

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28  
29  
30  
31  
32  
33  
34  
35

# 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



36

37 **1. Terms and definitions**

<b>Term</b>	<b>Definition</b>
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, attributes and authentication 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].

38

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

42

43 To assert the values defined in this profile to the RPs the CSPs will use URIs which  
44 has the following prefix: \$PREFIX\$=<https://refeds.org/assurance>.

45

## 46 2. Assurance components

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

### 52 2.1 Identifier uniqueness

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

55

Value	Description
\$PREFIX\$/ID/unique	<ul style="list-style-type: none"> <li>- User account belongs to a single natural person</li> <li>- The person and the credential they are assigned is traceable i.e. the CSP knows who they are and can contact them</li> <li>- The user identifier will not be re-assigned</li> <li>- The user identifier is one of these: eduPersonUniqueID, SAML2 persistent ID or eduPersonTargetedID<sup>1</sup></li> </ul>

56

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

62

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

65

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.

66

67 The intention is that:

68

---

<sup>1</sup> 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  
70 ePPN attribute value shares the same uniqueness properties as  
71 `eduPersonUniqueID` (`ePUIID`, [`eduPerson`]), SAML2 persistent ID and  
72 `eduPersonTargetedID` (`ePTID`, [`eduPerson`]).  
73 - If the Home organisation asserts `unique` only, an ePPN value released by it is  
74 not assumed to fulfill the uniqueness property.  
75 - A user may have more than one ePPN at one time or over time, but non re-  
76 assignment means that the same ePPN value shall never refer to two different  
77 users.

78

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

80

- 81 - If the Home organisation asserts `no-eppn-reassign`, the Relying party knows  
82 that when it observes a given ePPN value it will always belong to the same  
83 individual.  
84 - If the Home organisation asserts `eppn-reassign-1y`, the Relying party knows  
85 that if an ePPN holder doesn't show up for one year, the ePPN holder may  
86 have been changed. A safe practice for the Relying Party is to close a user  
87 account or remove the ePPN value associated to it if the user hasn't logged in  
88 for one year.  
89 - If the Home Organisation asserts neither `no-eppn-reassign` nor `eppn-`  
90 `reassign-1y`, the Relying Party cannot rely on ePPN as a unique user identifier  
91 but should use it only in combination with another identifier that is unique  
92 (such as `ePTID`, SAML2 persistent nameID or `ePUIID`).

## 93 2.2 Identity proofing and credential issuance, renewal and 94 replacement

95

96 This section describes the requirements for:

97

- 98 - Identity Proofing, which is the process by which the CSP captures and verifies  
99 sufficient information to identify a user to a specified or understood level of  
100 assurance [X.1254].  
101 - Credential issuance, which is the process of providing or otherwise associating  
102 a user with a particular credential, or the means to produce a credential  
103 [X.1254].  
104 - Renewal, which is the process whereby the life of an existing credential is  
105 extended [X.1254].  
106 - Replacement, which is the process whereby a user is issued a new credential,  
107 or a means to produce a credential, to replace a previously issued credential  
108 that has been revoked [X.1254].  
109

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

114 given user).

115

Value	Description
\$PREFIX\$/IAP/local-enterprise	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).
\$PREFIX\$/IAP/assumed	Identity proofing and credential issuance, renewal, and replacement qualify to any of <ul style="list-style-type: none"> <li>- 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]</li> <li>- IGTF level BIRCH [IGTF]</li> <li>- section 2.1.2, section 2.2.2 and section 2.2.4 of eIDAS assurance level low [eIDAS LoA]</li> </ul>
\$PREFIX\$/IAP/verified	Identity proofing and credential issuance, renewal, and replacement qualifies to any of <ul style="list-style-type: none"> <li>- section 5.3.2-5.3.2.9, section 5.3.2.12 and 5.3.3 of Kantara assurance level 3 [Kantara SAC]</li> <li>- section 2.1.2, section 2.2.2 and section 2.2.4 of eIDAS assurance level substantial [eIDAS LoA]</li> </ul>

