Account Checking on a SP

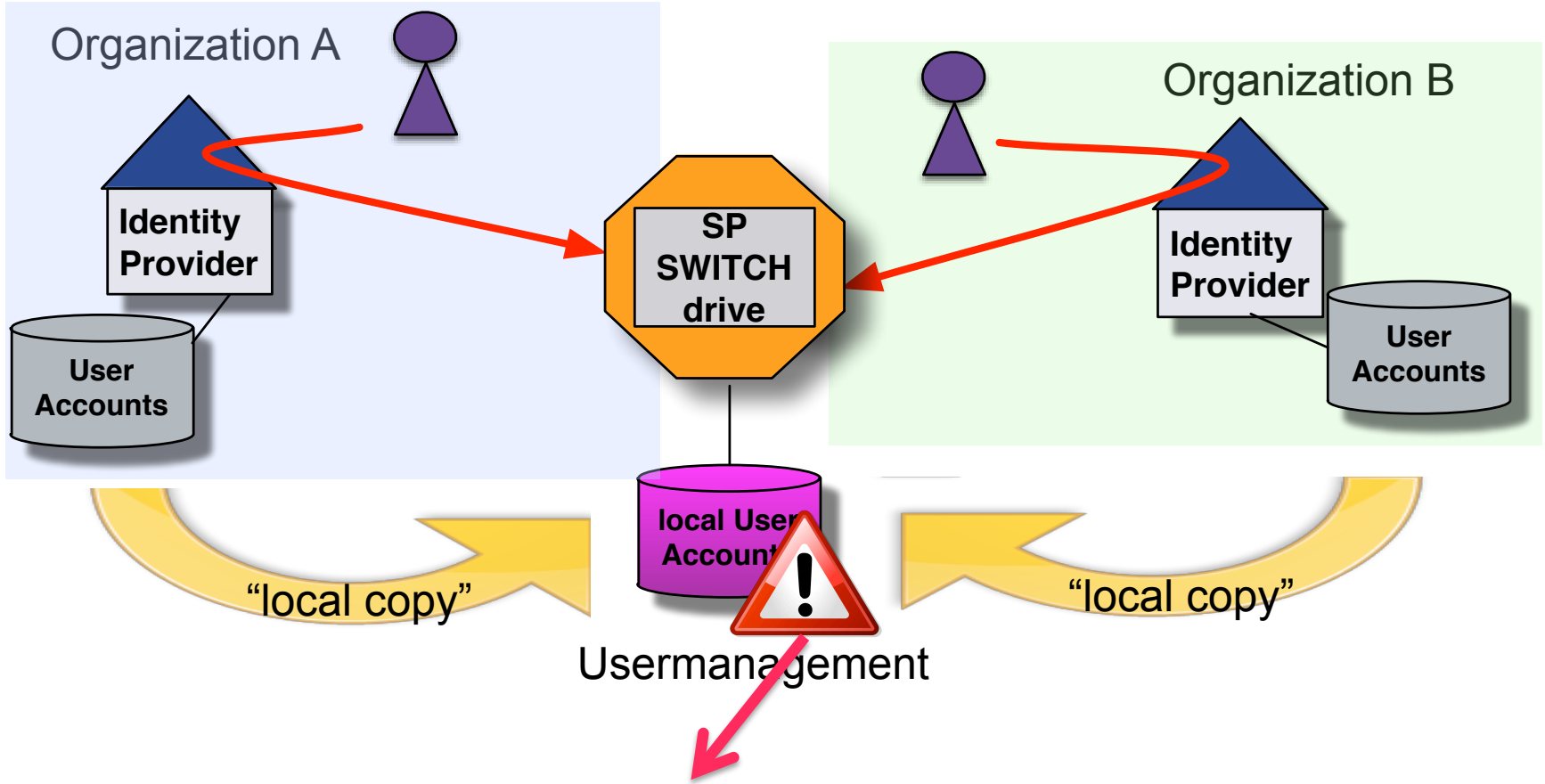
Based on SAML AttributeQuery

SWITCH

SWITCHaai Team
aai@switch.ch

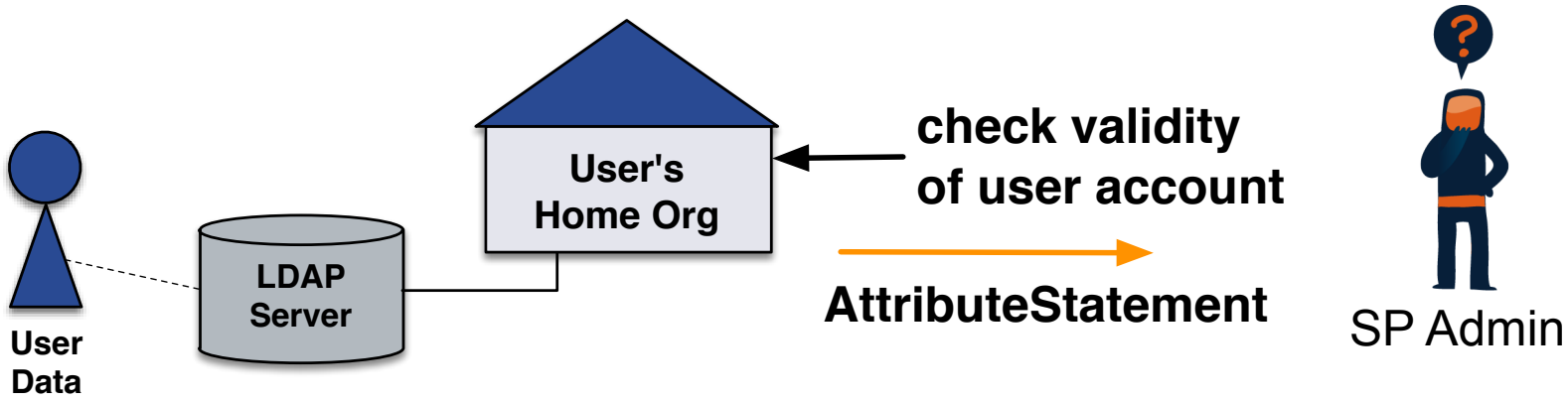
Berne, 13 August 2014

Why do account checking?



