REFEDS Assurance Framework v1.0

REFEDS Assurance working group

Publication History: V1.0 For Consultation

Abstract:

This profile splits assurance into the four orthogonal components of the identifier uniqueness and the identity, authentication and attribute assurance. The Credential Service Provider assigns one or more values from one or more components to each credential and delivers the value(s) to the Relying Party in an assertion. Some values are also expressed as an Entity Attribute of an Identity Provider. For conformance to this profile, only meeting the baseline expectations for Identity Providers is required.

To serve the Relying Parties seeking for simplicity, the components are further collapsed to two assurance profiles (with the arbitrary names Cappuccino and Espresso) which cover all components. This profile also specifies how to represent the values using federated identity protocols, currently SAML 2.0.

Table of Contents

1. Terms and definitions ............................................................... 2
2. Assurance components ............................................................. 3
  2.1 Identifier uniqueness .................................................................. 3
  2.2 Identity proofing and credential issuance, renewal and replacement .................................. 4
  2.3 Authentication ............................................................................ 5
  2.4 Attribute quality and freshness .................................................. 5
3. Conformance criteria ........................................................................ 7
4. Assurance profiles ........................................................................... 8
5. Representation on federated protocols ............................................. 9
  5.1. Security Assertion Markup Language 2.0 (SAML) ........................................ 9
6. References ...................................................................................... 11

Appendix A: Local enterprise -- Good enough for internal systems ........... 12
Appendix B: Examples ........................................................................ 13
Example on assertions ........................................................................ 13
1. Terms and definitions

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Credential</td>
<td>A set of data presented as evidence of a claimed identity and/or entitlements [X.1254].</td>
</tr>
<tr>
<td>Credential Service Provider (CSP)</td>
<td>A trusted actor that issues and/or manages credentials [X.1254]. In the context of this specification, CSP refers to the Identity Provider and the associated Identity Management system that manages the user identities, attributes and authentication observed by the Relying Parties.</td>
</tr>
<tr>
<td>No re-assignment (of an identifier)</td>
<td>No re-assignment means that while a user can be assigned a new identifier value (such as, an eduPersonUniqueID attribute value [eduPerson]), the old value MUST NOT be recycled to another user. However, the identifier value can be assigned back to the same user (for instance, if a departed person later returns back to the organisation).</td>
</tr>
<tr>
<td>Relying Party (RP)</td>
<td>Actor that relies on an identity assertion or claim [X.1254].</td>
</tr>
</tbody>
</table>

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].

To assert the values defined in this profile to the RPs the CSPs will use URIs which has the following prefix: $PREFIX$=https://refeds.org/assurance.
2. Assurance components

This section introduces four assurance components which each represent a different aspect of assurance. The components are orthogonal i.e. a CSP can assert one or more values from different components independently. The value pertains to the user represented in the assertion and different users or the same user in different authenticated sessions can qualify to different values.

2.1 Identifier uniqueness

This component describes how a CSP expresses that an identifier represents a single natural person and if that person remains the same over time.

<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>$PREFIX$/ID/unique</td>
<td>- User account belongs to a single natural person</td>
</tr>
<tr>
<td></td>
<td>- The person and the credential they are assigned is traceable i.e. the CSP knows who they are and can contact them</td>
</tr>
<tr>
<td></td>
<td>- The user identifier will not be re-assigned</td>
</tr>
<tr>
<td></td>
<td>- The user identifier is one of these: eduPersonUniqueID, SAML2 persistent ID or eduPersonTargetedID</td>
</tr>
</tbody>
</table>

Within the REFEDS community there is a long legacy of using eduPersonPrincipalName (ePPN, [eduPerson]) attribute as a human-readable user identifier despite its undefined re-assignment practice. The table below defines two alternative values the CSP can use to indicate its ePPN re-assignment practice to the RPs that prefer to use ePPN.

The values are mutually exclusive. A CSP MAY assert one of them but MUST NOT assert several.

