What happens...
...when a current affiliation ends?

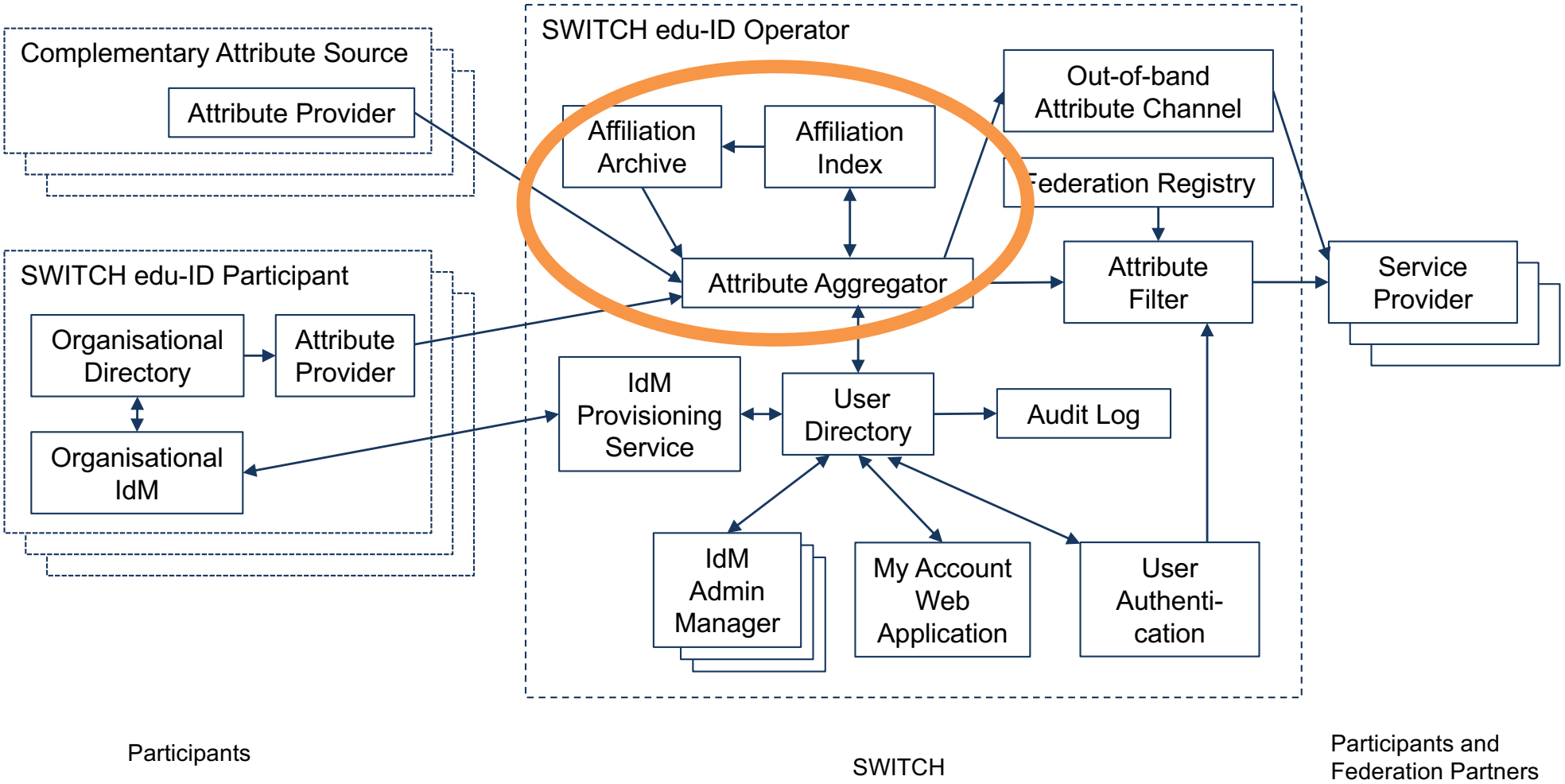
SWITCH

Etienne Dysli-Metref
etienne.dysli-metref@switch.ch

Bern, 14.03.2018

What is an affiliation?