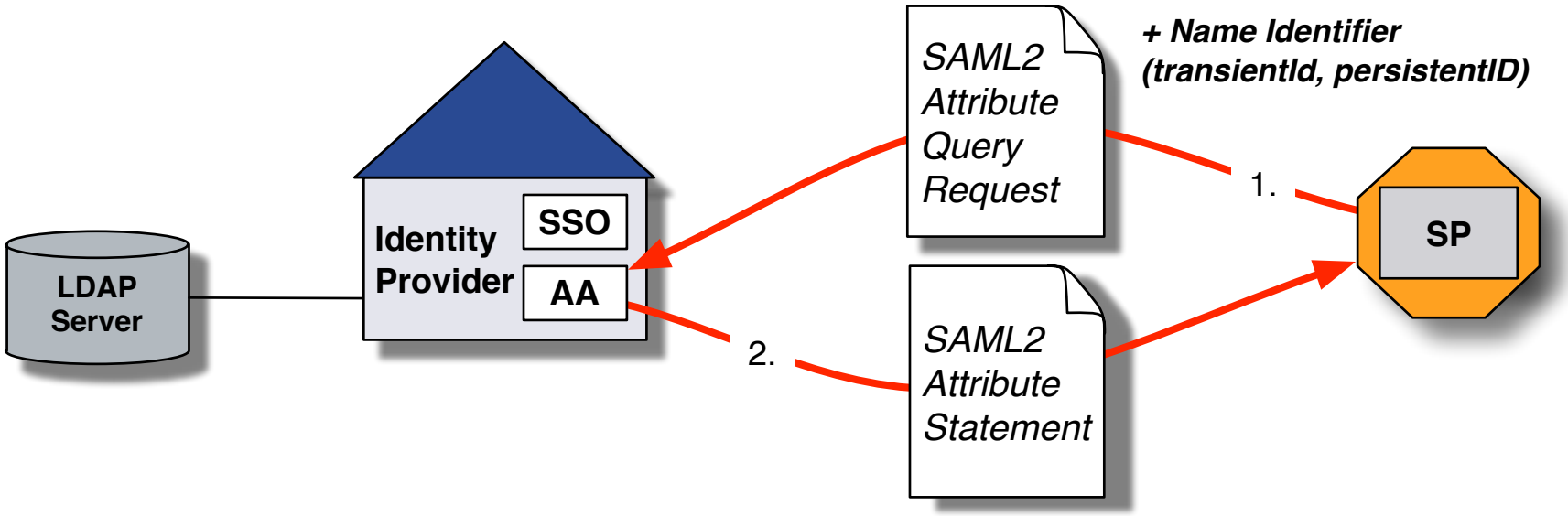
Idea

Validity of user account



- The SP sends an AttributeQuery to the IdP
- The SP receives an AttributeStatement from the IdP
- Process the result and do the “housekeeping” in your application

