SAML2 Persistent-ID

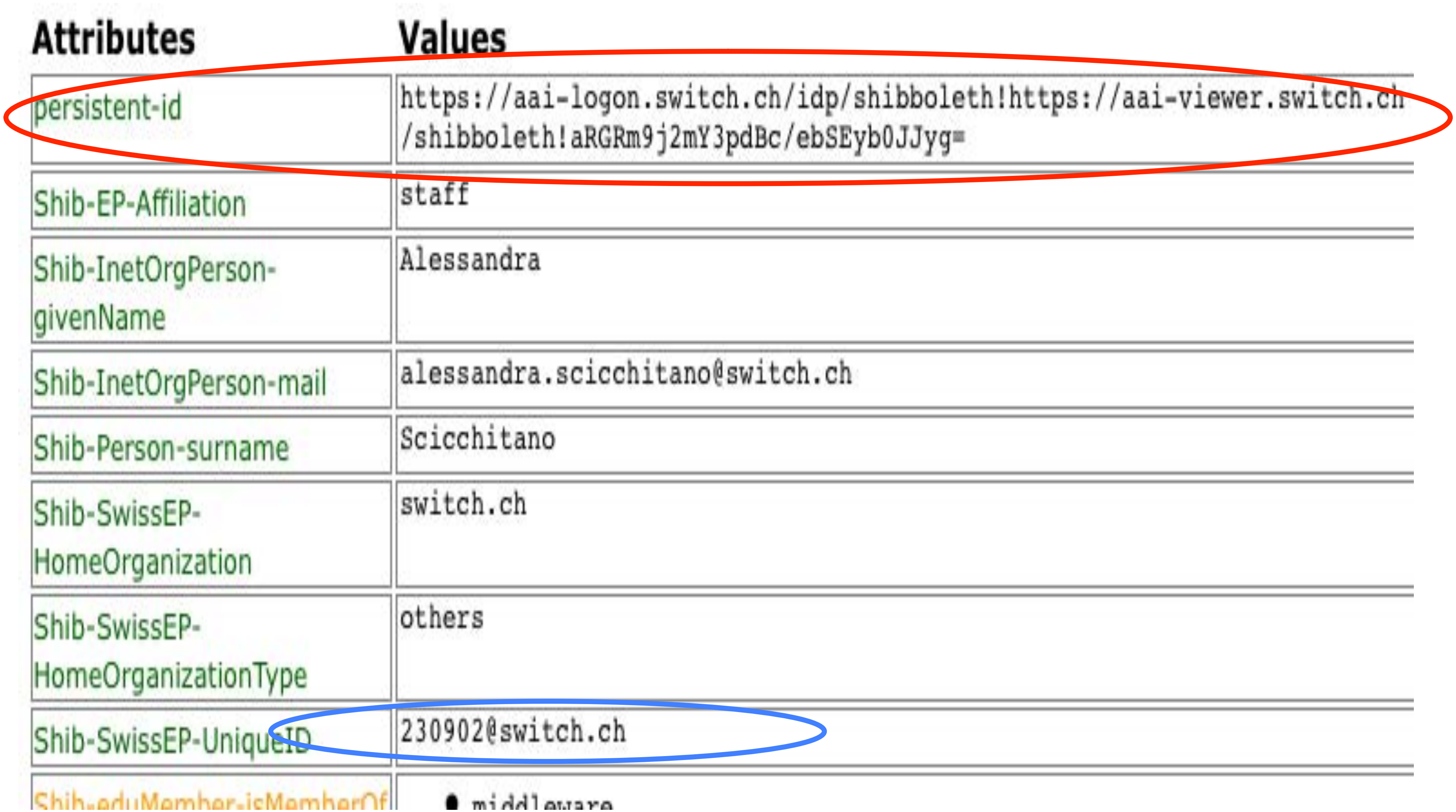
Why to use it? How to use it?

SWITCH
Serving Swiss Universities

Alessandra Scicchitano
alessandra.scicchitano@switch.ch

Bern, 24 May 2011

…but what are we talking about???



Attributes	Values
persistent-id	https://aai-logon.switch.ch/idp/shibboleth!https://aai-viewer.switch.ch /shibboleth!aRGRm9j2mY3pdBc/ebSEyb0JJyg=
Shib-EP-Affiliation	staff
Shib-InetOrgPerson-givenName	Alessandra
Shib-InetOrgPerson-mail	alessandra.scicchitano@switch.ch
Shib-Person-surname	Scicchitano
Shib-SwissEP-HomeOrganization	switch.ch
Shib-SwissEP-HomeOrganizationType	others
Shib-SwissEP-UniqueID	230902@switch.ch
Shib-eduMember-isMemberOf	● middleware

Why to use it?

