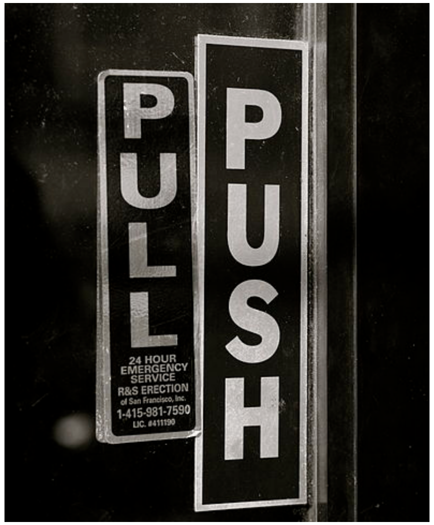
SAML Attribute Query

Pulling attributes from an IdP



SWITCH

Lukas Hämmerle
lukas.haemmerle@switch.ch

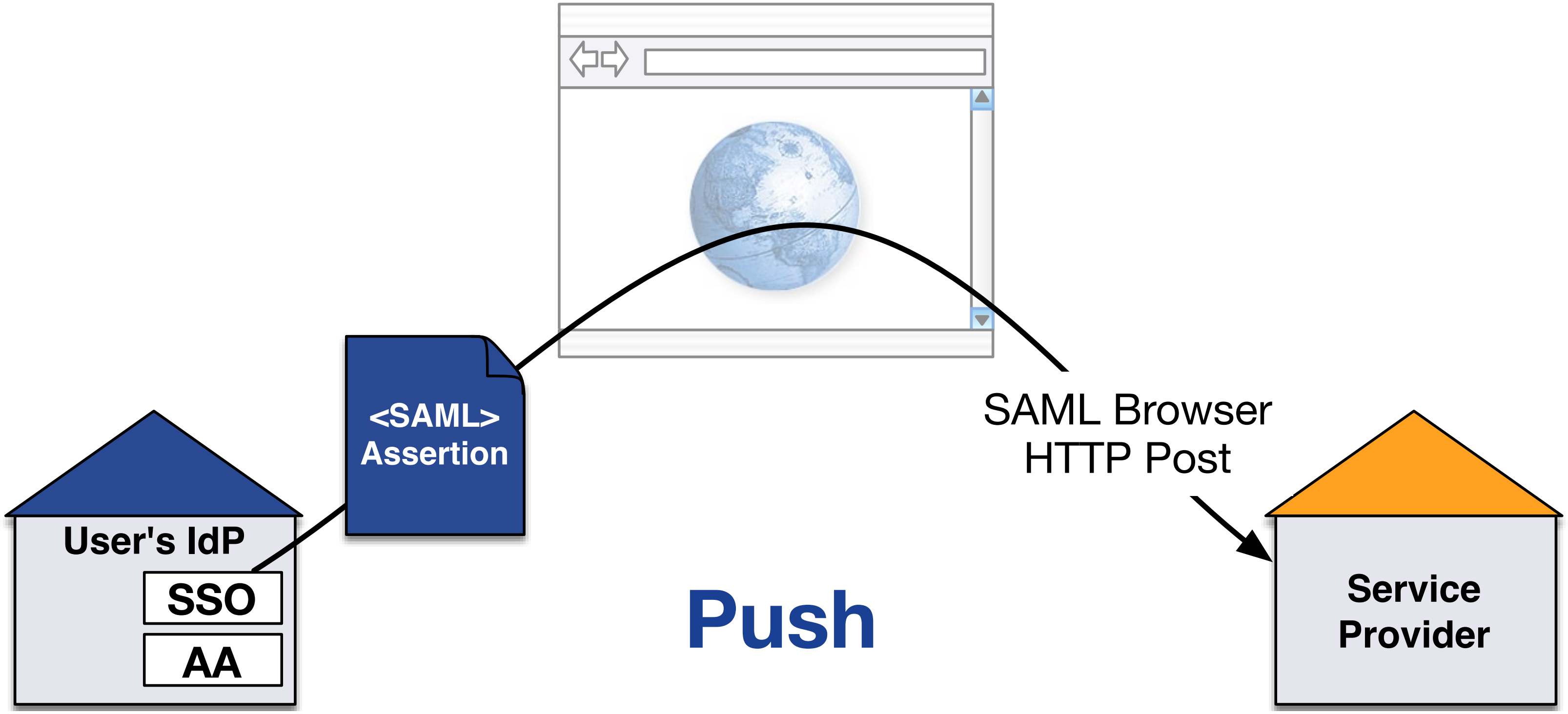
Berne, 30. June 2016

SAML Attribute Query

- What is it?
- For what is it useful?
- How to use it?
- How can my IdP support it?

