

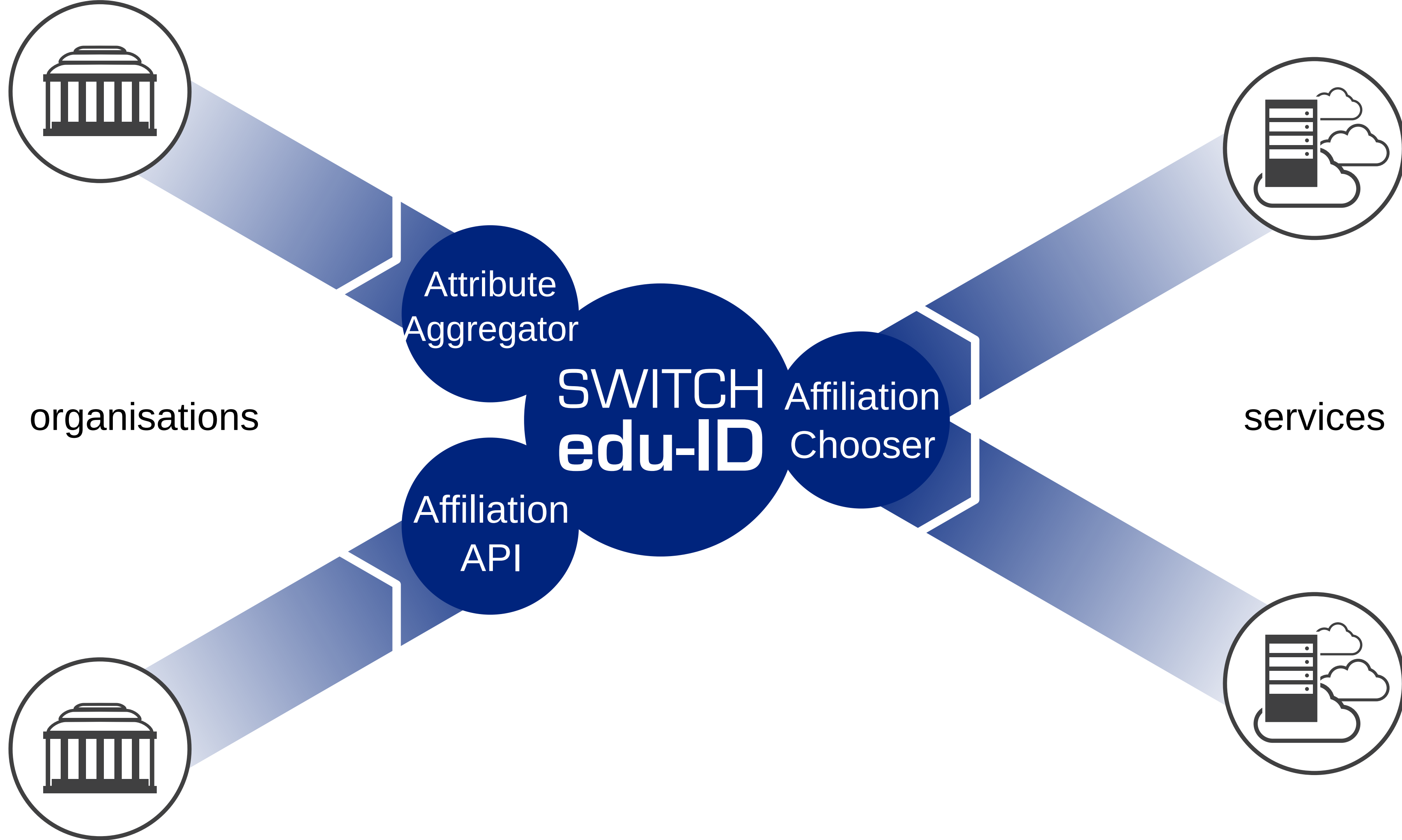
# SWITCH edu-ID

## How to spoof Identity Providers

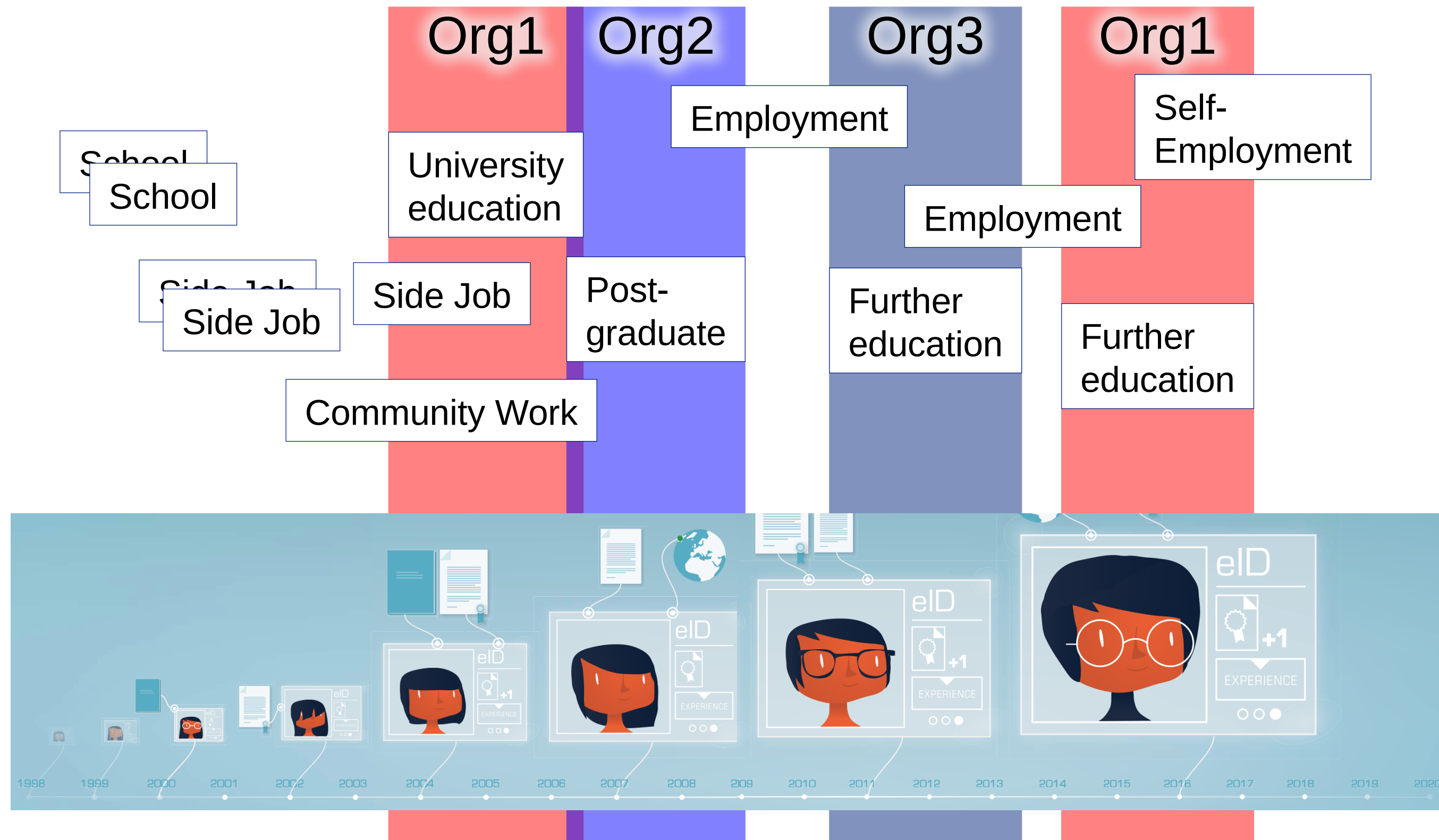
SWITCH

Etienne Dysli Metref  
software engineer  
[etienne.dysli-metref@switch.ch](mailto:etienne.dysli-metref@switch.ch)

