Release of assurance statements in the attribute eduPersonAssurance based on SWAMID Identity Profiles

In the SWAMID Federation Policy it's defined in the last paragraph in section 4.3 SWAMID Member that all SWAMID Members and their Subjects MUST fulfil one or more of the SWAMID Identity Assurance Profiles. This page describes what attribute values should be released in the attribute for SWAMID Identity Assurance Profiles, including mapped values for REFEDS Assurance Framework. Please note that Identity Providers only can release assurance information for SWAMID Identity Assurance Profiles they are approved for.

Text in green shows where there is a difference between SWAMID Identity Assurance Level Profiles, i.e. the nearest "lower level".

SWAMID Identity Assurance Profile 1

A user that fulfils SWAMID Identity Assurance Level 1 Profile should get the following values in the attribute eduPersonAssurance:

- http://www.swamid.se/policy/assurance/al1
- https://refeds.org/assurance
- https://refeds.org/assurance/ID/unique
- https://refeds.org/assurance/ID/eppn-unique-no-reassign
- https://refeds.org/assurance/IAP/low
- https://refeds.org/assurance/ATP/ePA-1m

SWAMID Identity Assurance Profile 2

A user that fulfils SWAMID Identity Assurance Level 2 Profile should get the following values in the attribute eduPersonAssurance:

- http://www.swamid.se/policy/assurance/al1
- http://www.swamid.se/policy/assurance/al2
- https://refeds.org/assurance
- https://refeds.org/assurance/profile/cappuccino
- https://refeds.org/assurance/ID/unique
- https://refeds.org/assurance/ID/eppn-unique-no-reassign
- https://refeds.org/assurance/IAP/low
- https://refeds.org/assurance/IAP/medium
- https://refeds.org/assurance/IAP/local-enterprise
- https://refeds.org/assurance/ATP/ePA-1m

SWAMID Identity Assurance Profile 3 without multi-factor authentication

A user that fulfils SWAMID Identity Assurance Level 3 Profile should be signaled as SWAMID Identity Assurance Profile 2 when not performing a multi-factor authentication.

SWAMID Identity Assurance Profile 3 including multi-factor authentication

A user that fulfils SWAMID Identity Assurance Level 3 Profile should get the following values in the attribute eduPersonAssurance:

- http://www.swamid.se/policy/assurance/al1
- http://www.swamid.se/policy/assurance/al2
- http://www.swamid.se/policy/assurance/al3
- https://refeds.org/assurance
- https://refeds.org/assurance/profile/cappuccino
- https://refeds.org/assurance/profile/espresso
- https://refeds.org/assurance/ID/unique
- https://refeds.org/assurance/ID/eppn-unique-no-reassign
- https://refeds.org/assurance/IAP/low
- https://refeds.org/assurance/IAP/medium
- https://refeds.org/assurance/IAP/high

- https://refeds.org/assurance/IAP/local-enterprise
- https://refeds.org/assurance/ATP/ePA-1m

Additional information on specific REFEDS Assurance Framework values

https://refeds.org/assurance

SWAMID Identity Assurance Profiles fulfils item 1-3 of the REFEDS Assurance Framework baseline expectations cited below. Item 3-4 is enforced by SWAMID SAML WebSSO Technology Profile.

For an Identity Provider to conform to this REFEDS Assurance Framework it is REQUIRED to conform to the following baseline expectations for Identity Providers:

1. *The Identity Provider is operated with organizational-level authority*
2. *The Identity Provider is trusted enough that it is (or it could be) used to access the organization's own systems*
3. *Generally-accepted security practices are applied to the Identity Provider*
4. *Federation metadata is accurate, complete, and includes at least one of the following: support, technical, admin, or security contacts*

https://refeds.org/assurance/ID/unique

In section 5.2.3 of all SWAMID Identity Assurance Profiles it's defined that a user must be represented with one or more unique identifiers. It's defined in 5.5.4 and 5.5.5 of the SWAMID SAML WebSSO Technology Profile that an Identity Provider must support the release of SAML 2.0 Subject Identifier Attribute subject-id and SAML 2.0 Subject Identifier Attribute pairwise-id and that the values must be not reassigned. This attribute value defines that released values of the identifier attributes must be unique and never reused for another user. However, the value doesn't imply that you release all identifier attributes.

The identifier MUST have the following four properties:

- *(Unique-1) The user identifier represents a single natural person;*
- *(Unique-2) The Identity Provider can contact the person to whom the identifier is issued;*
- *(Unique-3) The user identifier is never re-assigned; and*
- *(Unique-4) The user identifier is eduPersonUniqueId, SAML 2.0 persistent name identifier, SAML 2.0 Subject Identifier Attribute subject-id or SAML 2.0 Subject Identifier Attribute pairwise-id.*

Note also that the identifier eduPersonUniqueId is not used in SWAMID attribute release best practice as of April 2021.

https://refeds.org/assurance/ID/eppn-unique-no-reassign

In 5.2.3 of all SWAMID Identity Assurance Profiles it's defined that a user must be represented with one or more unique identifiers. It's defined in 5.5.3 of the SWAMID SAML WebSSO Technology Profile that an Identity Provider must support the release of eduPersonPrincipleName and that it must be not reassigned. This attribute value defines that the released value of the attribute eduPersonPrincipalName must be unique and never reused for another user. However, the value doesn't imply that you release the attribute.

The expected Service Provider behaviour for observing eduPersonPrincipalName re-assignment:

- *If the Identity Provider asserts eppn-unique-no-reassign, the Relying Party knows that when it observes a given ePPN value it will always belong to the same individual.*

https://refeds.org/assurance/IAP/local-enterprise

SWAMID Identity Assurance Level 2 and Level 3 Profiles fulfill the requirements. You should not release local-enterprise for SWAMID Identity Assurance Level 1 users since the profile only requires that it's a natural person, not an identified natural person.

https://refeds.org/assurance/ATP/ePA-1m

In 5.5.9 and 5.5.10 of the SWAMID SAML WebSSO Technology Profile it's defined that attribute release from an Identity Provider must follow the organisation administrative processes and changes must reflected in attribute release within one work week.

This attribute value signals that the values of the attributes eduPersonAffiliation and eduPersonScopedAffliation changes within one month from the departure from the organisation or change of organisational roles (i.e., if an employee no longer is defined as an employee or a student is no longer a student). In REFEDS Assurance Framework it's defined that "a departure" from an organisation takes place when the organisation decides that the user doesn't have a continuing basis for the affiliation value and therefore loses their organisational role and privileges (i.e., can no longer speak for the organisation in that role).

The organisational business practices here may vary; for instance:

- *In some organisations a researcher loses their organisational role and privileges the day their employment or other contract ends, in some organisations there is a defined grace period.*
- *In some universities a student loses their organisational role and privileges the day they graduate, in some organisations the student role and privileges remain effective until the end of the semester.*

REFEDS Assurance Framework imposes no particular requirements on the organisational business practices regarding when the departure takes place. This value is intended to indicate only the maximum latency for the Identity Provider's identity management system to reflect the departure in the user's attributes.

Notice also that this section does not require that the departing user's account must be removed or disabled; only that the affiliation attribute value as observed by the Service Provider is updated.

Technical implementation

SWAMID has published information in Swedish on how to configure release of assurance via the attribute **eduPersonAssurance**.

- Signalera tillitsprofil genom eduPersonAssurance