<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>$PREFIX$/ID/no-eppn-reassign</td>
<td>eduPersonPrincipalName values will not be re-assigned.</td>
</tr>
<tr>
<td>$PREFIX$/ID/eppn-reassign-1y</td>
<td>eduPersonPrincipalName values may be re-assigned after a hiatus period of 1 year or longer.</td>
</tr>
</tbody>
</table>

The intention is that:

---

1 eduPersonTargetedID is a legacy attribute. The use of the SAML 2.0 persistent nameID is encouraged, instead.
69  - if the Home organisation asserts unique and no-eppn-reassign, then also the
ePPN attribute value shares the same uniqueness properties as
eduPersonUniqueID (ePUID, [eduPerson]), SAML2 persistent ID and
eduPersonTargetedID (ePTID, [eduPerson]).
70  - If the Home organisation asserts unique only, an ePPN value released by it is
not assumed to fulfill the uniqueness property.
71  - A user may have more than one ePPN at one time or over time, but non re-
assignment means that the same ePPN value shall never refer to two different
users.

The expected Relying Party behaviour for observing ePPN re-assignment:

80  - If the Home organisation asserts no-eppn-reassign, the Relying party knows
that when it observes a given ePPN value it will always belong to the same
individual.
81  - If the Home organisation asserts eppn-reassign-ly, the Relying party knows
that if an ePPN holder doesn’t show up for one year, the ePPN holder may
have been changed. A safe practice for the Relying Party is to close a user
account or remove the ePPN value associated to it if the user hasn’t logged in
for one year.
82  - If the Home Organisation asserts neither no-eppn-reassign nor eppn-
reassign-ly, the Relying Party cannot rely on ePPN as a unique user identifier
but should use it only in combination with another identifier that is unique
(such as ePTID, SAML2 persistent nameID or ePUID).

2.2 Identity proofing and credential issuance, renewal and
replacement

This section describes the requirements for:

97  - Identity Proofing, which is the process by which the CSP captures and verifies
sufficient information to identify a user to a specified or understood level of
assurance [X.1254].
98  - Credential issuance, which is the process of providing or otherwise associating
a user with a particular credential, or the means to produce a credential
[X.1254].
99  - Renewal, which is the process whereby the life of an existing credential is
extended [X.1254].
100  - Replacement, which is the process whereby a user is issued a new credential,
or a means to produce a credential, to replace a previously issued credential
that has been revoked [X.1254].

These values are incremental i.e. constitute an ordered set of levels with increasing
requirements. The CSP asserting a value MUST also assert all preceding values (i.e. a
CSP asserting assumed must also assert local-enterprise and a CSP
asserting verified must also assert assumed and local-enterprise for a
given user).

<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>$PREFIX$/IAP/local-enterprise</td>
<td>The identity proofing and credential issuance, renewal and replacement are done in a way that is less than assumed but qualifies (or would qualify) the user to access the Home Organisation’s internal administrative systems (see appendix A).</td>
</tr>
<tr>
<td>$PREFIX$/IAP/assumed</td>
<td>Identity proofing and credential issuance, renewal, and replacement qualify to any of - sections 5.2.2-5.2.2.9, section 5.2.2.12 and section 5.2.3 of Kantara assurance level 2 [Kantara SAC] - IGTF level BIRCH [IGTF] - section 2.1.2, section 2.2.2 and section 2.2.4 of eIDAS assurance level low [eIDAS LoA]</td>
</tr>
<tr>
<td>$PREFIX$/IAP/verified</td>
<td>Identity proofing and credential issuance, renewal, and replacement qualifies to any of - section 5.3.2-5.3.2.9, section 5.3.2.12 and 5.3.3 of Kantara assurance level 3 [Kantara SAC] - section 2.1.2, section 2.2.2 and section 2.2.4 of eIDAS assurance level substantial [eIDAS LoA]</td>
</tr>
</tbody>
</table>

### 2.3 Authentication

This section describes the requirements for the user authentication. These values are incremental.

<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Placeholder for a reference to REFEDS authentication context definition for good-entropy</td>
<td></td>
</tr>
<tr>
<td><a href="https://refeds.org/profile/mfa">https://refeds.org/profile/mfa</a></td>
<td>Placeholder for a reference to REFEDS MFA Profile Recommendation (once agreed on and published).</td>
</tr>
</tbody>
</table>

### 2.4 Attribute quality and freshness

This section describes the requirements for the quality and freshness of the attributes (other than the unique identifier) the CSP delivers to the RP.

The requirements are limited to the eduPersonAffiliation and eduPersonScopedAffiliation attributes defined in [eduPerson]. The freshness of eduPersonAffiliation and eduPersonScopedAffiliation are further limited to
the following attribute values: faculty, student and member\(^2\). Other values and attributes are out of scope.