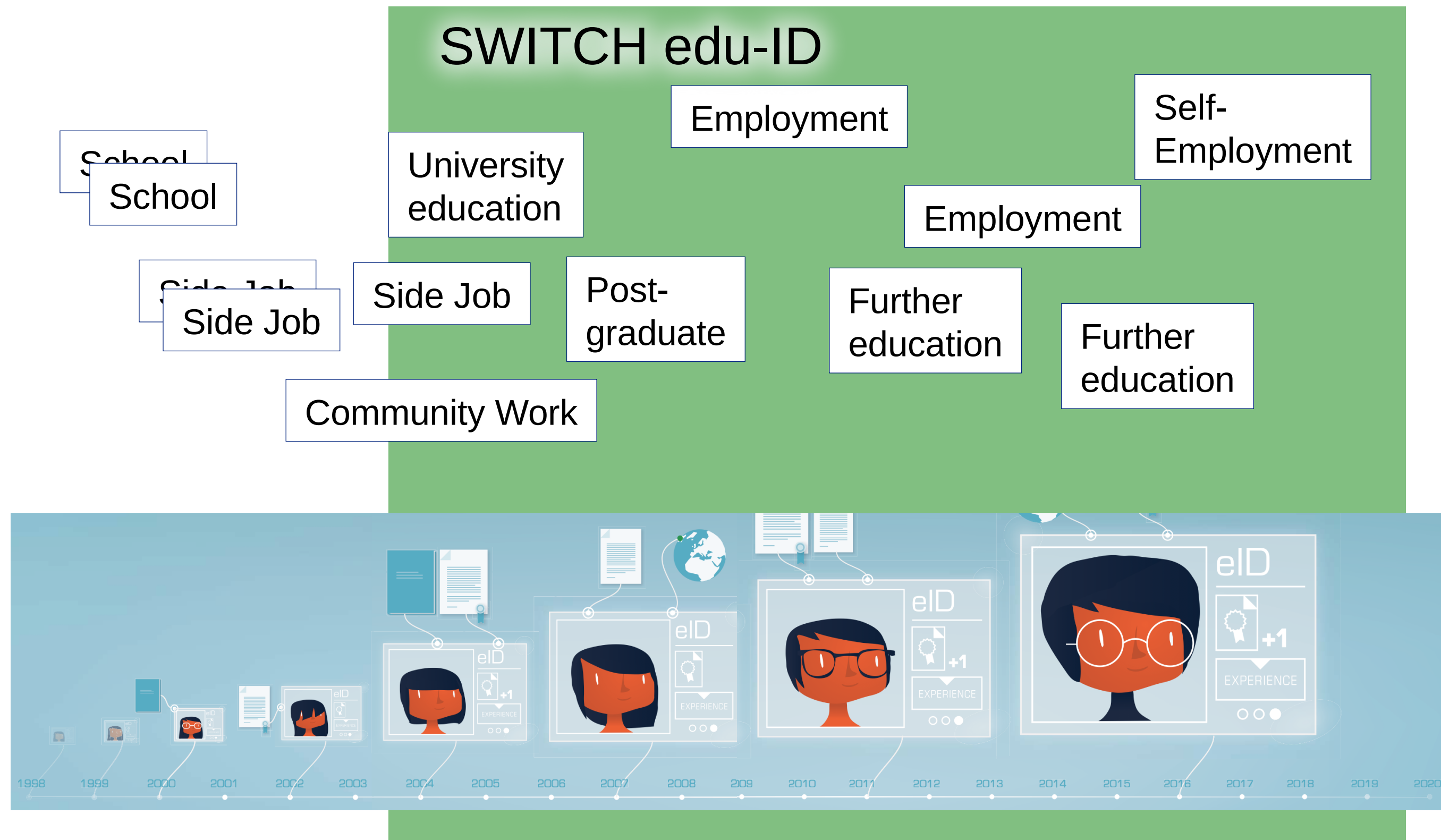
TNC19 2019-06-19



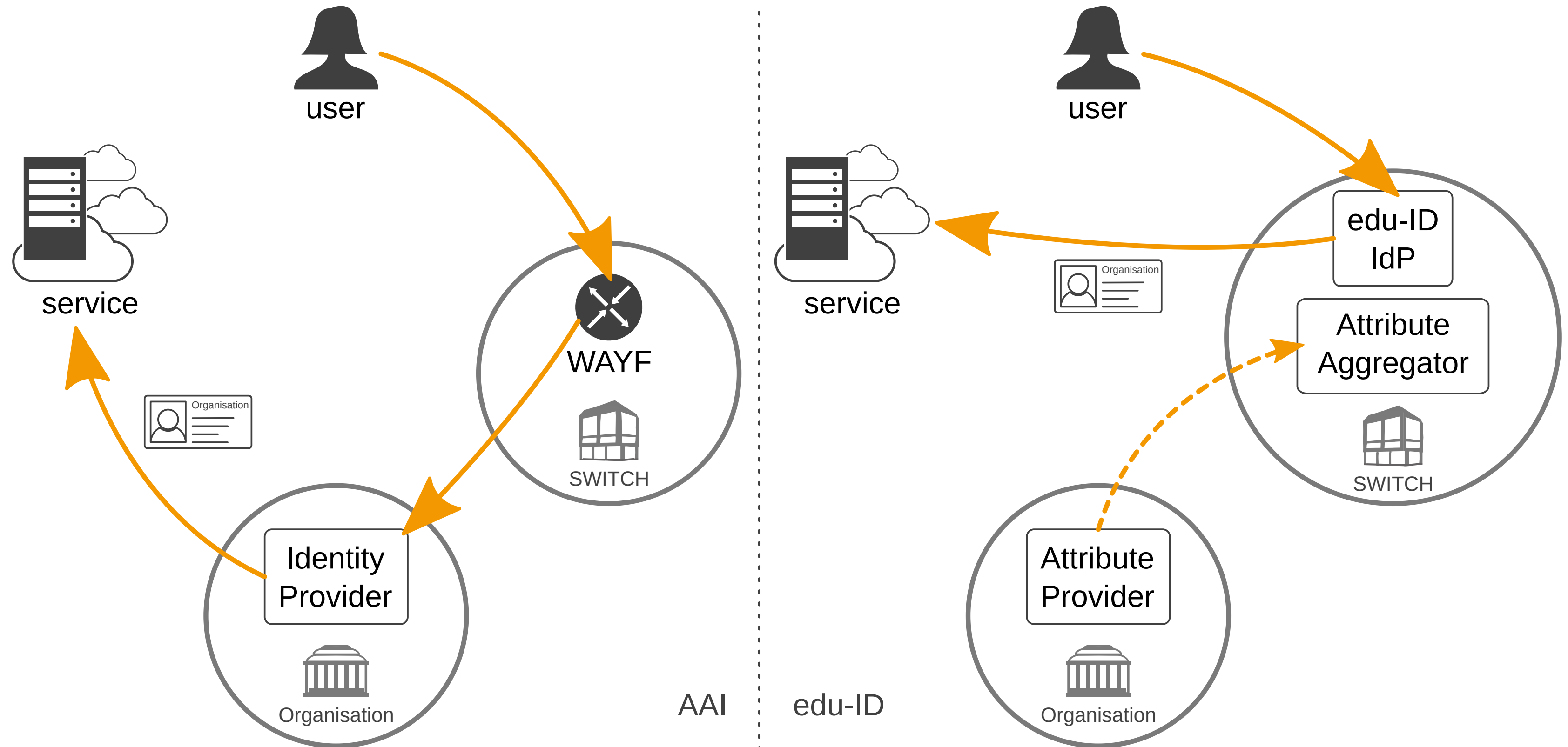
# Without edu-ID: identity tied to the organisation



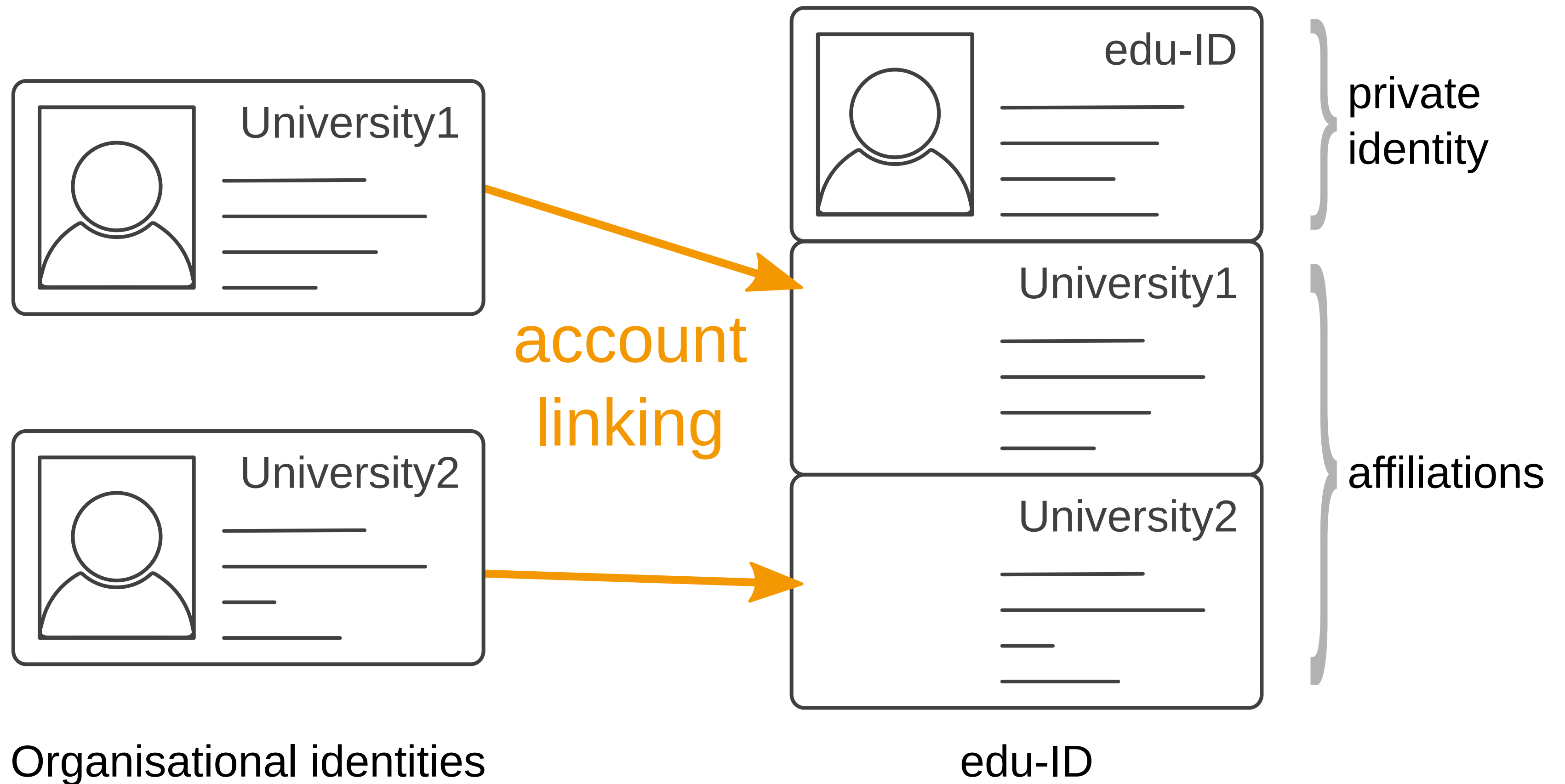
# With edu-ID: identity tied to the person



# Login flows: SWITCHaai vs. edu-ID



# Account linking and affiliations



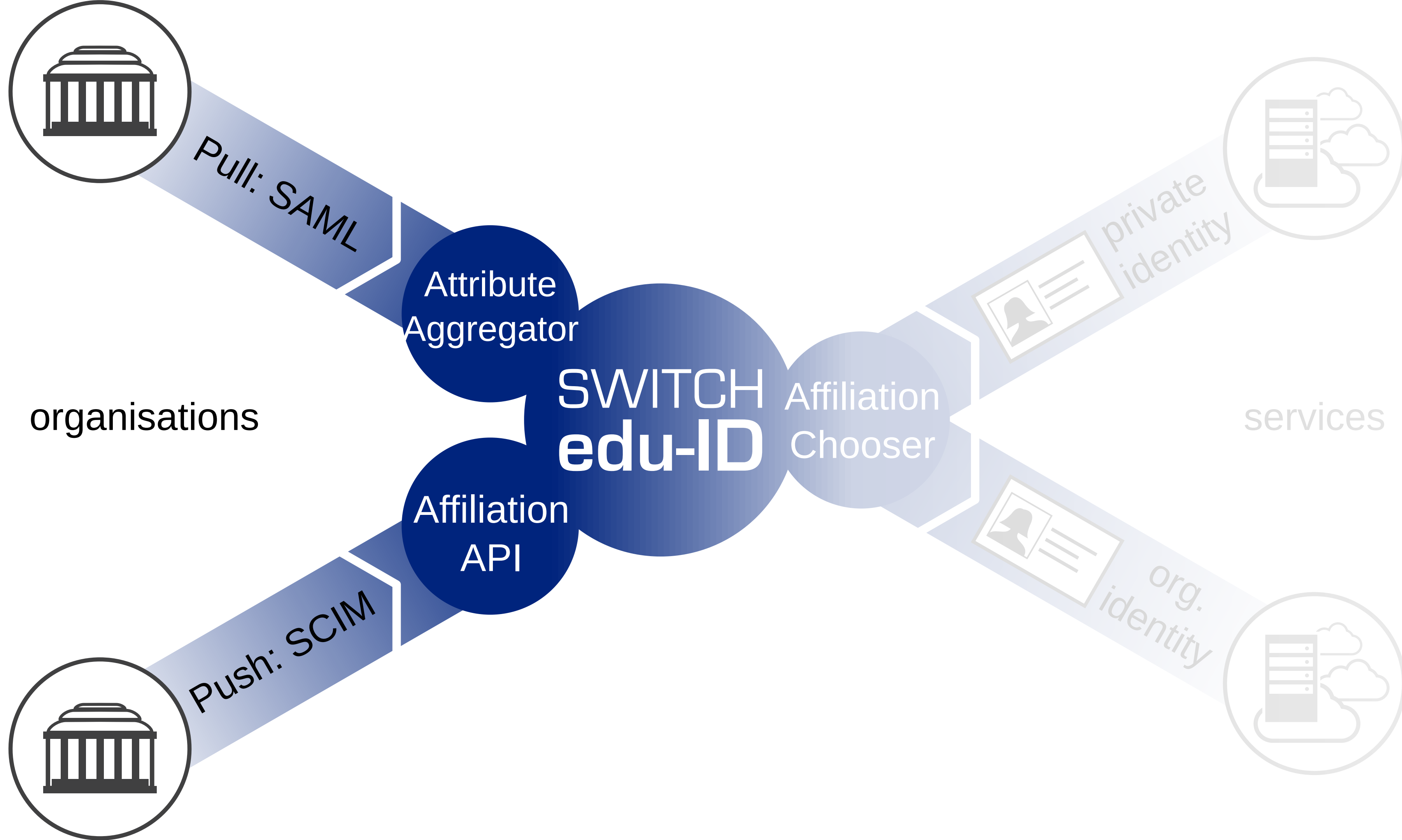
# Keeping affiliation attributes up to date

