REFEDS Assurance Framework ver 1.0 (DRAFT 2 May 2018)

REFEDS Assurance working group

Abstract

The Relying Parties of the research and education federations need to make decisions on how much to trust the assertions made by the Identity Providers and their back-end Credential Service Providers. This document introduces a framework for assurance and its expression using common identity federation protocols.

This framework splits assurance into the three orthogonal components of the identifier uniqueness and the identity and attribute assurance. The assurance of authentication is not covered by this specification. 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. For conformance to this framework, 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 framework also specifies how to represent the values using federated identity protocols, currently SAML 2.0 and OpenID Connect.

Table of Contents

1. Terms and definitions

Term	Definition
Credential	A set of data presented as evidence of a claimed identity and/or entitlements [X.1254].
Credential Service Provider (CSP)	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 and attributes observed by the Relying Parties.
No re-assignment (of an identifier)	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).
Relying Party (RP)	Actor that relies on an identity assertion or claim [X.1254].

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 have the following prefix:

```
$PREFIX$=https://refeds.org/assurance
```

2. Assurance components

This section introduces three 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 can qualify to different values.

This framework does not define the assurance of user authentication. See Appendix C for more information on REFEDS specifications for user authentication.

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.

Value	Description
`$PREFIX$/ID/unique`	- User account belongs to a single natural person - CSP can contact the person to whom the account is issued - The user identifier will not be re-assigned - The user identifier is eduPersonUniqueID, OpenID Connect sub (type: public) or one of the pairwise identifiers recommended by REFEDS[1]

In addition to the identifiers mentioned in the definition of `unique`, 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[2] that a CSP declaring `unique` can use to indicate the extent to which this applies to ePPN.

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

Value	Description
`$PREFIX$/ID/no-eppn-reassign`	eduPersonPrincipalName values will not be re-assigned.
`$PREFIX$/ID/eppn-reassign-1y`	eduPersonPrincipalName values may be re-assigned after a hiatus period of 1 year or longer.

The intention is that

- if the Home organisation asserts `unique` and `no-eppn-reassign`, then the ePPN attribute value also shares the same uniqueness properties as eduPersonUniqueID (ePUID).
- If the Home organisation asserts `unique` only, an ePPN value released by it is not assumed to fulfill the uniqueness property

[1] eduPersonTargetedID is a legacy attribute. When considering eduPersonTargetedID,the use of the SAML 2.0 persistent nameID is encouraged, instead. See the accompanying documentation for more information.

[2] There may be also other specifications that address the ePPN re-assignment practices. It is the responsibility of those making the assertions to ensure that the assertions do not conflict with any other specifications. For the list of current REFEDS specifications, see https://refeds.org/specifications

- 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

- 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
- If the Home organisation asserts `eppn-reassign-1y`, 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.The Relying Party can also use some out-of-band mechanism to verify whether the user is still the same person.
- If the Home Organisation asserts neither `no-eppn-reassign` nor `eppn-reassign-1y`, 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 ePUID).

Finally, the reader is reminded that they should not assume any uniqueness property that goes beyond the specification of the attribute. For instance, a Relying Party should not assume that the holder of an ePPN value is the receiver of an email message sent using the ePPN value as the receiver address.

2.2. Identity proofing and credential issuance, renewal and replacement

This section describes the requirements for

- 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].
- 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].
- Renewal, which is the process whereby the life of an existing credential is extended [X.1254].
- 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 `high` MUST also assert (and comply with) the value `medium` and `low` for a given user. The CSP asserting a value `medium` MUST also assert (and comply with) the value `low` for a given user.

Value	**Description**
`$PREFIX$/IAP/low`	Identity proofing and credential issuance, renewal, and replacement qualify to any of - sections 5.1.2-5.1.2.9 and section 5.1.3 of Kantara assurance

	level 1 [Kantara SAC] - IGTF level DOGWOOD [IGTF] - IGTF level ASPEN [IGTF]
`$PREFIX$/IAP/medium`	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] - IGTF level CEDAR [IGTF] - section 2.1.2, section 2.2.2 and section 2.2.4 of eIDAS assurance level low [eIDAS LoA]
`$PREFIX$/IAP/high`	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]

A CSP MAY also assert the following value independent of the values above:

Value	**Description**
`$PREFIX$/IAP/local-enterprise`	The identity proofing and credential issuance, renewal and replacement are done in a way that qualifies (or would qualify) the user to access the Home Organisation's internal administrative systems (see appendix A).