Two very good reasons:

- **Privacy**

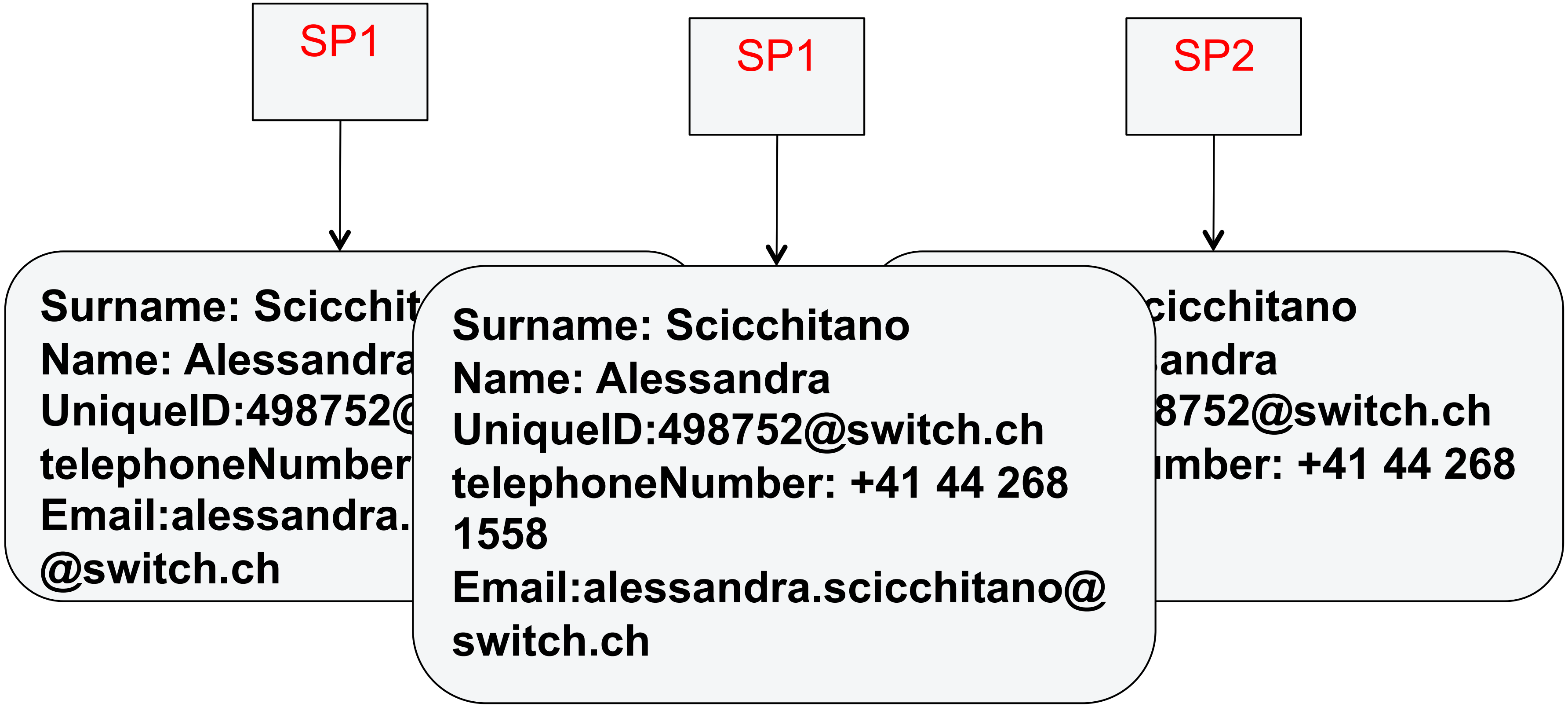
  It helps to better protect all users' information.

- **Account checking**

  It helps to check faster whether an account is still active or not.

Privacy

Why is it so unsafe to have an id that doesn't change?



SP1

Surname: Scicchit
Name: Alessandra
UniqueID:498752@
telephoneNumber
Email:alessandra.
@switch.ch

SP1

Surname: Scicchitano
Name: Alessandra
UniqueID:498752@switch.ch
telephoneNumber: +41 44 268
1558
Email:alessandra.scicchitano@
switch.ch

SP2

cicchitano
andra
8752@switch.ch
umber: +41 44 268

Account Checking

What do you do when SPs store accounts of users that don’t exist anymore? Or their info is old and needs to be updated?