## Challenges

- **SPs should not have to change anything** to use SWITCH edu-ID
- account linking → *copies* organisation-managed attributes
- update our copy? transmit to services?

## Our solutions

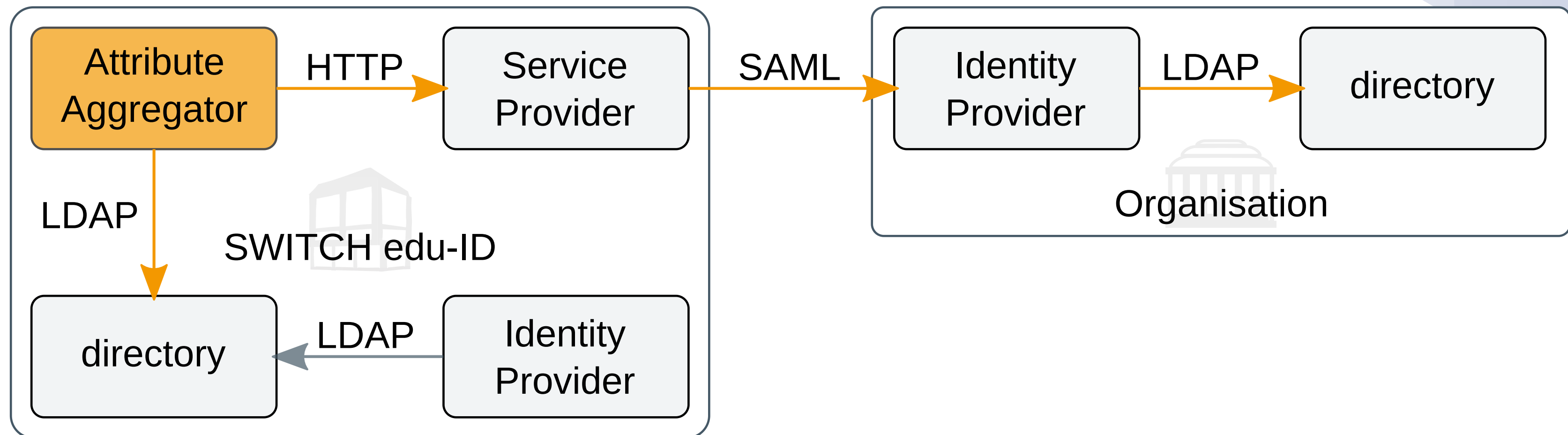
- Either we **pull** attributes from each organisation,
- or organisations **push** data changes to us.
- Send one or all affiliations to SPs?





# Pull: the Attribute Aggregator

- Reuse the organisation IdP's ability to respond to SAML attributes queries
- Reuse the Shibboleth SP to make SAML attribute queries for us



# Pull: the Attribute Aggregator

## Once a day

- collects all stored *current affiliations*
- issues a SAML attribute query to their originating IdP
- replaces the set of attributes by the new one received
- if IdP replies that the person is no longer affiliated, flags the old set of attributes as a *former affiliation*

# Shibboleth SP configuration

```
<ApplicationDefaults>
  <Sessions>
    <Handler type="AttributeResolver" Location="/AttributeResolver"
      acl="127.0.0.1 ::1"/>
  </Sessions>

  <AttributeResolver type="Query" subjectMatch="true"
    exceptionId="attributeResolutionException"/>
</ApplicationDefaults>
```

## Example manual HTTP request

```
curl --get "https://test.eduid.ch/Shibboleth.sso/AttributeResolver" \
  --data-urlencode "format=urn:oasis:names:tc:SAML:2.0:nameid-format:persistent" \
  --data-urlencode "entityID=https://aai-logon.switch.ch/idp/shibboleth" \
  --data-urlencode "nameId=A++ZTP/Gbj0vuShuQoVuDzdDlLIqNRm1pGYYapdHI14="
```

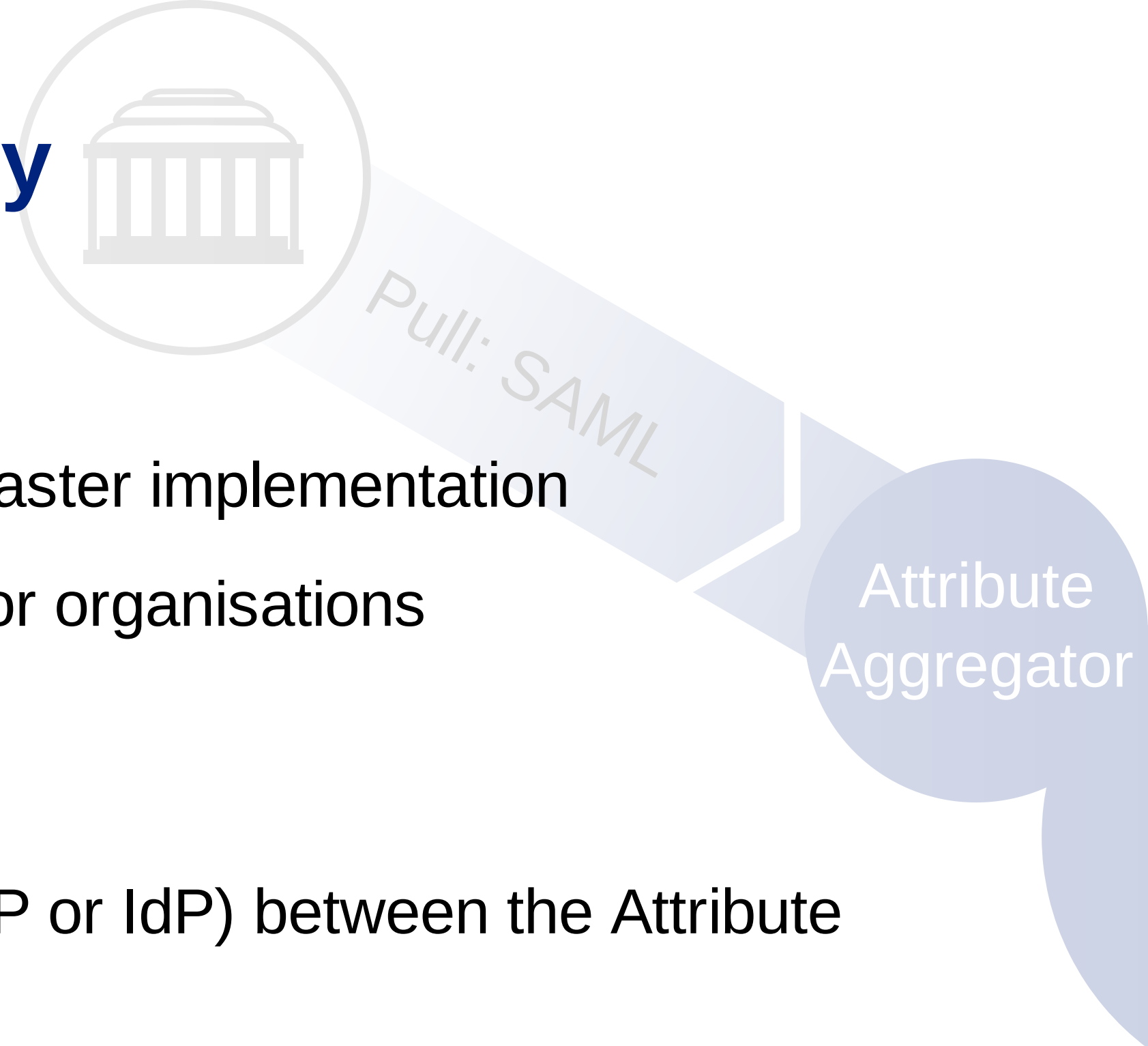
# Problem: no clear signal about account (in)validity

Example SP error response (but HTTP 200 OK...)

```
{
  "attributeResolutionException": [
    "Attribute%20authority%20returned%20a%20SAML%20error."
  ],
  "persistent-id": [
    "https://aai-logon.switch.ch/idp/shibboleth!https://test.eduid.ch/shibboleth!A++ZTP/Gbj0vuShuQoVuDzdDlLIqNRm1pGYYapdHI14="
  ]
}
```

- queried identifier always echoed in response
- different errors look the same
- even doing SAML processing ourselves would not help

# Attribute Aggregator summary



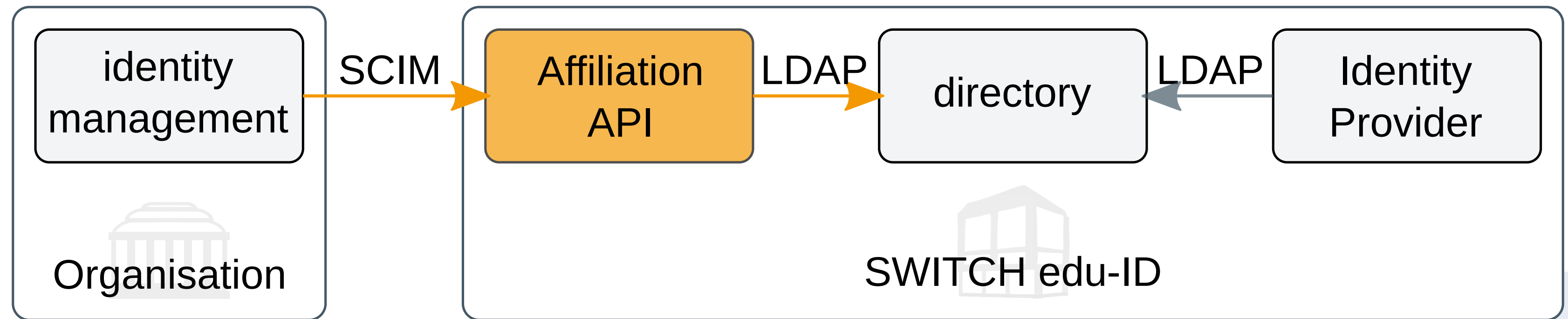
## Advantages

- no need to code SAML/XML processing ⇒ faster implementation
- works with out-of-the-box IdPs ⇒ no effort for organisations