116

## 117 2.3 Authentication

118

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

121

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

122

## 123 2.4 Attribute quality and freshness

124

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

127

128 The requirements are limited to the eduPersonAffiliation and  
 129 eduPersonScopedAffiliation attributes defined in [eduPerson]. The freshness  
 130 of eduPersonAffiliation and eduPersonScopedAffiliation are further limited to

131 the following attribute values: faculty, student and member<sup>2</sup>. Other values and  
132 attributes are out of scope.

133  
134 The freshness of eduPersonAffiliation and eduPersonScopedAffiliation intends to serve  
135 the RPs who want to couple their users' access rights with their continuing  
136 institutional role.  
137

Value	Description
\$PREFIX\$/ATP/ePA-1m	eduPersonAffiliation and eduPersonScopedAffiliation attributes (if populated) reflect user's departure within 30 days time

138  
139 "A departure" takes place when the organisation decides that the user doesn't have a  
140 continuing basis for the affiliation value (i.e., can no longer speak for the organisation  
141 in that role). The practices here may vary; for instance:

- 142
- 143 - In some organisations a researcher ceases to be a faculty member the day  
144 their employment or other contract ends, in some organisations there is a  
145 defined grace period.
  - 146 - In some universities a student ceases to be a student the day they graduate,  
147 in some organisations the student status remains effective until the end of the  
148 semester.

149  
150 This value is intended to indicate only that there is a maximum latency of one month  
151 for the CSP's identity management system to reflect the user's affiliation change in  
152 their attributes.

153  
154 Notice also that this section does not require that the departing user's account must  
155 be closed; only that the affiliation attribute value as observed by the RPs is updated.

---

<sup>2</sup> Values faculty, student and member appear to be used consistently across federations [ePSA Comparison].

156

157 **3. Conformance criteria**

158 For a CSP to conform to this profile it is REQUIRED to conform to the following  
159 baseline expectations for Identity Providers:

160

- 161 1. The Identity Provider is operated with organizational-level authority.
- 162 2. The Identity Provider is trusted enough to be used to access the organization's  
163 own systems.
- 164 3. Generally-accepted security practices are applied to the Identity Provider.
- 165 4. Federation metadata is accurate, complete, and includes site technical, admin,  
166 and securitybcontacts, MDUI information.

167

168 A CSP indicates its conformance to this profile by asserting \$PREFIX\$.

169

## 170 4. Assurance profiles

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

173

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

176

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

179

180 The table below defines the following assurance profiles:

181

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

186

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

187

188 For instance, if a user qualifies to all values required according to the column  
 189 "Espresso" (including their multi-factor authentication was performed during the  
 190 session) the CSP MUST assert also both Espresso and Cappuccino for this user.  
 191 However, if multi-factor authentication was omitted and authentication qualifying only  
 192 to `good-entropy` was carried out during the session, the CSP MUST assert  
 193 Cappuccino and MUST NOT assert Espresso.



194

 195 **5. Representation on federated protocols**

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

 198 **5.1. Security Assertion Markup Language 2.0 (SAML)**

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

- 201
- 202 • **eduPersonAssurance** attribute, as defined in [eduPerson].
  - 203 • **AuthenticationContextClassRef**, as defined in section 2.7.2.2. of [SAML Core].
  - 204 • **SAML2 metadata entity attributes**, using the EntityAttribute name  
 205 "urn:oasis:names:tc:SAML:attribute:assurance-certification" [**TO BE DONE**]
- 206