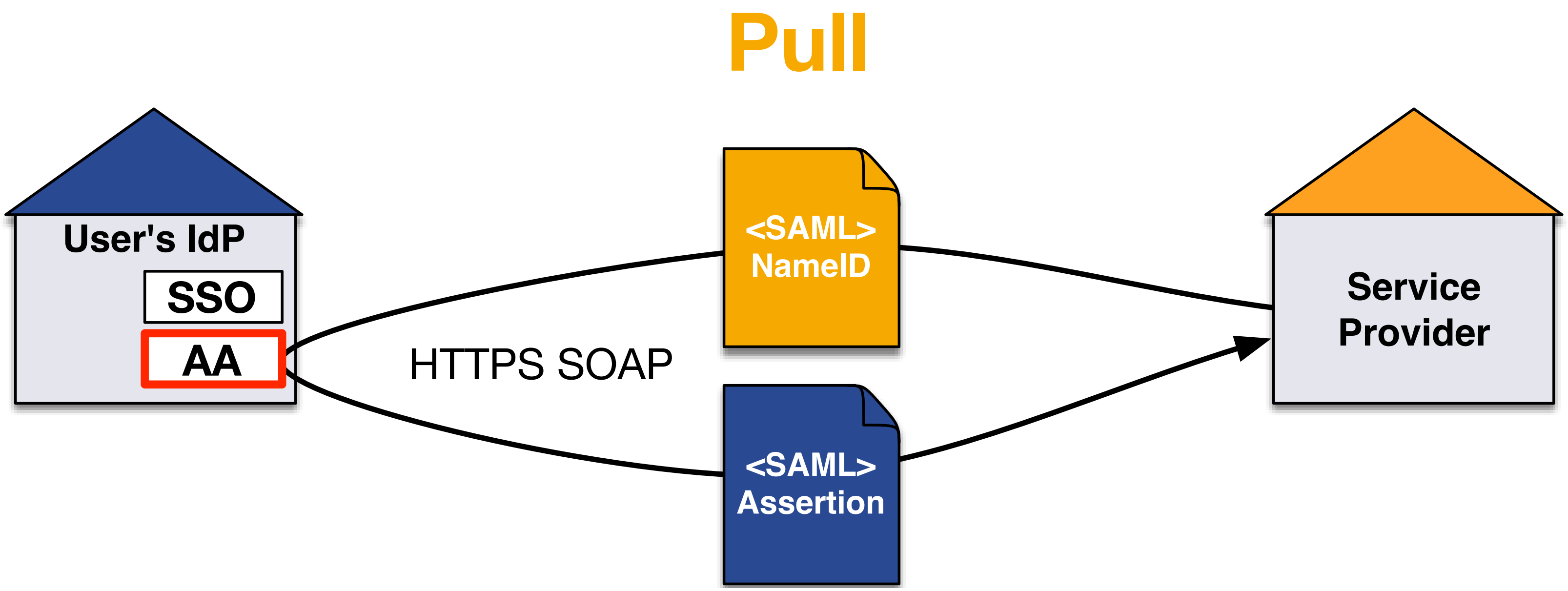
Attribute Query in greater detail:
https://www.switch.ch/aai/support/presentations/techupdate-2014/04_Account_Checking.pdf

Normal AAI Login



- Assertion sent via web browser to SP
- Requires user and his web browser

SAML Attribute Query



- SP queries IdP Attribute Authority (AA) asking for assertion
- SAML PersistentID/eduPersonTargetedID needed by SP
- No user involvement or web browser needed

So why are Attribute Queries useful?

Get **up-to-date** user **attributes** at any time **without user involvement** from IdP!

- Only possible if user at least once accessed SP (and gave consent to release attributes to this SP)
- Update user account data on request
- Detect if user still has an account at IdP
  (no personal attributes probably means no account anymore)
- Easy to use:

  ```
  curl -k 'https://localhost/Shibboleth.sso/AttributeQuery?
  entityID=#IdP#&nameId=#PersistentID#'
  ```

  ➔ Attributes as JSON data

- Needed for **Swiss edu-ID** to keep user data up-to-date!