## Drawbacks

- masks many possible errors (network, HTTP or IdP) between the Attribute Aggregator and the target IdP
- no reliable criteria to expire affiliations, needs additional guessing  
⇒ delayed updates
- no direct way to report invalid data to the organisation

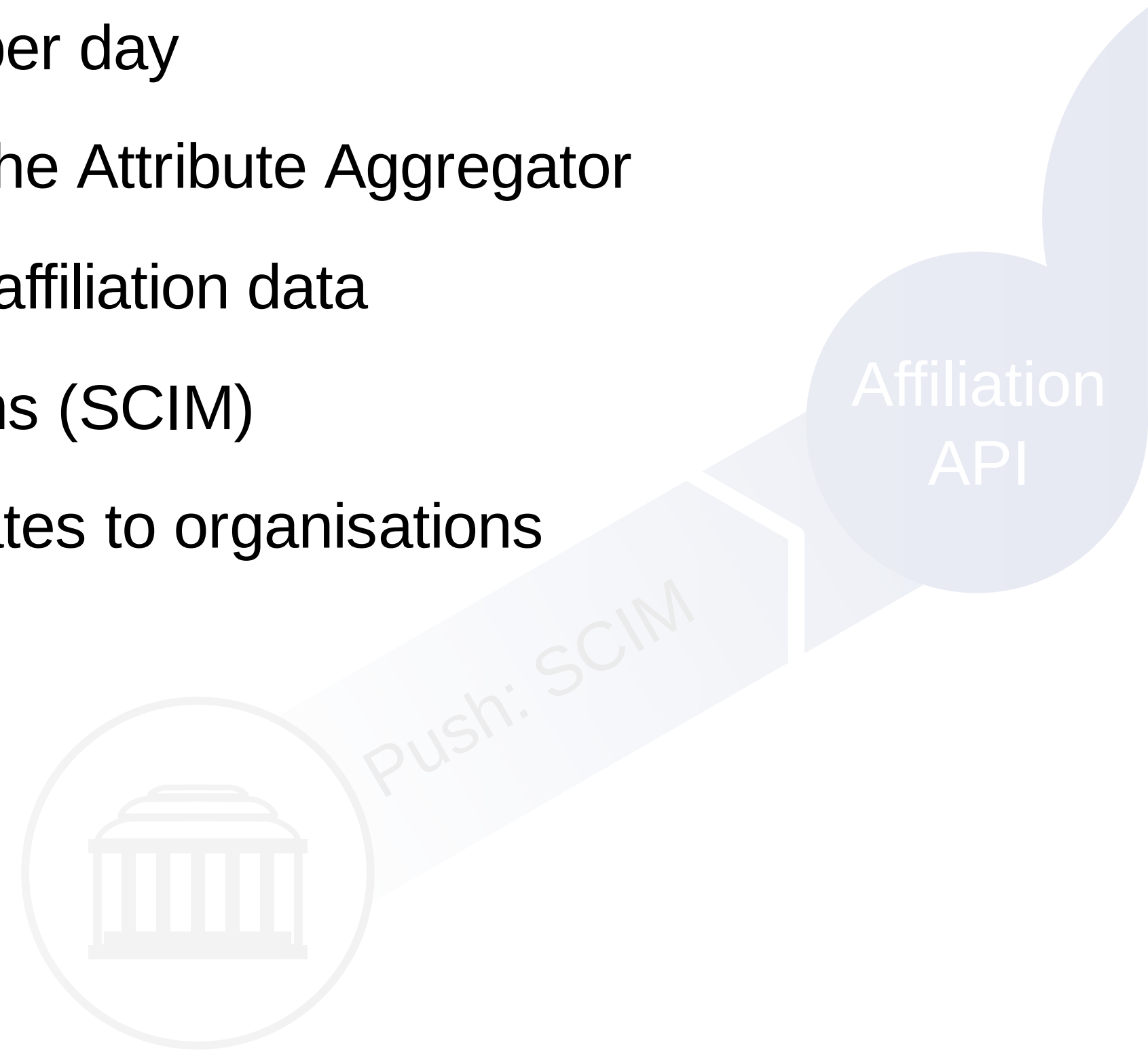
# Push: Affiliation API

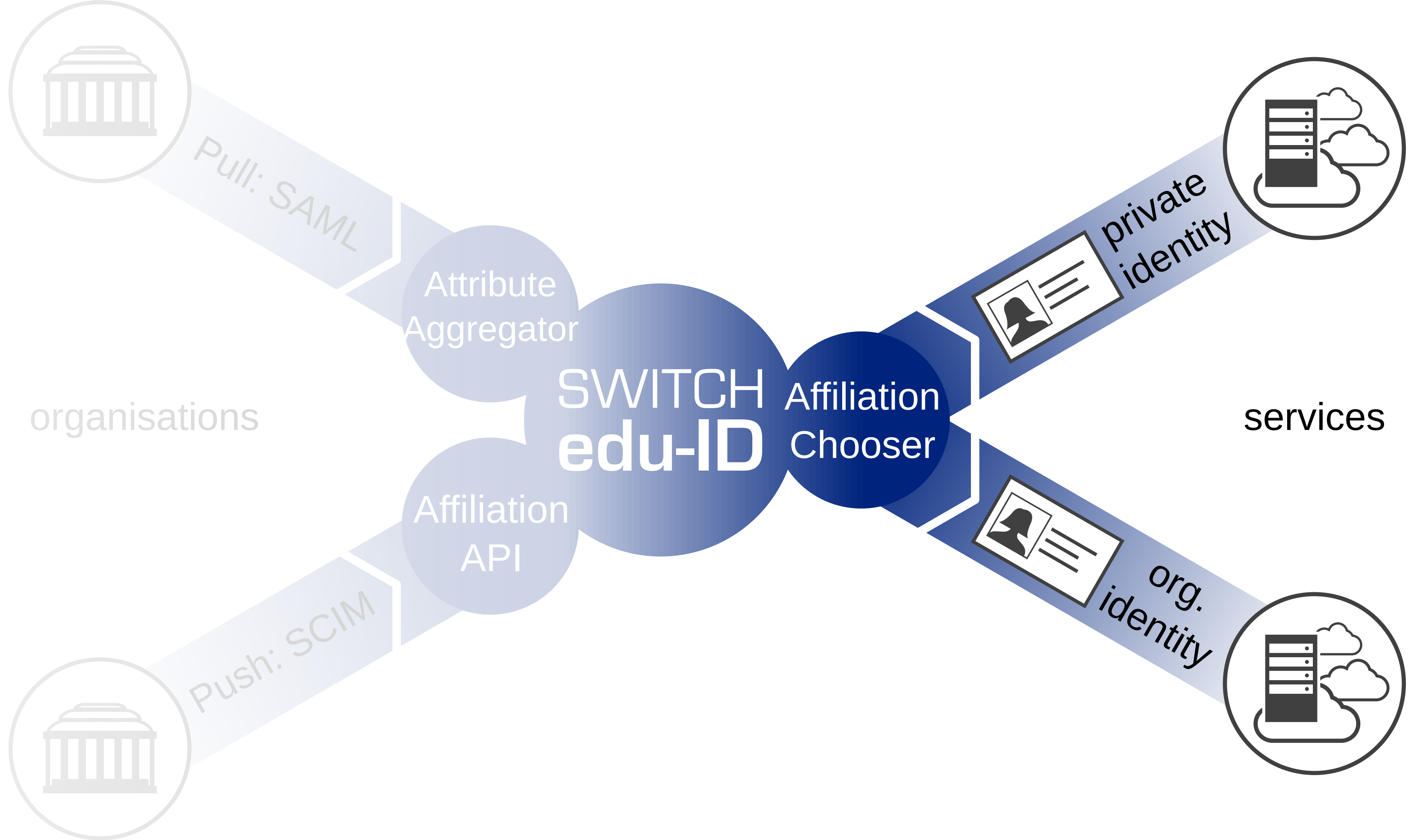


- organisations send affiliation data to the edu-ID system themselves
- SCIM 2.0 API, custom resource type Affiliation
- offers the usual create, read, update and delete (expire) operations
- used in production by one organisation (1 out of 3 migrated organisations)

# Affiliation API: our favourite option

- implementation effort for organisations, but...
- changes take effect immediately, not once per day
- not subject to uncertainty of expiration like the Attribute Aggregator
- direct channel to report invalid/inconsistent affiliation data
- integrates with identity management systems (SCIM)
- clearly delegates responsibility of data updates to organisations







# Juggling identities: the Affiliation Chooser

## Affiliation Chooser

### Choose an Identity to Proceed

**You are about to access the service 'AAI Attributes Viewer' with one of your identities. Choose one to proceed.**


When you return to the service it will recognize you with the identity you choose now.