SAML Attribute Query



- Service Provider (SP) directly queries Attribute Authority (AA) of Identity Provider for user attributes using a NameId
- Usually transient or persistent NameID is used
- Shibboleth SP/IdP supports Attribute Queries

- All SWITCHaai IdPs support stored persistentIDs (persistentID stored in database that maps to the localID)

Persistent ID and Attribute Queries

Serialized Example of a persistentID:

https://aai-login.tw.switch.ch/idp/shibboleth!
https://testsp.tw. switch.ch/shibboleth!
jrdV9rog57INTKp9EB1vmyRfmgc=

localEntity	peerEntity	principalName	localId	persistentId	peerProvidedId	creationDate	deactivationDate
https://aai-login.tw.switch.ch/idp/shibboleth	https://aai-viewer.switch.ch/shibboleth	student1	2490257@example.org	dfF12dKDk1ymiJrn34NaLSsM8bw=	NULL	2013-07-23 15:13:22	NULL
https://aai-login.tw.switch.ch/idp/shibboleth	https://aai-demo.switch.ch/shibboleth	student2	8548997@example.org	ANS7jbdGduIMWCevMqHyKgqQqs4=	NULL	2013-07-23 15:52:45	NULL
https://aai-login.tw.switch.ch/idp/shibboleth	https://aai-viewer.switch.ch/shibboleth	student2	8548997@example.org	O1lODO/Ji5GfMQxEeHq6NZ6Mqx8=	NULL	2013-07-23 16:00:46	NULL
https://aai-login.tw.switch.ch/idp/shibboleth	https://rr.aai.switch.ch/shibboleth	student1	2490257@example.org	Jy1jI/XxpTK34NeMQ5VXFQ4U/Uw=	NULL	2013-08-05 09:28:19	NULL
https://aai-login.tw.switch.ch/idp/shibboleth	https://aai-demo.switch.ch/shibboleth	student1	2490257@example.org	SzPThGVlohQaXZerDcC2+FPw8AU=	NULL	2013-09-18 12:55:01	NULL
https://aai-login.tw.switch.ch/idp/shibboleth	https://testsp.tw.switch.ch/shibboleth	student1	2490257@example.org	hJMJb+/aqWYv1Tuj+IQylylqj2A=	NULL	2013-09-19 16:10:35	NULL
https://aai-login.tw.switch.ch/idp/shibboleth	https://aai-viewer.switch.ch/shibboleth	staff3	7622788@example.org	3oiPFq38oIyS4+h7J/VRwwAZTGI=	NULL	2014-01-06 11:24:36	NULL
https://aai-login.tw.switch.ch/idp/shibboleth	https://aai-demo.switch.ch/shibboleth	staff3	7622788@example.org	2m2ipfQvPCLfReyyl+bR3h9v3gU=	NULL	2014-01-06 11:25:01	NULL
https://aai-login.tw.switch.ch/idp/shibboleth	https://testsp.tw.switch.ch/shibboleth	student2	8548997@example.org	jrdV9rog57INTKp9EB1vmyRfmgc=	NULL	2014-01-30 08:50:28	NULL
https://aai-login.tw.switch.ch/idp/shibboleth	https://testsp.tw.switch.ch/shibboleth	staff3	7622788@example.org	YVlAKbj81gi5E+EF+f2rUS+2FGk=	NULL	2014-01-30 09:08:30	NULL
https://aai-login.tw.switch.ch/idp/shibboleth	https://attribute-viewer.aai.switch.ch/shibboleth	student1	2490257@example.org	bbVdShGObKqP0NJHYT6eSYwtNlA=	NULL	2014-06-13 16:32:34	NULL

11 rows in set (0.00 sec)

- Opaque
- Targeted: Same user has different persistentIDs for different services
- Once SP has user's persistentID, attributes can be queried at any time (without users involvement)