2.3. 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, eduPersonScopedAffiliation and eduPersonPrimaryAffiliation attributes defined in [eduPerson]. The freshness of the attribute is further limited to the following attribute values: faculty, student and member[3]. Other values and attributes are out of scope.

[3] Values faculty, student and member appear to be used consistently across federations [ePSA Comparison].

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

The values are hierarchical. A CSP which asserts `$PREFIX$/ATP/ePA-1d` MUST assert also `$PREFIX$/ATP/ePA-1m` for a given user.

Value	Description
`$PREFIX$/ATP/ePA-1m`	eduPersonAffiliation, eduPersonScopedAffiliation and eduPersonPrimaryAffiliation attributes (if populated and released to the RP) reflect user's departure within 30 days time
`$PREFIX$/ATP/ePA-1d`	eduPersonAffiliation, and eduPersonScopedAffiliation and eduPersonPrimaryAffiliation attributes (if populated and released to the RP) reflect user's departure within one days time

"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 or one day 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.

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 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

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 and 3 into two assurance profiles Cappuccino and Espresso.

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

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 (`$PREFIX$/profile/espresso`)

A CSP qualifies to a profile if it asserts (and complies with) all the values marked as ‘X’ in the column.

Value	Cappuccino	Espresso
`$PREFIX$`	X	X
`$PREFIX$/ID/unique`	X	X
`$PREFIX$/ID/no-eppn-reassign`		
`$PREFIX$/ID/eppn-reassign-1yr`		
`$PREFIX$/IAP/low`	X	X
`$PREFIX$/IAP/medium`	X	X
`$PREFIX$/IAP/high`		X
`$PREFIX$/IAP/local-enterprise`		
`$PREFIX$/ATP/ePA-1m`	X (*)	X (*)
`$PREFIX$/ATP/ePA-1d`		

(*) The CSP can omit this requirement if it doesn’t populate and release the attribute values defined in section 2.3 for this user.

For instance, if a user qualifies to all values required according to the column “Espresso” the CSP SHOULD assert Espresso for this user.

Notice that the assurance profiles do not cover the authentication assurance of the user session. The deployers are encouraged to use the profiles in conjunction with specifications focusing on authentication. See Appendix C for REFEDS profiles on authentication assurance.

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)

In SAML, this assurance framework is represented using the multi-valued **eduPersonAssurance** attribute, as defined in [eduPerson]. See Appendix B for examples.

5.2. OpenID Connect (OIDC)

In OIDC, this assurance framework is represented using the multi-valued **eduPersonAssurance** claim, as defined in [REFEDS OIDCre]. See Appendix B for examples.

6. References

eduPerson	Internet2/MACE. eduPerson Object Class Specification (201602). http://software.internet2.edu/eduperson/internet2-mace-dir-eduperson-201602.html
eIDAS LoA	European Commission. Commission Implementing Regulation (EU) 2015/1502 of 8 September 2015 on setting out minimum technical specifications and procedures for assurance levels for electronic identification means. http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:JOL_2015_235_R_0002
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
IGTF	Groep, D (editor). IGTF Levels of Authentication Assurance, version 1.0. https://www.igtf.net/ap/authn-assurance/
Kantara SAC	Kantara Initiative. Kantara Identity Assurance Framework. Kantara IAF-1400 Service Assessment Criteria v5.0. https://kantarainitiative.org/confluence/display/LC/Identity+Assurance+Framework
REFEDS	OpenID Connect for Research and Education Working Group. Mapping

OIDCre	SAML attributes to OIDC Claims. Referenced 9 February 2018. https://wiki.refeds.org/display/GROUPS/Mapping+SAML+attributes+to+OIDC+Claims
RFC2119	Bradner, S. Key words for use in RFCs to Indicate Requirement Levels. RFC2119. https://www.ietf.org/rfc/rfc2119.txt
X.1254	International Telecommunication Union. Series X. Data Networks, Open System Communication and Security. Cyberspace security – Identity management. Entity authentication assurance framework. Standard X.1254.https://www.itu.int/rec/T-REC-X.1254

198

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 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
- eduPerson affiliation value(s) 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/low`
- `$PREFIX$/IAP/medium`
- `$PREFIX$/IAP/high`
- `$PREFIX$/ATP/ePA-1m`
- `$PREFIX$/ATP/ePA-1d`
- `$PREFIX$/profile/cappuccino`

Appendix C: Examples on Authentication Assurance

The REFEDS Assurance Framework does not cover the authentication assurance of the user. The deployers are encouraged to use the framework in conjunction with specifications focusing on authentication.