**Staff @ SWITCH Staff**  
[etienne.dysli-metref@switch.ch](mailto:etienne.dysli-metref@switch.ch)



**Private Person**  
[etienne.dysli-metref@switch.ch](mailto:etienne.dysli-metref@switch.ch)



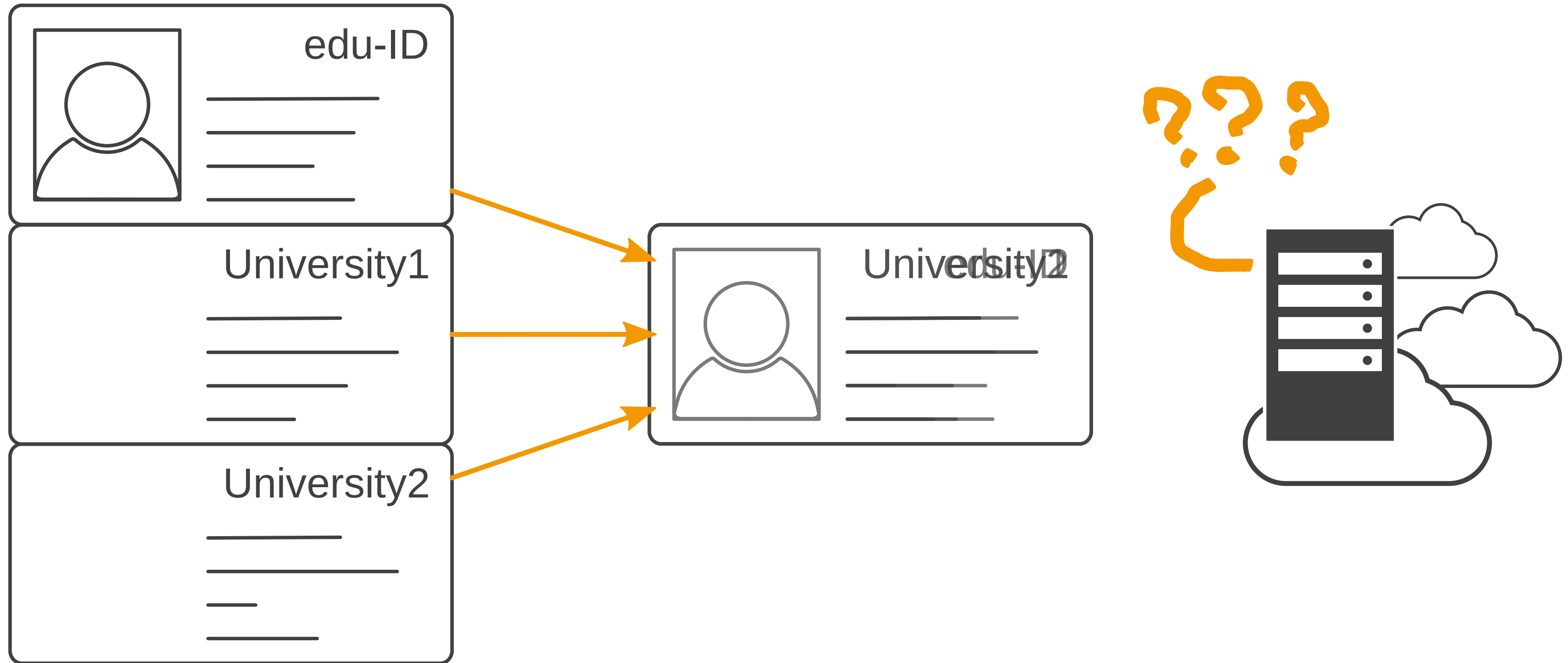
 [Manage your identities](#)

**SWITCH**

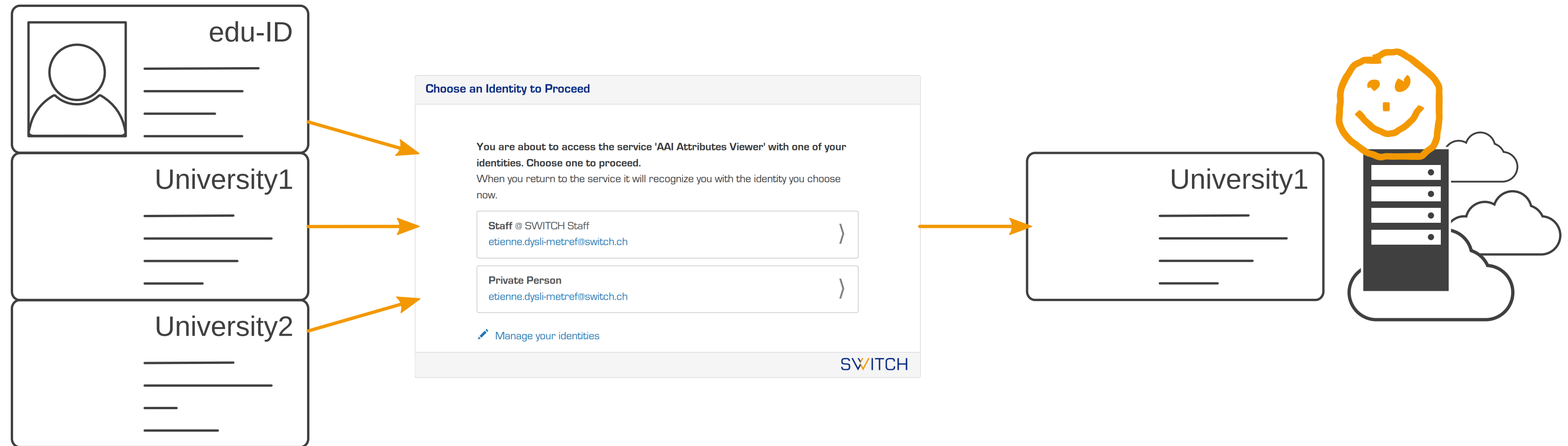
# How to transmit multiple identities?