Requirements

- Shibboleth SP ≥ 2.5.0
- SP must use persistentID
- Requires attribute query extension by Japanese Federation GakuNin
  - requests the AttributeStatement based on user's identifier to an IdP and outputs the resulting attribute in JSON format.
  - Provides a handler to make fast Attribute Queries via web
  - Extension will be integrated on SP in the near future

Attribute Query with extension

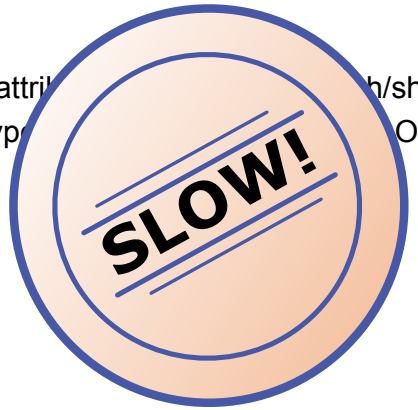
- curl -k 'https://localhost/Shibboleth.sso/AttributeQuery?entityID=https://aai-logon.switch.ch/idp/shibboleth&nameId=NRDnNTHBcKe4fwB7AG9p/psQG1o=’
- Result: JSON Object:


```
{
   "displayName" : "Thomas Weller",
   "postalAddress" : "SWITCH$Werdstrasse 2$CH-8004 Zürich",
   "telephoneNumber" : "+41 44 268 1550",
   "isMemberOf" : ”abc; x123, b312",
   "mail" : "thomas.weller@switch.ch",
   "persistent-id" : "https://aai-logon.switch.ch/idp/shibboleth!https://attribute-viewer.aai.switch.ch/shibboleth!P2HjBH……",
   "schacHomeOrganizationType" : "urn:schac:homeOrganizationType:ch:others;urn:schac:homeOrganizationType:int:nren",
   "gender" : "1",
   "dateOfBirth" : ”….",
   "cn" : "Thomas Weller",
   "homeOrganizationType" : "others",
   "uniqueID" : "74….@switch.ch",
   "homeOrganization" : "switch.ch",
   "schacHomeOrganization" : "switch.ch",
   "preferredLanguage" : "en",
   "givenName" : "Thomas",
   "surname" : "Weller",
   "scoped-affiliation" : "staff@switch.ch;member@switch.ch",
   "principalName" : "74…..@switch.ch",
   "affiliation" : "member;staff",
   "uid" : "weller"
}
```