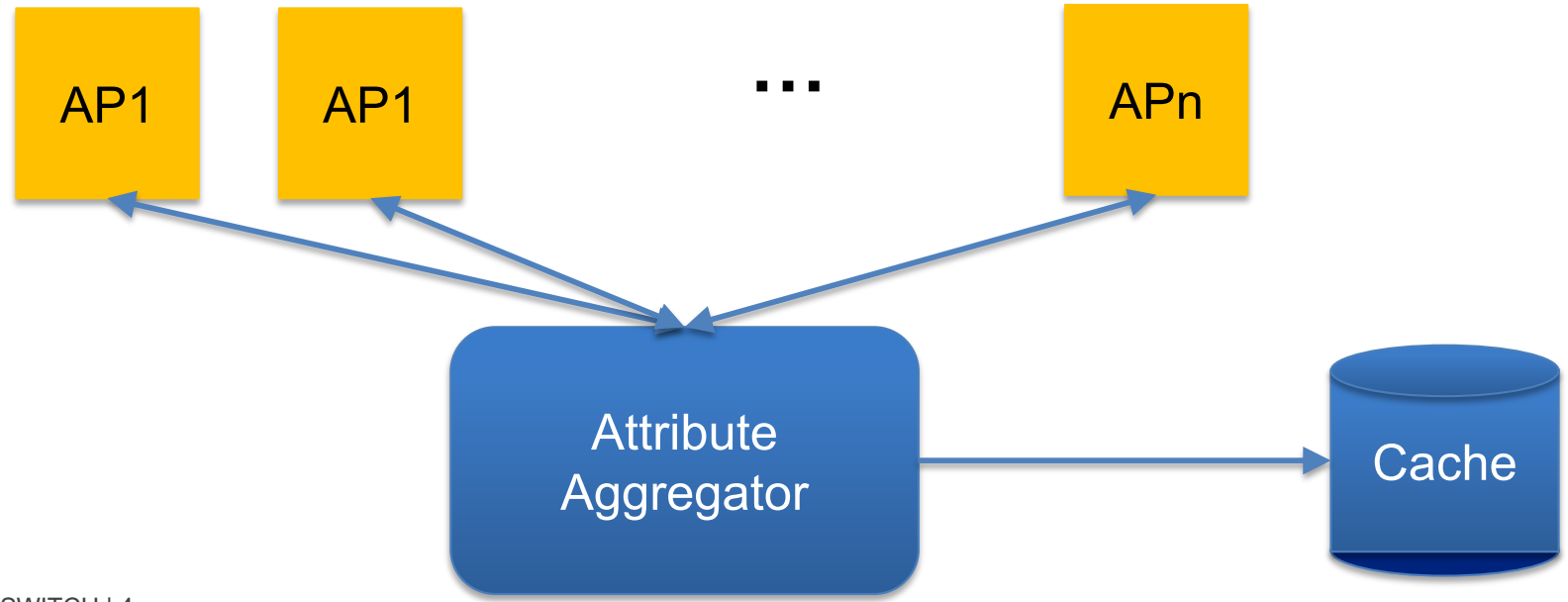
- Role held by an end user associated with an organisation in the SWITCHaai Federation.
- Created by linking a *base identity* with the organisation-related identity of the user.
- A base identity can be linked with none, one or multiple affiliations.
- An existing affiliation is described as a *current affiliation*; a previous, no longer active, affiliation is described as a *former affiliation*.


Complementary Attribute Source
Attribute Provider
SWITCH edu-ID Participant
Organisational Directory
Attribute Provider
Organisational IdM
SWITCH edu-ID Operator
Affiliation Archive
Affiliation Index
Out-of-band Attribute Channel
Federation Registry
Attribute Aggregator
Attribute Filter
Service Provider
IdM Provisioning Service
User Directory
Audit Log
IdM Admin Manager
My Account Web Application
User Authenti-cation
Participants
SWITCH
Participants and Federation Partners