The freshness of eduPersonAffiliation and eduPersonScopedAffiliation intends to serve the RPs who want to couple their users’ access rights with their continuing institutional role.

<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>$PREFIX$/ATP/ePA-1m</td>
<td>eduPersonAffiliation and eduPersonScopedAffiliation attributes (if populated) reflect user’s departure within 30 days time</td>
</tr>
</tbody>
</table>

"A departure" takes place when the organisation decides that the user doesn’t have a continuing basis for the affiliation value (i.e., can no longer speak for the organisation in that role). The practices here may vary; for instance:

- In some organisations a researcher ceases to be a faculty member the day their employment or other contract ends, in some organisations there is a defined grace period.
- In some universities a student ceases to be a student the day they graduate, in some organisations the student status remains effective until the end of the semester.

This value is intended to indicate only that there is a maximum latency of one month for the CSP’s identity management system to reflect the user’s affiliation change in their attributes.

Notice also that this section does not require that the departing user’s account must be closed; only that the affiliation attribute value as observed by the RPs is updated.

---

\(^2\) Values faculty, student and member appear to be used consistently across federations [ePSA Comparison].
3. Conformance criteria

For a CSP to conform to this profile 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 to 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 site technical, admin, and security contacts, MDUI information.

A CSP indicates its conformance to this profile by asserting $PREFIX$. 
4. Assurance profiles

To serve the RPs seeking for simplicity, this section collapses the components presented in section 2 into two assurance profiles Cappuccino and Espresso.

The CSPs who populate the assurance assertions presented in the section 2 MUST populate also all assurance profiles to which they qualify.

A CSP that asserts the assurance profile Espresso MUST assert also the assurance profile Cappuccino.

The table below defines the following assurance profiles:

- Assurance profile Cappuccino for low-risk research use cases
  ($PREFIX$/profile/cappuccino)
- Assurance profile Espresso for use cases requiring verified identity and two factor authentication ($PREFIX$/profile/espresso)

<table>
<thead>
<tr>
<th>Value</th>
<th>Cappuccino</th>
<th>Espresso</th>
</tr>
</thead>
<tbody>
<tr>
<td>$PREFIX$/ID/unique</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>$PREFIX$/ID/no-eppn-reassign</td>
<td></td>
<td></td>
</tr>
<tr>
<td>$PREFIX$/ID/eppn-reassign-lyr</td>
<td></td>
<td></td>
</tr>
<tr>
<td>$PREFIX$/IAP/local-enterprise</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>$PREFIX$/IAP/assumed</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>$PREFIX$/IAP/verified</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>$PREFIX$/AAP/good-entropy</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td><a href="https://refeds.org/profile/mfa">https://refeds.org/profile/mfa</a></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>$PREFIX$/ATP/ePA-1m</td>
<td>X</td>
<td>X</td>
</tr>
</tbody>
</table>

For instance, if a user qualifies to all values required according to the column “Espresso” (including their multi-factor authentication was performed during the session) the CSP MUST assert also both Espresso and Cappuccino for this user.

However, if multi-factor authentication was omitted and authentication qualifying only to good-entropy was carried out during the session, the CSP MUST assert Cappuccino and MUST NOT assert Espresso.
5. Representation on federated protocols

This section specifies how the values presented in the previous section shall be represented using federated identity protocols.

5.1. Security Assertion Markup Language 2.0 (SAML)

The table below presents how this assurance profile is represented using the SAML framework. Following presentations are used:

- `eduPersonAssurance` attribute, as defined in [eduPerson].
- `AuthenticationContextClassRef`, as defined in section 2.7.2.2. of [SAML Core].
- `SAML2 metadata entity attributes`, using the EntityAttribute name “urn:oasis:names:tc:SAML:attribute:assurance-certification” [TO BE DONE]

<table>
<thead>
<tr>
<th>Value</th>
<th>eduPerson Assurance</th>
<th>AuthenticationContextClassRef</th>
<th>SAML2 Metadata entity attribute</th>
</tr>
</thead>
<tbody>
<tr>
<td>$PREFIX$/ID/unique</td>
<td>X</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>$PREFIX$/ID/no-eppn-reassign</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>$PREFIX$/ID/eppn-reassign-ly</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>$PREFIX$/IAP/local-enterprise</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>$PREFIX$/IAP/assumed</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>$PREFIX$/IAP/verified</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>$PREFIX$/AAP/good-entropy</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td><a href="https://refeds.org/profile/mfa">https://refeds.org/profile/mfa</a></td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>$PREFIX$/ATP/ePA-1m</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>$PREFIX$/profile/cappuccino</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>$PREFIX$/profile/espresso</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
</tbody>
</table>

