Account Checking on a SP
Based on SAML AttributeQuery

Berne, 13 August 2014

SWITCHaai Team
aai@switch.ch
Why do account checking?

user data might be outdated
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 persistentID (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=

<table>
<thead>
<tr>
<th>Local Entity</th>
<th>Peer Entity</th>
<th>PrincipalName</th>
<th>localId</th>
<th>persistentId</th>
<th>peerProvidedId</th>
<th>creationDate</th>
<th>deactivationDate</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="https://aai-login.tw.switch.ch/idp/shibboleth">https://aai-login.tw.switch.ch/idp/shibboleth</a></td>
<td><a href="https://aai-viewer.switch.ch/shibboleth">https://aai-viewer.switch.ch/shibboleth</a></td>
<td>student1</td>
<td><a href="mailto:24082570@casper.o.com">24082570@casper.o.com</a></td>
<td>cFFFa2b4lXy90LZv39n3a9x3fBHc+</td>
<td>NULL</td>
<td>2013-07-23 15:13:32</td>
<td>NULL</td>
</tr>
<tr>
<td><a href="https://aai-login.tw.switch.ch/idp/shibboleth">https://aai-login.tw.switch.ch/idp/shibboleth</a></td>
<td><a href="https://aai-viewer.switch.ch/shibboleth">https://aai-viewer.switch.ch/shibboleth</a></td>
<td>student1</td>
<td><a href="mailto:24082570@casper.o.com">24082570@casper.o.com</a></td>
<td>dY12Rg9v3H4KIV76K9Ug8t4+</td>
<td>NULL</td>
<td>2013-07-23 15:08:44</td>
<td>NULL</td>
</tr>
<tr>
<td><a href="https://aai-login.tw.switch.ch/idp/shibboleth">https://aai-login.tw.switch.ch/idp/shibboleth</a></td>
<td><a href="https://aai-viewer.switch.ch/shibboleth">https://aai-viewer.switch.ch/shibboleth</a></td>
<td>student1</td>
<td><a href="mailto:24082570@casper.o.com">24082570@casper.o.com</a></td>
<td>e9Fh003bH93Gv09cG64vUg8t4+</td>
<td>NULL</td>
<td>2013-07-23 12:58:19</td>
<td>NULL</td>
</tr>
<tr>
<td><a href="https://aai-login.tw.switch.ch/idp/shibboleth">https://aai-login.tw.switch.ch/idp/shibboleth</a></td>
<td><a href="https://testsp.tw.switch.ch/shibboleth">https://testsp.tw.switch.ch/shibboleth</a></td>
<td>student1</td>
<td><a href="mailto:24082570@casper.o.com">24082570@casper.o.com</a></td>
<td>h11v8+x9pH7iC7t9+J/iy+ig8t4+</td>
<td>NULL</td>
<td>2013-09-19 16:10:13</td>
<td>NULL</td>
</tr>
<tr>
<td><a href="https://aai-login.tw.switch.ch/idp/shibboleth">https://aai-login.tw.switch.ch/idp/shibboleth</a></td>
<td><a href="https://testsp.tw.switch.ch/shibboleth">https://testsp.tw.switch.ch/shibboleth</a></td>
<td>staff1</td>
<td><a href="mailto:5627898@casper.o.com">5627898@casper.o.com</a></td>
<td>3yiHFg9v3H4KIV76K9Ug8t4+</td>
<td>NULL</td>
<td>2013-04-01 11:24:36</td>
<td>NULL</td>
</tr>
<tr>
<td><a href="https://aai-login.tw.switch.ch/idp/shibboleth">https://aai-login.tw.switch.ch/idp/shibboleth</a></td>
<td><a href="https://testsp.tw.switch.ch/shibboleth">https://testsp.tw.switch.ch/shibboleth</a></td>
<td>staff1</td>
<td><a href="mailto:5627898@casper.o.com">5627898@casper.o.com</a></td>
<td>d21g0F9v3H4KIV76K9Ug8t4+</td>
<td>NULL</td>
<td>2013-01-04 11:28:15</td>
<td>NULL</td>
</tr>
<tr>
<td><a href="https://aai-login.tw.switch.ch/idp/shibboleth">https://aai-login.tw.switch.ch/idp/shibboleth</a></td>
<td><a href="https://testsp.tw.switch.ch/shibboleth">https://testsp.tw.switch.ch/shibboleth</a></td>
<td>student1</td>
<td><a href="mailto:24082570@casper.o.com">24082570@casper.o.com</a></td>
<td>bHl6h9b003bH93Gv09cG64vUg8t4+</td>
<td>NULL</td>
<td>2013-01-30 09:06:38</td>
<td>NULL</td>
</tr>
<tr>
<td><a href="https://aai-login.tw.switch.ch/idp/shibboleth">https://aai-login.tw.switch.ch/idp/shibboleth</a></td>
<td><a href="https://testsp.tw.switch.ch/shibboleth">https://testsp.tw.switch.ch/shibboleth</a></td>
<td>student1</td>
<td><a href="mailto:24082570@casper.o.com">24082570@casper.o.com</a></td>
<td>bHl6h9b003bH93Gv09cG64vUg8t4+</td>
<td>NULL</td>
<td>2013-01-30 15:10:34</td>
<td>NULL</td>
</tr>
</tbody>
</table>

- **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:

```json
{
"displayName" : "Thomas Weller",
"postalAddress" : "SWITCH$Werdstrasse 2$CH-8004 Zürich",
"telephoneNumber" : "+41 44 268 1550",
"isMemberOf" : "abc; x123, b312",
"mail" : "thomas.weller@switch.ch",
"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


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!PDg6jPP.....
schacHomeOrganizationType: 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
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