REFEDS has published profiles on authentication assurance, such as

- REFEDS Multi-Factor Authentication (MFA) Profile (https://refeds.org/profile/mfa)
- REFEDS Single-Factor Authentication (SFA) Profile (https://refeds.org/profile/sfa)

Below are examples on how these profiles can be used in conjunction with the REFEDS Assurance Framework.

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 Multi-factor authentication

An SP requests multi-factor authentication (Comparison attribute present):

```
<samlp:RequestedAuthnContext Comparison="exact">
   <saml:AuthnContextClassRef>
      https://refeds.org/profile/mfa
   </saml:AuthnContextClassRef>
</samlp:RequestedAuthnContext>
```

An IdP responds multi-factor authentication:

```
<saml:AuthnContext>
   <saml:AuthnContextClassRef>
      https://refeds.org/profile/mfa
  </saml:AuthnContextClassRef>
</saml:AuthnContext>
```

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

```
<samlp:Status>
  <samlp:StatusCode
  Value="urn:oasis:names:tc:SAML:2.0:status:NoAuthnContext”/>
</samlp:Status>
```

Example 2: An SP prefers MFA but accepts single-factor authentication

An SP presents a list of authentication contexts in the order of preference (Comparison attribute omitted, applying the default value “`exact`”):

```
<samlp:RequestedAuthnContext>
   <saml:AuthnContextClassRef>
      https://refeds.org/profile/mfa
   </saml:AuthnContextClassRef>
   <saml:AuthnContextClassRef>
      https://refeds.org/profile/sfa
   </saml:AuthnContextClassRef>
</samlp:RequestedAuthnContext>
```

An IdP responds single-factor authentication:

```
<saml:AuthnContext>
   <saml:AuthnContextClassRef>
      https://refeds.org/profile/sfa
  </saml:AuthnContextClassRef>
</saml:AuthnContext>
```

Examples on OIDC acr claims

Example 1: An RP requests multi-factor authentication

An RP issues a claims request, with “essential”:true qualifier as defined in [OIDC Core, section 5.5]:

```
 {
   "id_token":
    {
     "acr": {"essential": true,
            "value": "https://refeds.org/profile/mfa"}
    }
  }
```

An OP responds with an ID token indicating MFA:

```
 {
   "iss": "https://server.example.com",
   "sub": "24400320",
   "aud": "s6BhdRkqt3",
   "nonce": "n-0S6_WzA2Mj",
   "exp": 1311281970,
   "iat": 1311280970,
   "auth_time": 1311280969,
   "acr": "https://refeds.org/profile/mfa"
  }
```

Alternatively, an OP responds to the client that it cannot satisfy the request[4]:

```
 HTTP/1.1 302 Found
  Location: https://client.example.org/cb?
    error=invalid_request
&error_description=The%20specified%20authentication%20context%20requir
ements%20cannot%20be%20met%20by%20the%20responder.
    &state=af0ifjsldkj
```

Example 2: An RP prefers MFA but accepts SFA

An RP issues a claims request with a list of authentication contexts in the order of preference and “essential”:true qualifier as defined in [OIDC Core, section 5.5]:

```
 {
   "id_token":
    {
     "acr": {"essential": true,
            "values": ["https://refeds.org/profile/mfa",
                       "https://refeds.org/profile/sfa"]}
    }
  }
```

An OP responds with an ID token indicating SFA:

```
 {
   "iss": "https://server.example.com",
   "sub": "24400320",
   "aud": "s6BhdRkqt3",
   "nonce": "n-0S6_WzA2Mj",
   "exp": 1311281970,
   "iat": 1311280970,
   "auth_time": 1311280969,
   "acr": "https://refeds.org/profile/sfa"
  }
```

[4] Currently there is no standard error code to signal OP’s inability to satisfy the requested authentication context. A dedicated error code may be later published by competent specification bodies.