = $d->login_user();`
- `if($hosts) { header('Location: http://publikum.library.ethz.ch/login/error.html?duplicate'); }`
- `else { if($d->get_remaining_time())`
- `header('Location: http://www.library.ethz.ch/');`
- `else`
- `header('Location: http://publikum.library.ethz.ch/login/error.html?exceeded');}`

SWITCH VHO admin tool



PINlogin database viewer

ETH-Bibliothek
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Status PINlogin • Donnerstag, 19.05.2011

Status aktuell

Filter: zreil

ID	Email	Name	Typ	Station	Start	Ende
924135@vho-switchaai.ch	lierz@library.ethz.ch	Zreil1, Gangwolf	kurz	lib-pub-ics-00	2011-05-19 12:59:51	2011-05-19 13:49:45

Status Archiv

Filter: zreil

ID	Email	Name	Typ	Station	Start	Ende	Zeit
924135@vho-switchaai.ch	lierz@library.ethz.ch	Zreil1, Gangwolf	kurz	lib-pub-zls-01	2011-05-19 12:47:03	2011-05-19 13:47:03	606

```
// http://publikum.library.ethz.ch/proxy/publikum.pac

function FindProxyForURL(url, host) {

if (shExpMatch(url, "http*://publikum.library.ethz.ch/*")
 || shExpMatch(url, "https://tools.vho-switchaai.ch/*")
 || shExpMatch(url, "https://wayf.switch.ch/*"))
   {return "DIRECT";}

if (shExpMatch(url, "https://aai-logon.*.ch/*")
 || shExpMatch(url, "https://aai-login.*.ch/*")
 || shExpMatch(url, "https://aai-idp.*.ch/*")
 || shExpMatch(url, "https://aai.*.ch/*")
 || shExpMatch(url, "https://idp.*.ch/*")
 || shExpMatch(url, "https://login2.*.ch/*"))
   {return "DIRECT";}

if (shExpMatch(url, "http*://proxy.ethz.ch/*"))
   {return "DIRECT";}

   return "PROXY proxy.ethz.ch:3128"; }
```

Modifications on proxy.ethz.ch

- forcing proxy usage in public workstation subnets of ETH-Bibliothek
- allowing proxy usage from whole SWITCHaai community

Forcing proxy usage in library's public workstation subnets:

```
acl library-public-hg  src 129.132.73.0/25
acl library-public-rz  src 129.132.41.16/28
acl library-public-hix src 129.132.49.192/28
acl library-public-hpx src 129.132.49.208/28
acl library-public-nw  src 129.132.49.224/28
acl library-public-cx  src 129.132.166.32/27

url_rewrite_access allow library-public-hg
url_rewrite_access allow library-public-rz
url_rewrite_access allow library-public-hix
url_rewrite_access allow library-public-hpx
url_rewrite_access allow library-public-nw
url_rewrite_access allow library-public-cx
```

Allowing proxy usage from whole SWITCHaai community

```
sub decide_proxy_access() {
    my $ACCEPT_PROXY_ACCESS = 0;

    if ($ENV{'REMOTE_ADDR'} eq "129.132.202.35") {
          $ACCEPT_PROXY_ACCESS = 3;
          return $ACCEPT_PROXY_ACCESS;
    }

    my $ip_match = match_ip($ENV{'REMOTE_ADDR'},
                                "129.132.73.0/25",
                                "129.132.41.16/28",
                                "129.132.49.192/28",
                                "129.132.49.208/28",
                                "129.132.49.224/28",
                                "129.132.166.32/27",
                                "129.132.238.45");

    if ($ENV{'HTTP_SHIB_SWISSEP_HOMEORGANIZATION'} eq "ethz.ch") {
          $ACCEPT_PROXY_ACCESS = 1;
          return $ACCEPT_PROXY_ACCESS;
    } else {
          if ($ip_match) {
              if ($ENV{'HTTP_SHIB_SWISSEP_HOMEORGANIZATIONTYPE'} =~
                     /^(university|uas|hospital|others|vho)$/) {
                   $ACCEPT_PROXY_ACCESS = 1;
                   return $ACCEPT_PROXY_ACCESS;
```

Hiding AAI dialogues of proxy

- only implicit because authentication is already done before
- no severe complaints from users getting confused when trying to overcome limitation

Conclusion

- Robust solution running since 2011-02-07
- Only few modifications of central proxy server needed
- Only very small modification of WAYF needed
- Can be easily extended/migrated as soon other AAI Identity Providers for private library customers are available

Questions ?

Live demo ?