Value	eduPerson Assurance	Authentica tionConte xtClassRef	SAML2 Metadata entity attribute
\$PREFIX\$			X
\$PREFIX\$/ID/unique	X		
\$PREFIX\$/ID/no-eppn-reassign	X		
\$PREFIX\$/ID/eppn-reassign-1y	X		
\$PREFIX\$/IAP/local-enterprise	X		
\$PREFIX\$/IAP/assumed	X		
\$PREFIX\$/IAP/verified	X		
\$PREFIX\$/AAP/good-entropy		X	
<a href="https://refeds.org/profile/mfa">https://refeds.org/profile/mfa</a>		X	
\$PREFIX\$/ATP/ePA-1m	X		
\$PREFIX\$/profile/cappuccino	X		X
\$PREFIX\$/profile/espresso	X		X

207

 208 The CSPs are expected to populate the \$PREFIX/AP/cappuccino and  
 209 \$PREFIX/AP/espresso metadata entity attributes if they are capable of fulfilling those  
 210 profiles at least for a subset of their users. The Relying Parties can make use of that  
 211 information to manage their list of CSPs who can provide assurance that  
 212 meets their requirements.

213

214 The CSP MUST present the values a particular authenticated user qualifies to in an  
215 assertion which the Relying Parties are advised to observe.

216

217 **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](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](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>
- RFC2119 Bradner, S. Key words for use in RFCs to Indicate Requirement Levels. RFC2119. <https://www.ietf.org/rfc/rfc2119.txt>
- SAML Core Cantor, S., Kemp, K., Philpott, R., Maler, E (editors). Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0. OASIS Standard. <http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf>
- 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>

218

## 219 **Appendix A: Local enterprise -- Good enough for** 220 **internal systems**

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

229  
230 Home Organisations may have several internal systems with varying assurance level  
231 requirements. It is assumed that the Home Organisation's internal systems referred  
232 to here could be:

- 233
- 234 - The ones that deal with money (for instance, travel expense management  
235 systems or invoice circulation systems).
  - 236 - The ones that deal with some employment-related personal data (for instance,  
237 employee self-service interfaces provided by the Human Resources systems).
  - 238 - The ones that deal with student information (for instance, administrative  
239 access to the student information system).

## 240 Appendix B: Examples

### 241 Example on assertions

242 A university who guarantees that its faculty members:

243

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

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

- 251 • \$PREFIX\$
  - 252 • \$PREFIX\$/ID/unique
  - 253 • \$PREFIX\$/IAP/local-enterprise
  - 254 • \$PREFIX\$/IAP/assumed
  - 255 • \$PREFIX\$/AAP/good-entropy
  - 256 • \$PREFIX\$/ATP/ePA-1m
  - 257 • \$PREFIX\$/profile/cappuccino
- 258 Examples on SAML authentication contexts

259 The XML namespaces used in the examples:

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

262

### 263 Example 1: An SP requests good-entropy

264

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

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

271

272 An IdP responds good-entropy:

```
273 <saml:AuthnContext>
274   <saml:AuthnContextClassRef>
275     https://refeds.org/assurance/AAP/good-entropy
276   </saml:AuthnContextClassRef>
277 </saml:AuthnContext>
```

278

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

```
280 <samlp:Status>
281   <samlp:StatusCode
```

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

284

### 285 **Example 2: An SP prefers MFA but accepts good-entropy**

286

287 An SP presents a list of authentication contexts in the order of preference  
288 (Comparison attribute omitted, applying the default value "exact"):

```
289 <samlp:RequestedAuthnContext>
290     <saml:AuthnContextClassRef>
291         https://refeds.org/profile/mfa
292     </saml:AuthnContextClassRef>
293     <saml:AuthnContextClassRef>
294         https://refeds.org/assurance/AAP/good-entropy
295     </saml:AuthnContextClassRef>
296 </samlp:RequestedAuthnContext>
```

297

298 An IdP responds good-entropy:

```
299 <saml:AuthnContext>
300     <saml:AuthnContextClassRef>
301         https://refeds.org/assurance/AAP/good-entropy
302     </saml:AuthnContextClassRef>
303 </saml:AuthnContext>
```

304