The CSPs are expected to populate the `$PREFIX/AP/cappuccino` and `$PREFIX/AP/espresso` metadata entity attributes if they are capable of fulfilling those profiles at least for a subset of their users. The Relying Parties can make use of that information to manage their list of CSPs who can provide assurance that meets their requirements.
The CSP MUST present the values a particular authenticated user qualifies to in an assertion which the Relying Parties are advised to observe.
6. References


ePSA Comparison Cormack, A., Linden, M. REFEDs ePSA usage comparison, version 0.13. https://blog.refeds.org/wp-content/uploads/2015/05/ePSAcomparison_0_13.pdf


RFC2119 Bradner, S. Key words for use in RFCs to Indicate Requirement Levels. RFC2119. https://www.ietf.org/rfc/rfc2119.txt


Appendix A: Local enterprise -- Good enough for internal systems

Some of the components in section 2 define an assurance level implicitly by a statement that the Level of assurance is good enough for accessing the Home Organisation's internal systems. This relies on the assumption that if the Home Organisation deems the assurance level good enough for accessing internal systems locally in the Home Organisation, the assurance level may be good enough for accessing some external resources, too. It is assumed that the Home Organisation has made a risk based decision on what exactly are the assurance level requirements for those accounts.

Home Organisations may have several internal systems with varying assurance level requirements. It is assumed that the Home Organisation’s internal systems referred to here could be:

- The ones that deal with money (for instance, travel expense management systems or invoice circulation systems).
- The ones that deal with some employment-related personal data (for instance, employee self-service interfaces provided by the Human Resources systems).
- The ones that deal with student information (for instance, administrative access to the student information system).
Appendix B: Examples

Example on assertions

A university who guarantees that its faculty members:

- Have unique ePUID values
- Are ID-proofed face-to-face using government-issued photo-ID
- Authenticate with passwords of good entropy
- eduPersonAffiliation value reflects their departure or role change promptly
- Identity management system qualifies to the baseline expectations for Identity Providers

Will assert to its faculty members the following multi-valued assurance assertion:

- $PREFIX$
- $PREFIX$/ID/unique
- $PREFIX$/IAP/local-enterprise
- $PREFIX$/IAP/assumed
- $PREFIX$/AAP/good-entropy
- $PREFIX$/ATP/ePA-1m
- $PREFIX$/profile/cappuccino

Examples on SAML authentication contexts

The XML namespaces used in the examples:

- samlp="urn:oasis:names:tc:SAML:2.0:protocol"
- saml="urn:oasis:names:tc:SAML:2.0:assertion"

Example 1: An SP requests good-entropy

An SP requests good-entropy (Comparison attribute present):

```
<samlp:RequestedAuthnContext Comparison="exact">
  <saml:AuthnContextClassRef>
    https://refeds.org/assurance/AAP/good-entropy
  </saml:AuthnContextClassRef>
</samlp:RequestedAuthnContext>
```

An IdP responds good-entropy:

```
<saml:AuthnContext>
  <saml:AuthnContextClassRef>
    https://refeds.org/assurance/AAP/good-entropy
  </saml:AuthnContextClassRef>
</saml:AuthnContext>
```

Alternatively, an IdP responds that it cannot satisfy the request:

```
<samlp:Status>
  <samlp:StatusCode
```
Example 2: An SP prefers MFA but accepts good-entropy

An SP presents a list of authentication contexts in the order of preference:

(Comparison attribute omitted, applying the default value "exact"): 

```xml
<samlp:RequestedAuthnContext>
  <saml:AuthnContextClassRef>
    https://refeds.org/profile/mfa
  </saml:AuthnContextClassRef>
  <saml:AuthnContextClassRef>
    https://refeds.org/assurance/AAP/good-entropy
  </saml:AuthnContextClassRef>
</samlp:RequestedAuthnContext>

An IdP responds good-entropy:

```xml
<saml:AuthnContext>
  <saml:AuthnContextClassRef>
    https://refeds.org/assurance/AAP/good-entropy
  </saml:AuthnContextClassRef>
</saml:AuthnContext>