Basically….nothing!

No way to find out whether the user still exists or whether his info is old.

……. and

How to use it????

Privacy

- **Example PersistentID**

It changes based on IdP and SP and user.

For different connections, different persistentIDs are generated.

https://idp.example.org/idp/shibboleth!https://sp.example.org/shibboleth!f74698d6-854c-480c-b566-702006318cc3c

Account Checking

Resolvertest Binary

A feature that is part of the SP (from 2.2 on) and allows to query the IdP based on the persistentID.

```
./resolvertest -saml2 \
-f urn:oasis:names:tc:SAML:2.0:nameid \
 format:persistent \
-n 26662bf3-f15e-418e-89f4-467788ff650b \
-i https://aai-logon.switch.ch/idp/shibboleth
```

....but

In order to use it, we first need to have it!

- IdPs must release the persistentID.

- On the other hand, SPs need to be changed in order to collect the persistentIDs.

PersistentID= PersistentNameID= TargetedID

We have referred so far to the PersistentID in a general way.

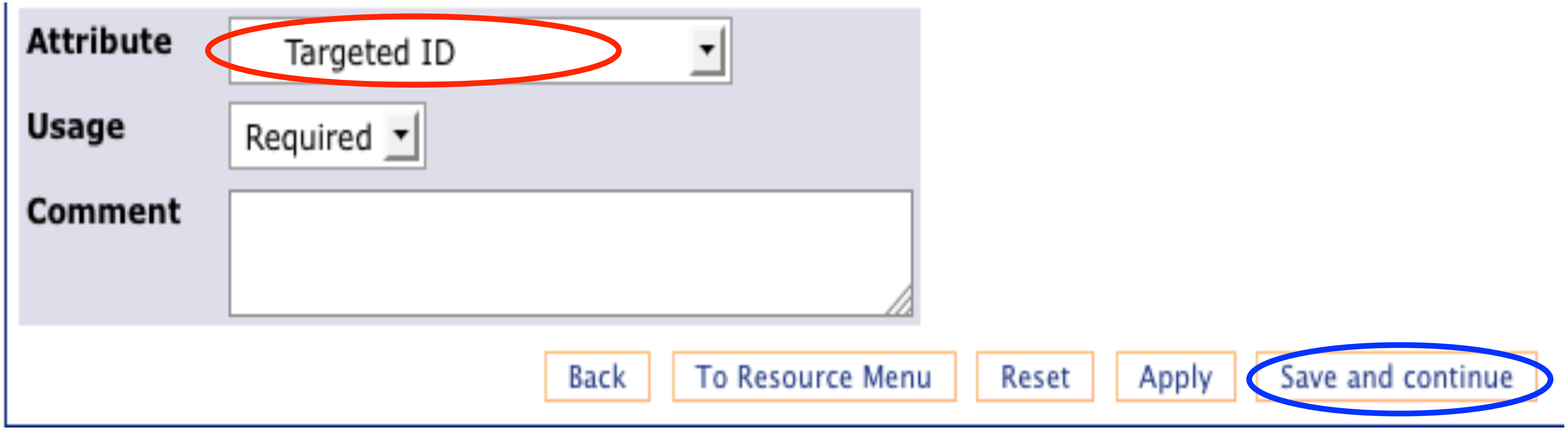
But to be more precise the PersistentID is two things in the SAML 2.0 assertion:

- A persistent NameID which appears in the <Subject>;
- An attribute called “eduPersonTargetedID”.

Sending both is the recommended way in the wiki.shibboleth.net

Change in the RR (case SP)

- In the RR, it is necessary to modify the list of Required Attributes



Attribute: Targeted ID

Usage: Required

Comment:

Changes in the SP

- 2. Two possible way to collect:

- Database (RR)
- or file (Wiki)

The length of the persistentID is not fixed and in theory can be huge, up to 1024 characters but this never really happens.

persistentId VARCHAR(256) NOT NULL

Transition Time

Before you can use the applications involving the persistentID, you have to consider a period of time needed to collect all persistentIDs.

This period of time can be short or long, based also on how many IDs you need to collect.

For the future SP, it would be an advantage to start collecting the persistentIDs straight from the beginning.

Conclusion

- Why to use it?

  Privacy and account checking

- How to use it?

  Protecting ad updating user's info and remove not anymore used accounts

The sooner you will start collecting the better it will be!