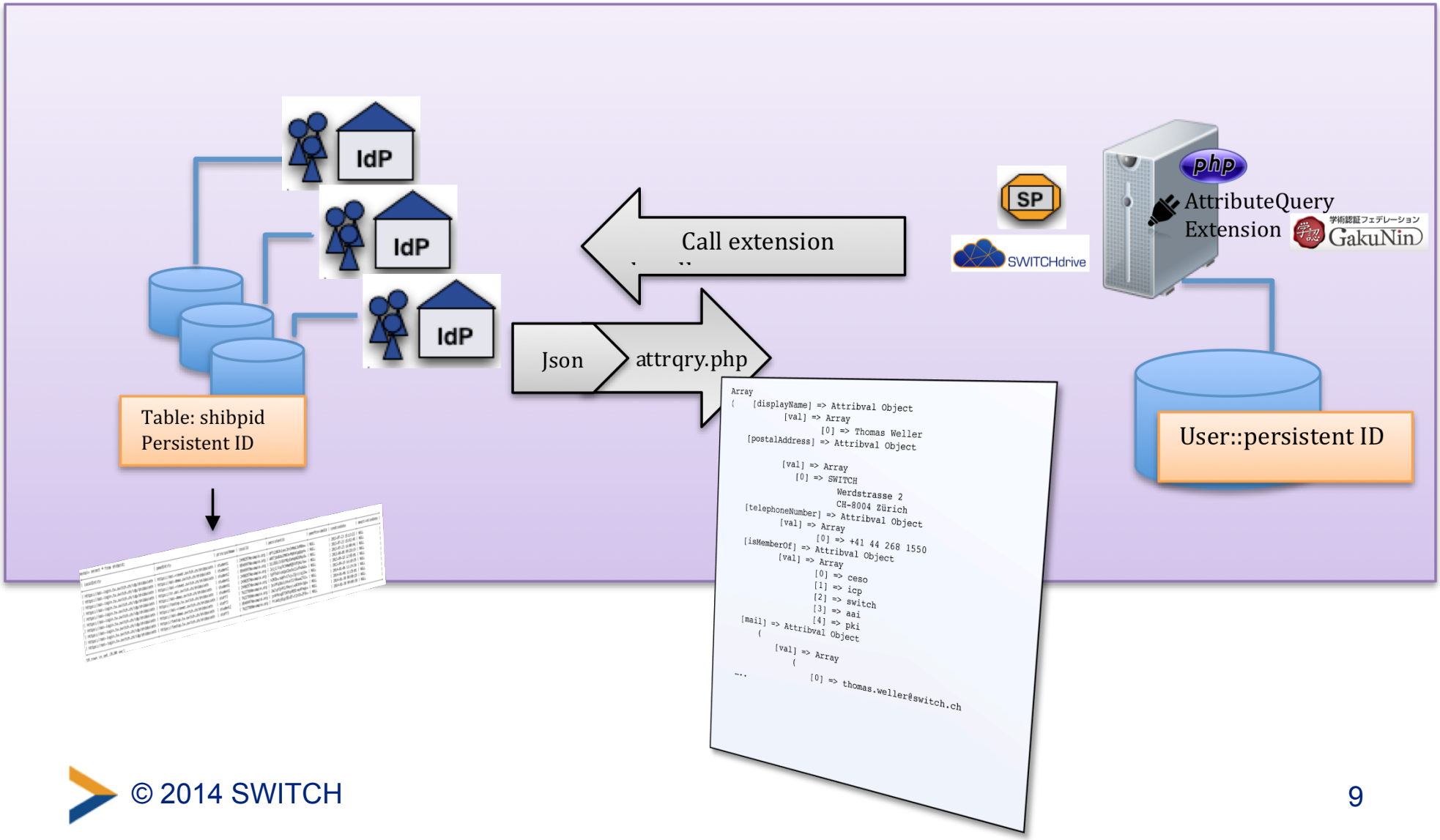
Attribute Query with resolvertest

- ./resolvertest -n PDg6jPP2HjBHuOFD4RFzb+2x+lM= -i https://aai-logon.switch.ch/idp/shibboleth -saml2 -f urn:oasis:names:tc:SAML:2.0:nameid-format:persistent

displayName: Thomas Weller
postalAddress: SWITCH$Werdstrasse 2$CH-8004 Zürich
telephoneNumber: +41 44 268 1550
isMemberOf: abc; x123, b312
mail: thomas.weller@switch.ch
persistent-id: https://aai-logon.switch.ch/idp/shibboleth!https://attri…h/shibboleth!PDg6jPP…..
schacHomeOrganizationType: urn:schac:homeOrganizationTyp…OrganizationType:int:nren
gender: 1
dateOfBirth:…..
cn: Thomas Weller
homeOrganizationType: others
uniqueID: 74….@switch.ch
homeOrganization: switch.ch
schacHomeOrganization: switch.ch
preferredLanguage: en
givenName: Thomas
surname: Weller
scoped-affiliation: staff@switch.ch;member@switch.ch



Implementation Idea for SWITCHdrive



Known issues

- wrong or persistentID does not exist
- User on LDAP does not or no longer exist

⇒ return of defined staticAttributes or / and Default values (IdP attribute-resolver) e.g.:

- uApprove: attribute consent set to “not released”

  ⇒ Attribute query plugin delivers always attributes

- User is not deleted in LDAP and has no login

⇒ Attribute query plugin delivers the attributes

- SP is responsible for ensuring that the IdP is not overloaded

Deployment and effort required

- Sources Attribute Query handler:
  - https://wiki.shibboleth.net/confluence/display/SHIB2/Contributions#Contributions-ServiceProviderExtensions
- Installation and first tests
  - ~ ½ - 1 day

If you are interested to deploy, get in contact with SWITCHaai: aai@switch.ch

Additional links

- AAI for mobile apps
  - https://www.switch.ch/aai/support/tools/aai-for-apps.html
- Documentation resolvertest
  - https://wiki.shibboleth.net/confluence/display/SHIB2/NativeSPresolvertest

Comments and summary

- AttributeQuery: approach to keep user accounts “clean”

- SP Admin: “Which approach for the solution?”
  - Resolvertest vs. attribute query handler (< 20 queries and synchronization ≥ 6 months)
  - costs and benefits should be balanced:
    - How many users
    - frequency of “synchronization”
    - further processing of return values