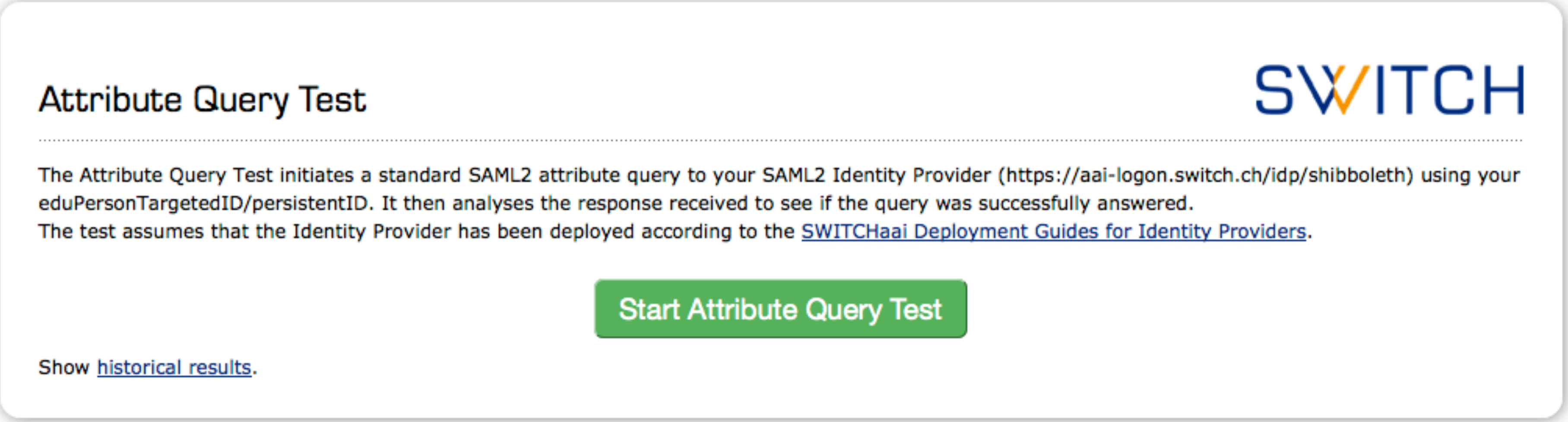
How to Perform an Attribute Query

- Shibboleth SP `resolvertest` binary
  - Bundled since Shibboleth SP 2.x
  - Slow and only for testing
  - Non standard form for returning attributes
  - Usage information in Shibboleth Wiki

- Shibboleth Attribute Query Plugin
  - Was plug-in but is now bundled with SP 2.6 (**released yesterday!**)
  - Developed by Japanese GakuNin federation
  - Very fast!
  - Accessible via URL (`/Shibboleth.sso/AttributeQuery?nameID=XY`)

Does it work for my IdP?

- Yes, it should if you used the SWITCHaai IdP guides!
- Test it: https://av.aai.switch.ch/aai/attribute-query-test/