# Send all identities together

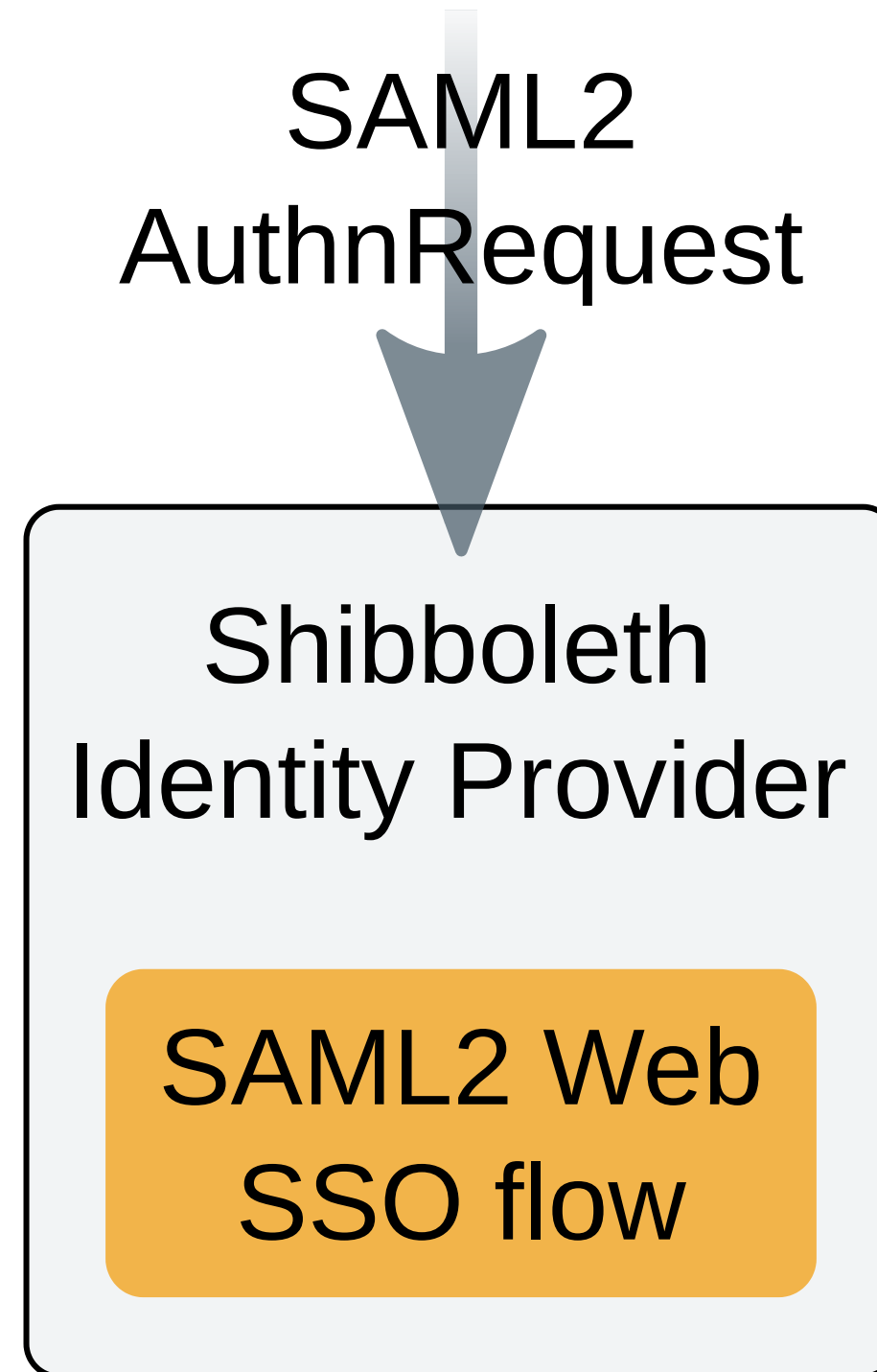


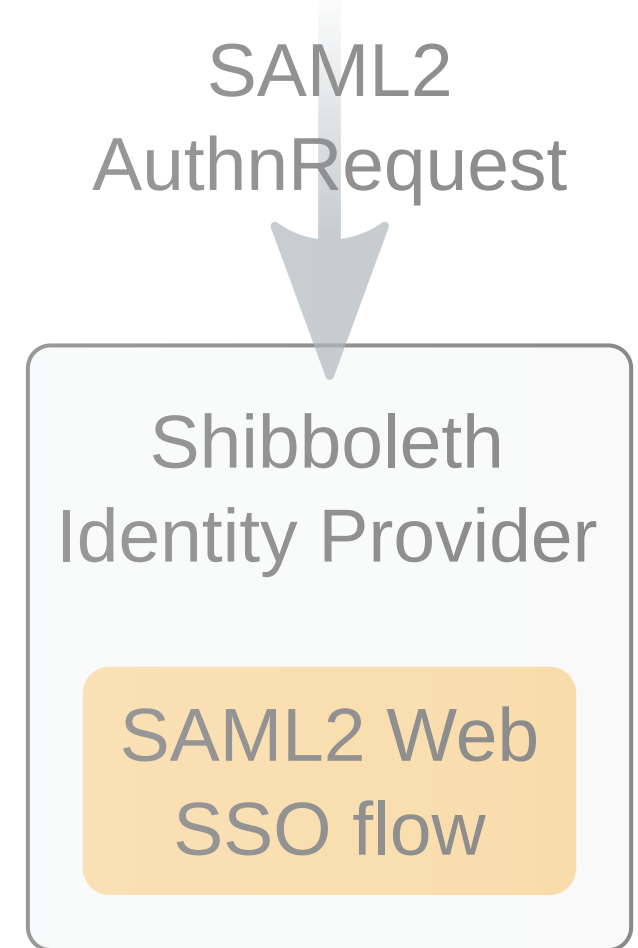
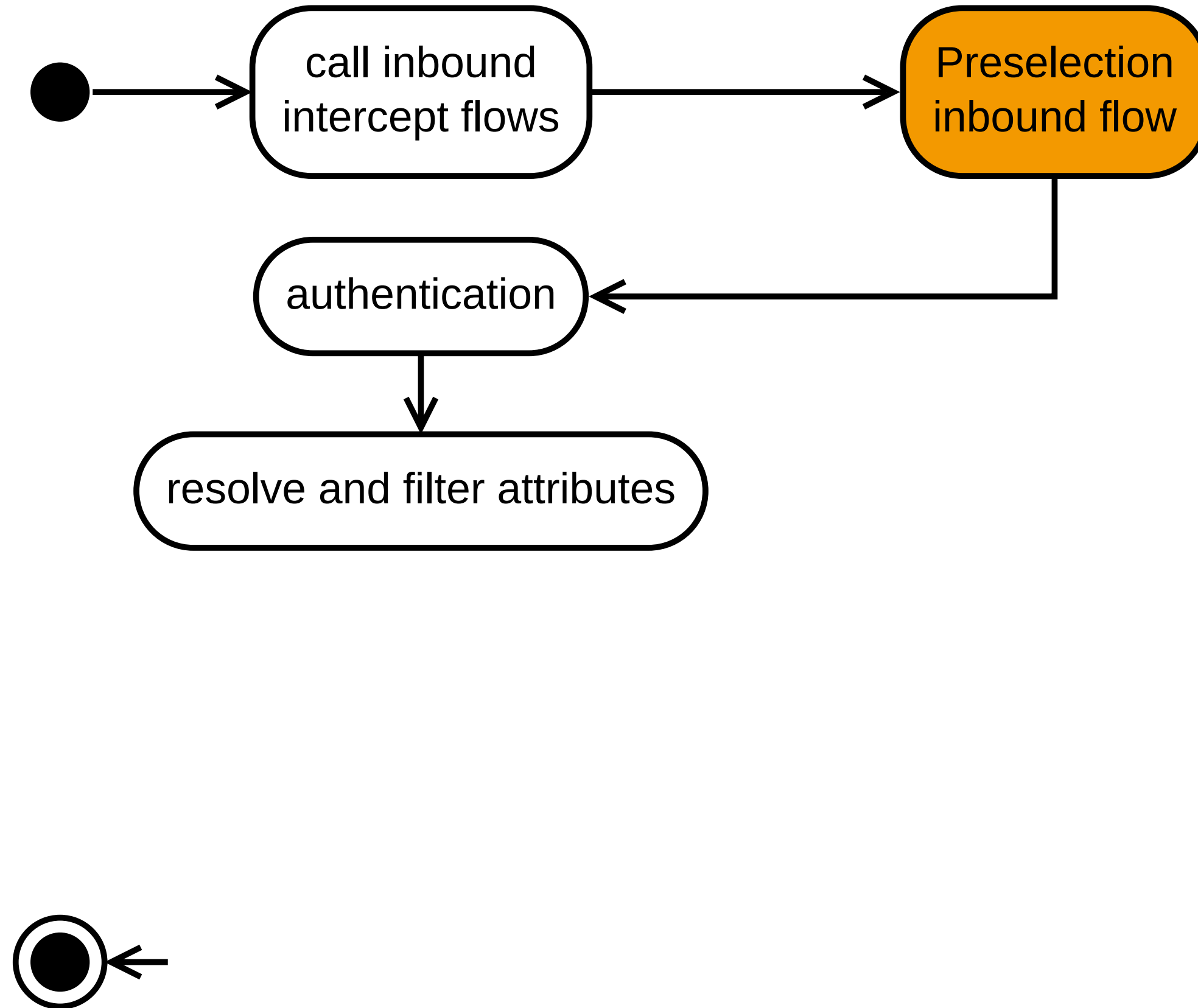
# Choose your own identity