Attribute aggregator

The attribute aggregator is a *cron job*

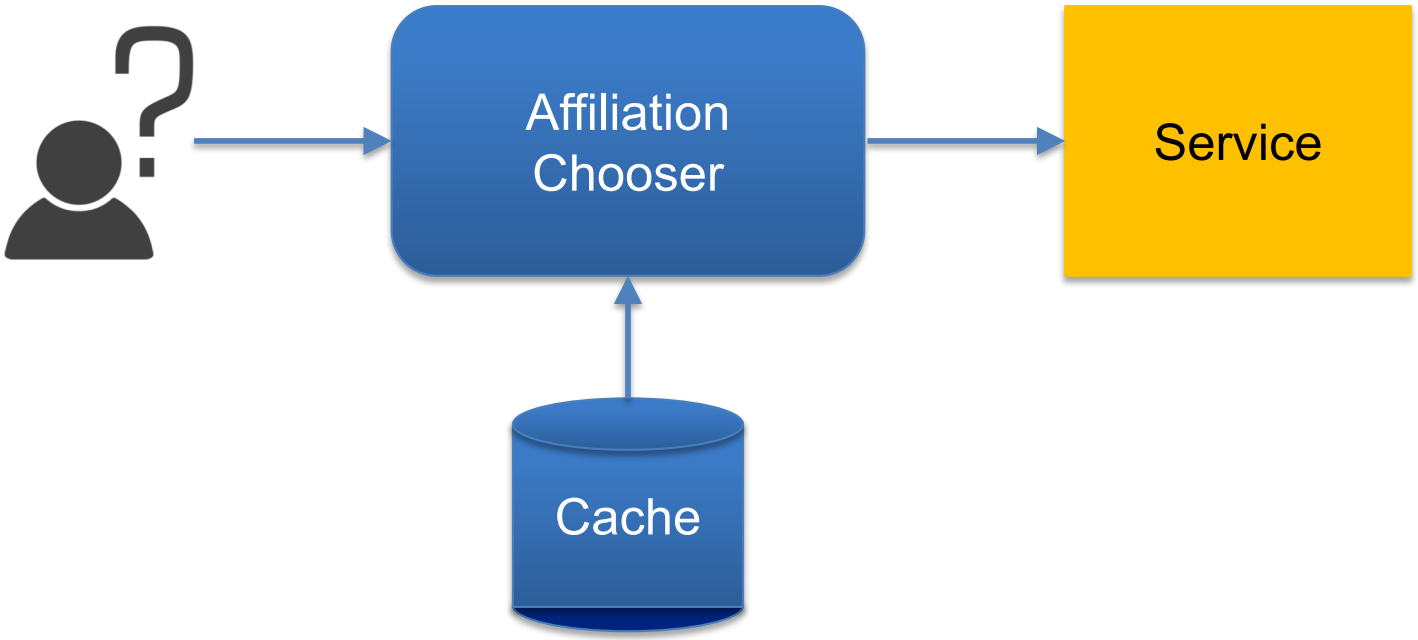
- Queries all attribute providers (your IdPs) for current affiliations.
- Uses the edu-ID SP as intermediary to query IdPs.
- For this, it needs an identifier, obtained when the account was linked (persistent ID).



Attribute aggregator

The attribute aggregator is a *cache*

- Affiliations are stored in the SWITCH edu-ID system.
- Allows the edu-ID IdP to take over the role of the institutional IdP and present the user, at login time, with a choice of affiliations.



Current and former affiliations

An affiliation ceases to be current when either:

- the attribute aggregator no longer receives attributes for a given user, or
- a migrated organisation notifies the edu-ID system (not implemented yet).

What does the SWITCH edu-ID system do with the affiliation data when it ceases to be current?

- Today: nothing happens
- Tag it as *former affiliation* (not implemented yet)

Attribute aggregator, under the hood

- Makes a SAML attribute query for all persistent IDs linked with each edu-ID account, ~40k queries in 4 hours.
- Going through the SP saves a lot in SAML implementation and processing but hides errors happening between SP and IdP.
- If attributes are received, then the affiliation is updated with new values. The affiliation stays *current*.
- If no attributes are received several times (days) in a row, the affiliation expires (not implemented yet).

Expiration of an affiliation

1. The affiliation is removed from the edu-ID account and stored in the *former affiliations* space. The edu-ID IdP will no longer send attributes related to this affiliation to SPs, nor offer it as a choice upon login.
2. SPs which have subscribed to affiliation changes are notified (not implemented yet). For example: SWITCHdrive, SWITCHengines, SPs in SWITCHaai.
3. SPs which have not subscribed will notice the affiliation change when the set of attributes they receive changes (upon next login or with an attribute query).

Preparation and next steps

For IdP Administrators

- After the SWITCH edu-ID adoption your IdP might remain and will in that case be called an *Attribute Provider* and you will be called *AP Administrator*.
- Make sure the SAML2 attribute query endpoint of your IdP is correctly published in the Resource Registry.
- Make sure your firewall and/or ACLs allow access to this endpoint from the edu-ID SP.
- Make sure your IdP's attribute filter allows releasing attributes to the edu-ID SP.
- [optional but recommended] Configure HomeOrganisation and HomeOrganisationType attributes with a Static DataConnector so that they are always released.