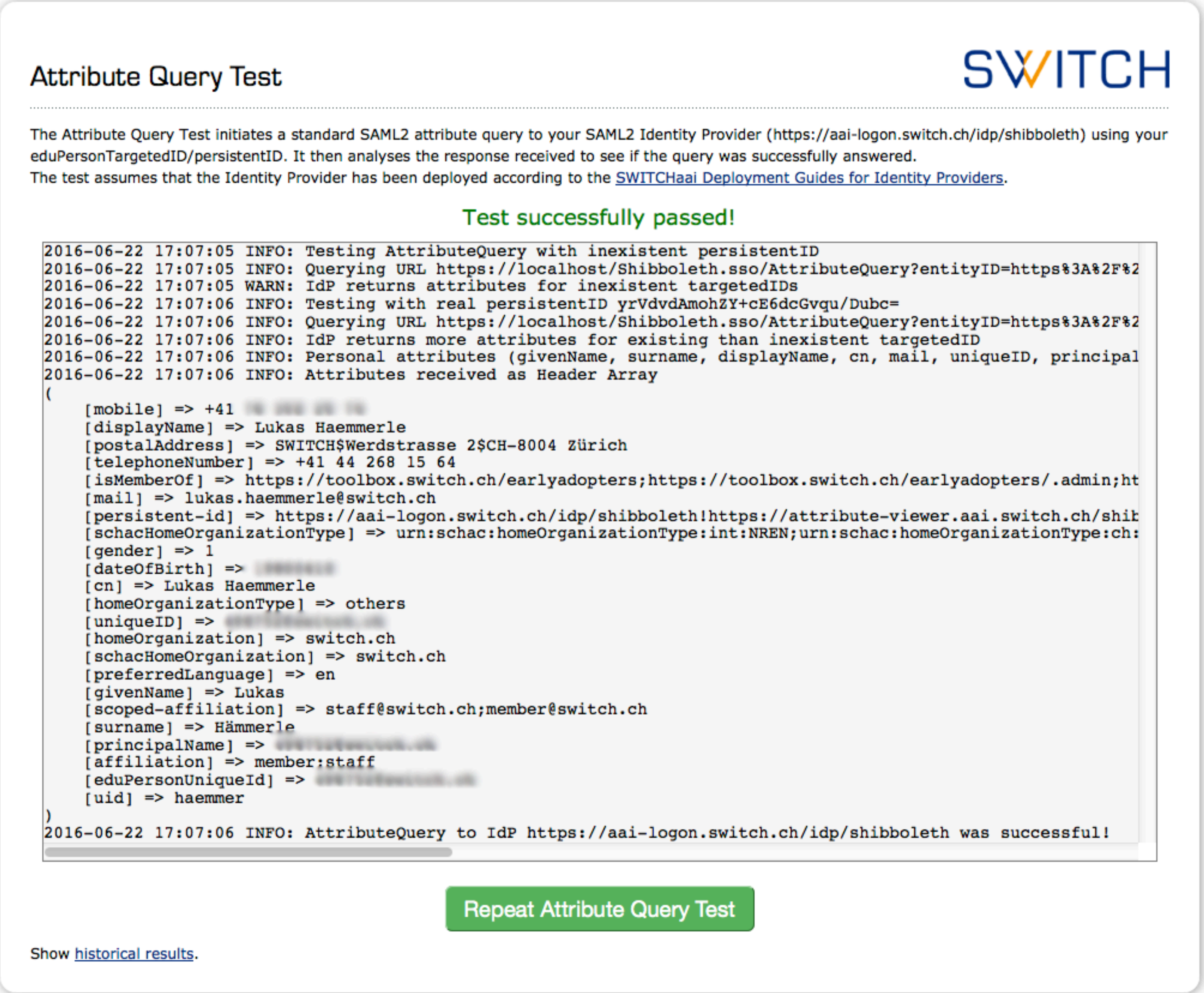


Attribute Query Test

The Attribute Query Test initiates a standard SAML2 attribute query to your SAML2 Identity Provider (https://aai-logon.switch.ch/idp/shibboleth) using your eduPersonTargetedID/persistentID. It then analyses the response received to see if the query was successfully answered.
The test assumes that the Identity Provider has been deployed according to the SWITCHaai Deployment Guides for Identity Providers.

Show historical results.

- 31 (49%) of 63 IdPs successfully took the the test (29.6.2016)



Attribute Query Test

The Attribute Query Test initiates a standard SAML2 attribute query to your SAML2 Identity Provider (https://aai-logon.switch.ch/idp/shibboleth) using your eduPersonTargetedID/persistentID. It then analyses the response received to see if the query was successfully answered.
The test assumes that the Identity Provider has been deployed according to the SWITCHaai Deployment Guides for Identity Providers.

Test successfully passed!

```
2016-06-22 17:07:05 INFO: Testing AttributeQuery with inexistent persistentID
2016-06-22 17:07:05 INFO: Querying URL https://localhost/Shibboleth.sso/AttributeQuery?entityID=https%3A%2F%2
2016-06-22 17:07:05 WARN: IdP returns attributes for inexistent targetedIDs
2016-06-22 17:07:06 INFO: Testing with real persistentID yrVdvdAmohZY+cE6dcGvqu/Dubc=
2016-06-22 17:07:06 INFO: Querying URL https://localhost/Shibboleth.sso/AttributeQuery?entityID=https%3A%2F%2
2016-06-22 17:07:06 INFO: IdP returns more attributes for existing than inexistent targetedID
2016-06-22 17:07:06 INFO: Personal attributes (givenName, surname, displayName, cn, mail, uniqueID, principal
2016-06-22 17:07:06 INFO: Attributes received as Header Array
(
    [mobile] => +41 [redacted]
    [displayName] => Lukas Haemmerle
    [postalAddress] => SWITCH$Werdstrasse 2$CH-8004 Zürich
    [telephoneNumber] => +41 44 268 15 64
    [isMemberOf] => https://toolbox.switch.ch/earlyadopters;https://toolbox.switch.ch/earlyadopters/.admin;ht
    [mail] => lukas.haemmerle@switch.ch
    [persistent-id] => https://aai-logon.switch.ch/idp/shibboleth!https://attribute-viewer.aai.switch.ch/shib
    [schacHomeOrganizationType] => urn:schac:homeOrganizationType:int:NREN;urn:schac:homeOrganizationType:ch:
    [gender] => 1
    [dateOfBirth] => [redacted]
    [cn] => Lukas Haemmerle
    [homeOrganizationType] => others
    [uniqueID] => [redacted]
    [homeOrganization] => switch.ch
    [schacHomeOrganization] => switch.ch
    [preferredLanguage] => en
    [givenName] => Lukas
    [scoped-affiliation] => staff@switch.ch;member@switch.ch
    [surname] => Hämmerle
    [principalName] => [redacted]
    [affiliation] => member;staff
    [eduPersonUniqueId] => [redacted]
    [uid] => haemmer
)
2016-06-22 17:07:06 INFO: AttributeQuery to IdP https://aai-logon.switch.ch/idp/shibboleth was successful!
```

Show historical results.