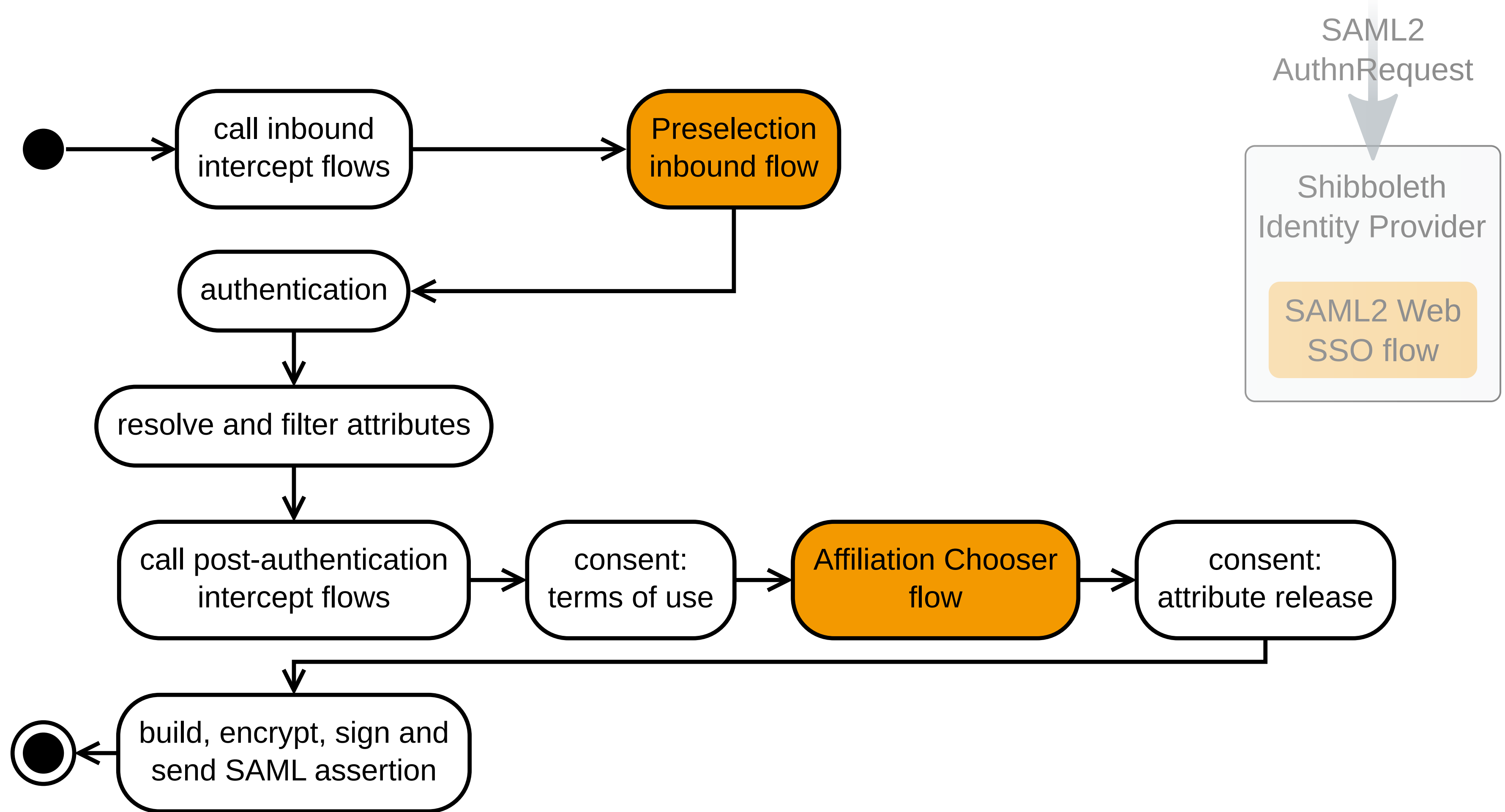


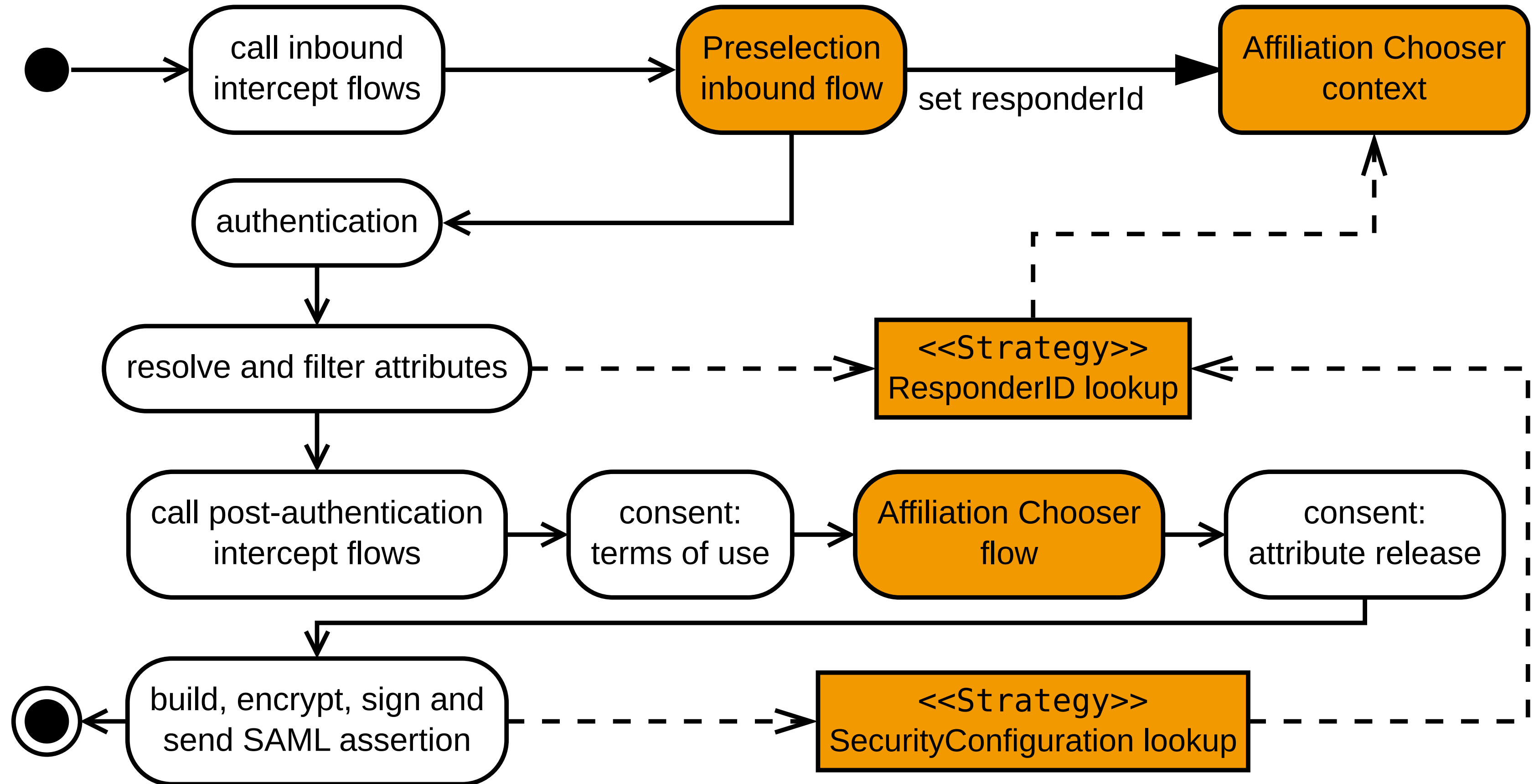
*classic attribute model*

# Inside the SWITCH edu-ID Identity Provider Affiliation Chooser implementation



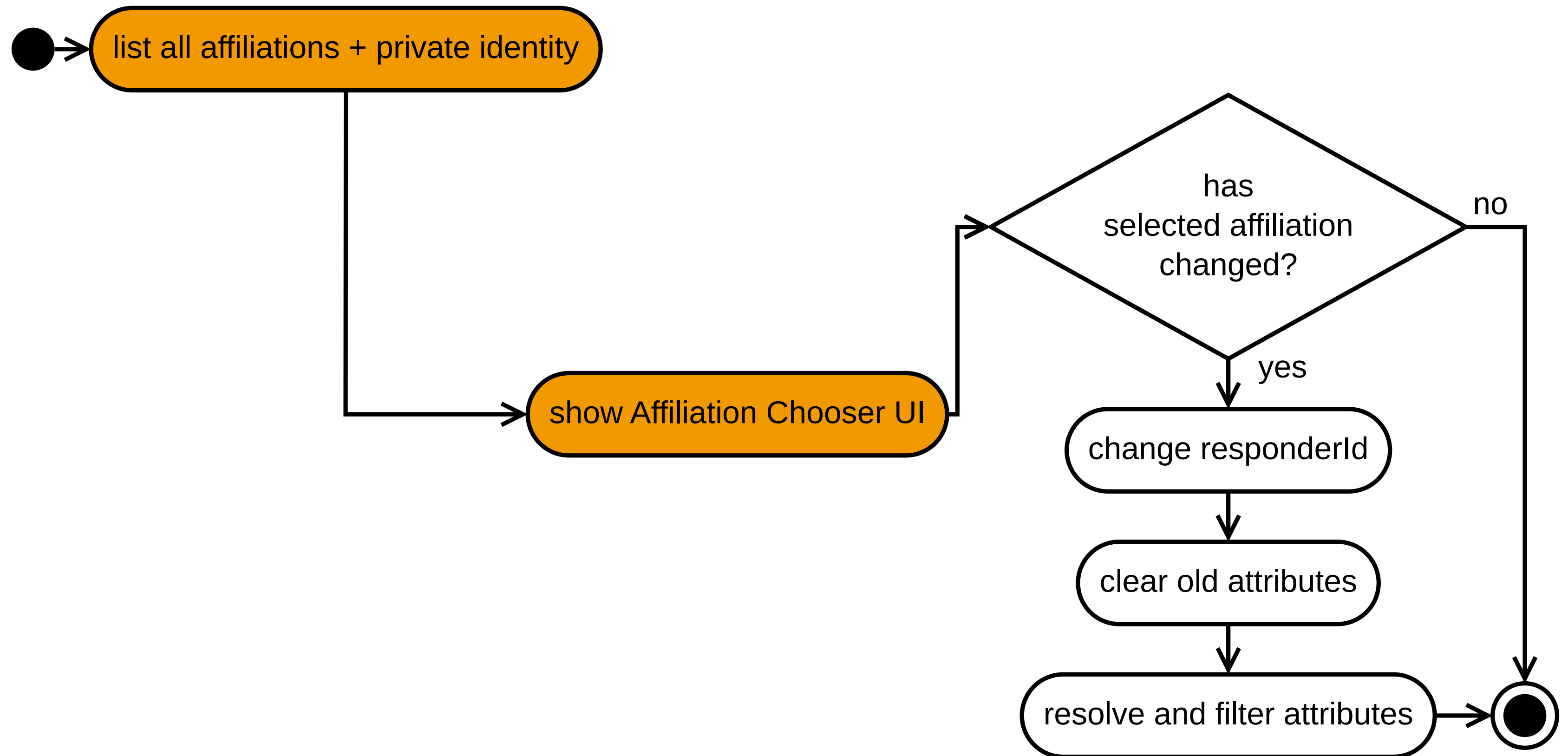




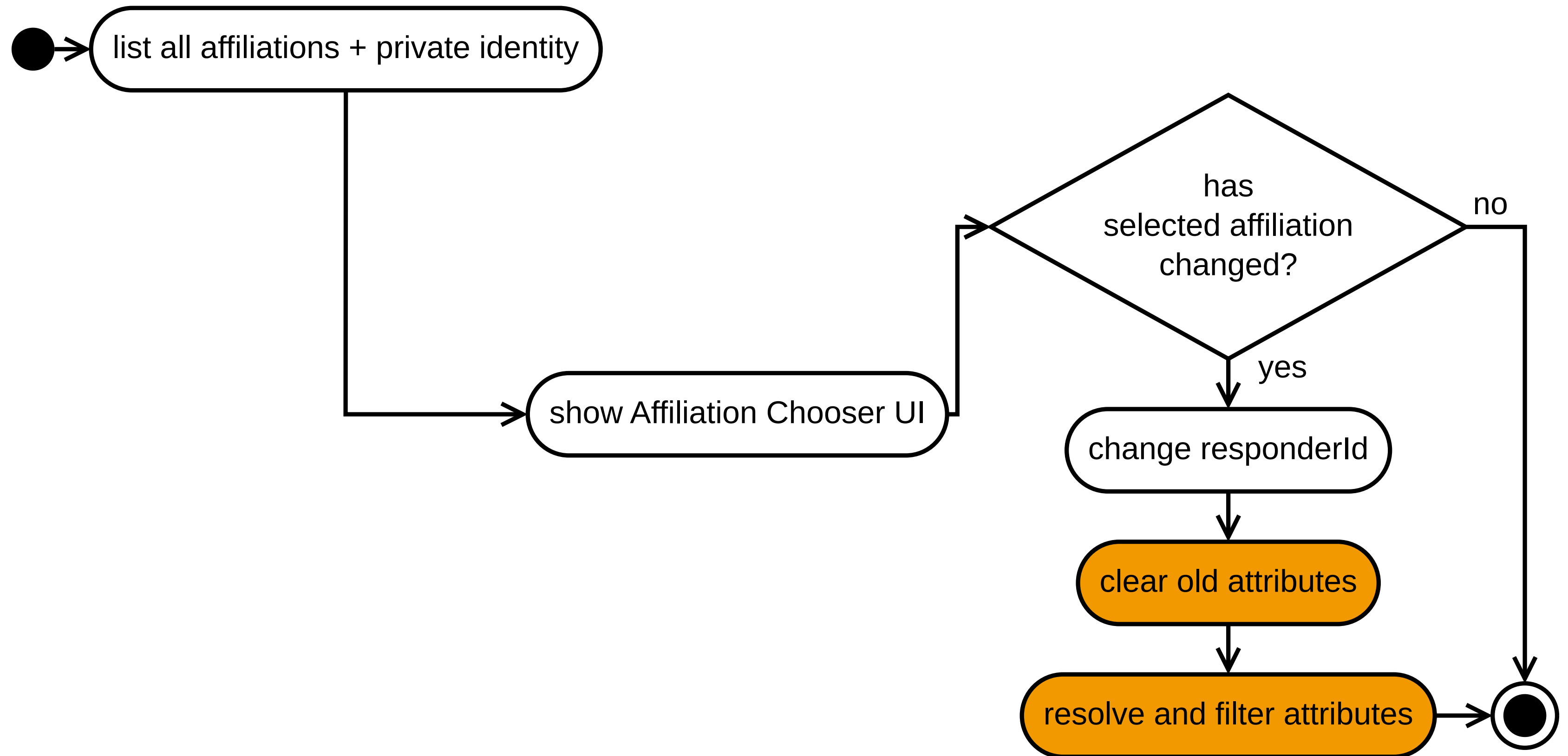




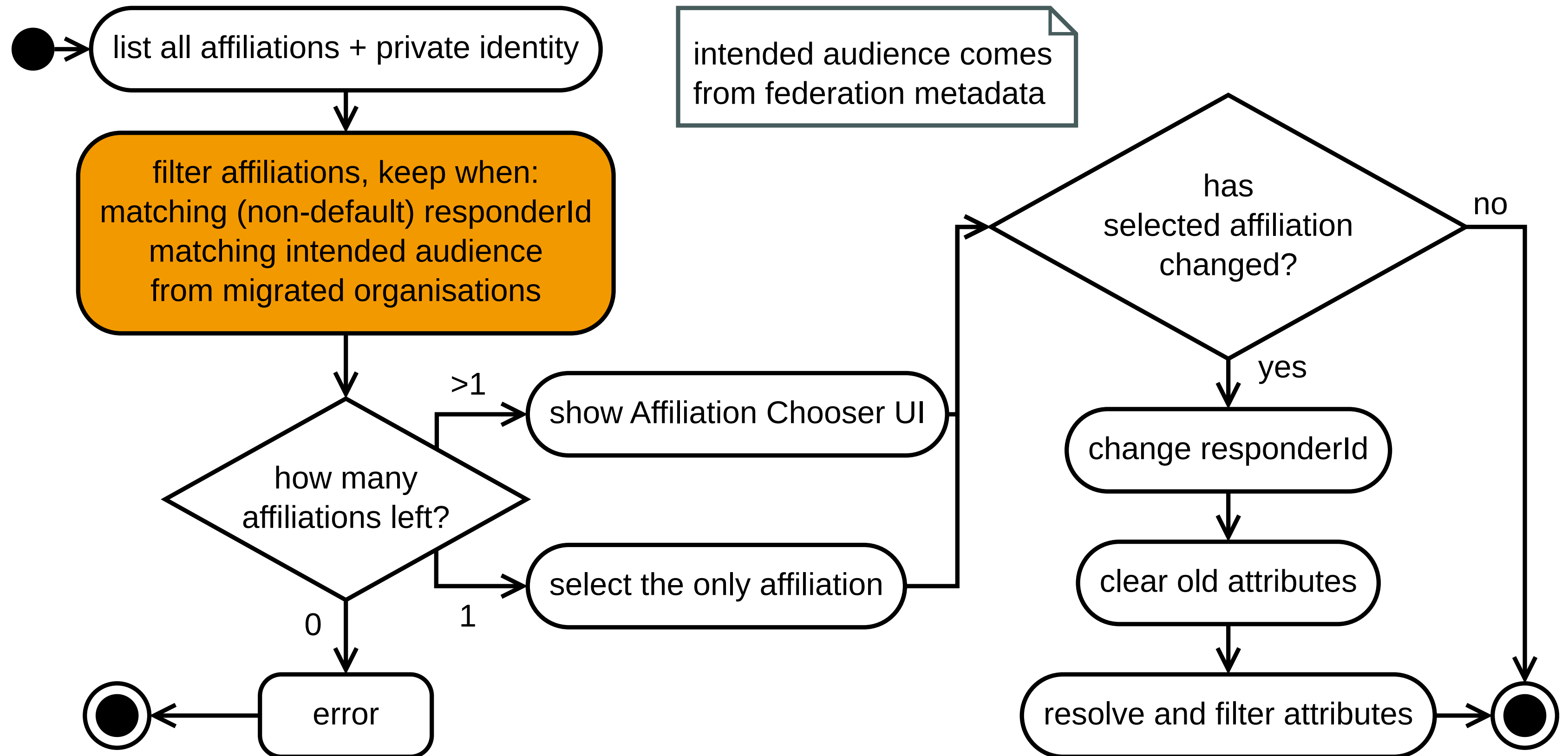
# Post-authentication intercept flow



# Post-authentication intercept flow



# Post-authentication intercept flow



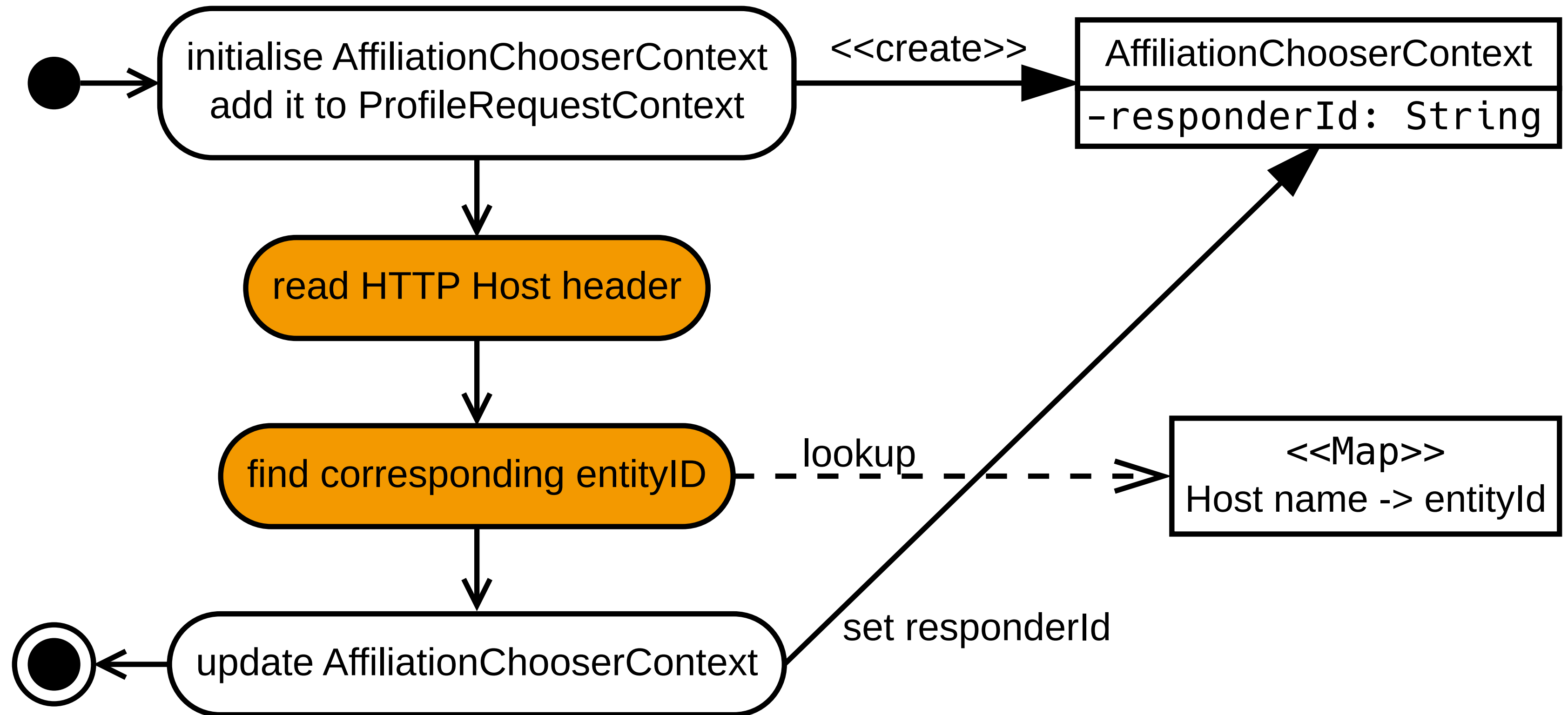
# Inbound intercept flow

- change migrated IdP's SAML endpoints to SWITCH edu-ID IdP with special host name <organisation>.login.eduid.ch:

```
<EntityDescriptor entityID="https://aai-logon.unilu.ch/idp/shibboleth">  
  <IDPSSODescriptor protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">  
    <SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"  
      Location="https://unilu.login.eduid.ch/idp/profile/SAML2/Redirect/SSO"/>  
    <SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"  
      Location="https://unilu.login.eduid.ch/idp/profile/SAML2/POST/SSO"/>  
    </IDPSSODescriptor>  
  </EntityDescriptor>
```

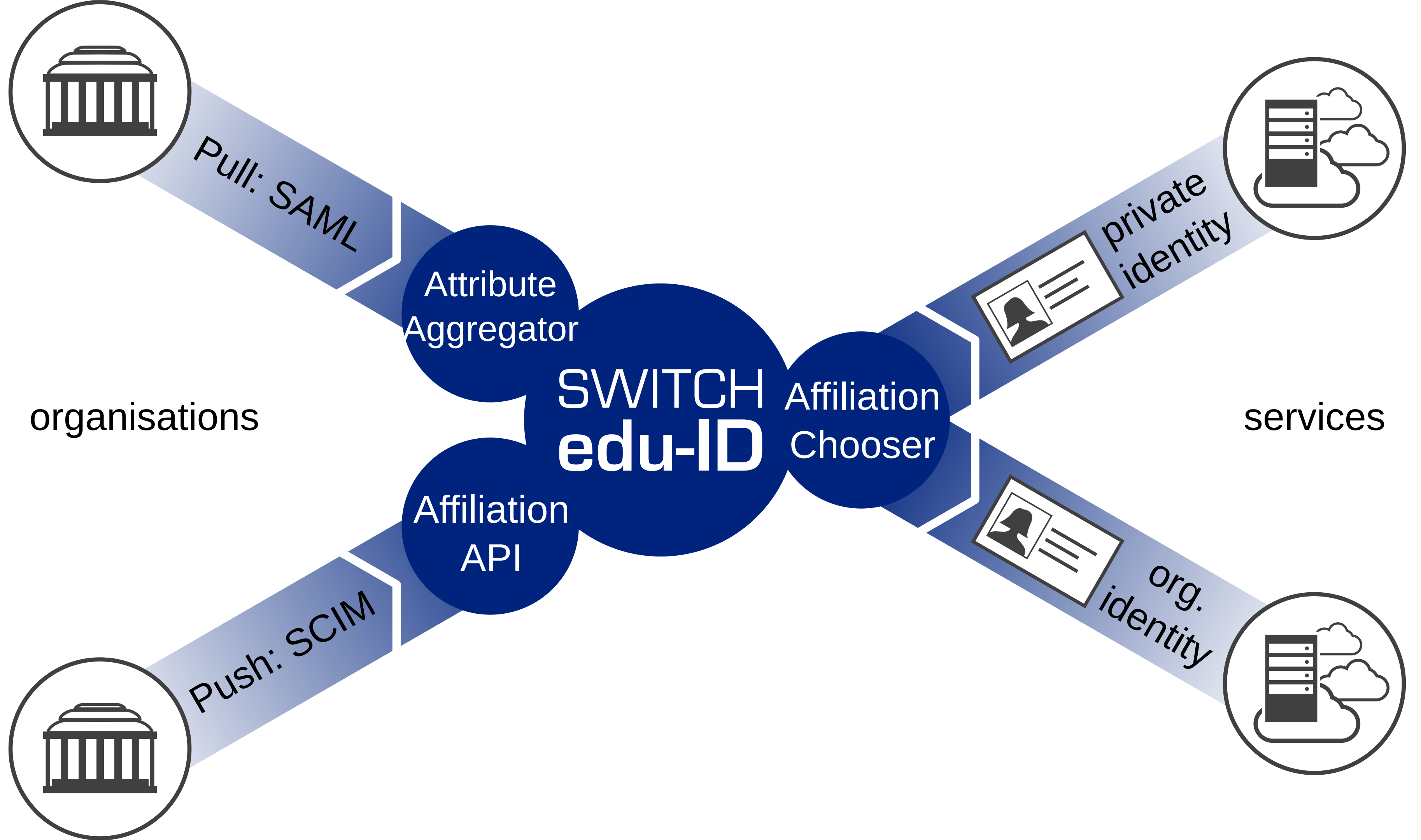
- selecting <organisation> in WAYF redirects to <organisation>.login.eduid.ch

# Inbound intercept flow



# Affiliation Chooser summary

- Shibboleth IdP v3 extension for the SWITCH edu-ID IdP
- many IdP configuration changes
- migrated organisation's IdP still in metadata but points to edu-ID IdP
- IdP keys copied from migrated organisations
- running in production since March 2018







# SWITCH

## Working for a better digital world

Etienne Dysli Metref  
software engineer  
[etienne.dysli-metref@switch.ch](mailto:etienne.dysli-metref@switch.ch)

<https://www.switch.ch/edu-id/>



# Shibboleth IdP configuration

Non-exhaustive list of configuration changes for the Affiliation Chooser

- responderId lookup **function**
- register intercept flows
- keys for all migrated organisations
- data connectors with activation conditions, split searches under private identity and affiliations
- attribute definitions with data connectors and activation conditions
- internal attribute definitions for the Affiliation Chooser UI
- subject canonicalisation to use internal edu-ID identifier

# Example: changes in conf/relying-party.xml

```
<bean id="shibboleth.DefaultRelyingParty" parent="RelyingParty"
  p:responderIdLookupStrategy-ref="affiliationchooser.ResponderIdLookup">
  <property name="profileConfigurations">
    <list>
      <bean parent="SAML2.SSO"
        p:inboundInterceptorFlows=
"#{ {'security-policy/saml2-sso', 'affiliation-chooser/inbound'} }"
        p:postAuthenticationFlows=
"#{ {'terms-of-use', 'affiliation-chooser/post-authn-chooser', 'attribute-release'} }"
        p:securityConfigurationLookupStrategy-ref=
"affiliationchooser.SecurityConfigurationLookup"/>
      <bean parent="SAML2.ECP" ... />
      <bean parent="SAML2.Logout" ... />
      <bean parent="SAML2.AttributeQuery" ... />
      <bean parent="SAML2.ArtifactResolution" ... />
    </list>
  </property>
</bean>
```