

TITLE / REFERENCE: REFEDS ASSURANCE FRAMEWORK v1.0

REFEDS Assurance Framework v1.0

2	REE	FDS	Assurance	working	aroun
3	KEL	ヒレる	Assurance	WOLKILIG	group

4 Publication History: V1.0 For Consultation

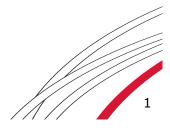
Abstract:

 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.

19 Table of Contents

21	1. Terms and definitions	2
22	2. Assurance components	3
23	2.1 Identifier uniqueness	3
24	2.2 Identity proofing and credential issuance, renewal and replacement	4
25	2.3 Authentication	5
26	2.4 Attribute quality and freshness	5
27	3. Conformance criteria	
28	4. Assurance profiles	8
29	5. Representation on federated protocols	
30	5.1. Security Assertion Markup Language 2.0 (SAML)	9
31	6. References	11
32	Appendix A: Local enterprise Good enough for internal systems	12
33	Appendix B: Examples	13
34	Example on assertions	13



37



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, 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", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].

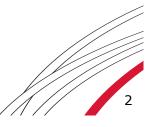
41 42

44

40

43 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.





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
- authenticated sessions can qualify to different values.

52 **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.

54 55

53

Value	Description	
\$PREFIX\$/ID/unique	 User account belongs to a single natural person The person and the credential they are assigned is traceable i.e. the CSP knows who they are and can contact them The user identifier will not be re-assigned The user identifier is one of these: eduPersonUniqueID, SAML2 persistent ID or eduPersonTargetedID¹ 	

56 57

58

59

60

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.

616263

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

64 assert several.

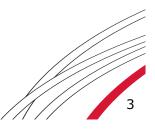
65

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

66 67

The intention is that:

¹ eduPersonTargetedID is a legacy attribute. The use of the SAML 2.0 persistent nameID is encouraged, instead.





70 71

72

73

74

75

76

77

78 79

80 81

82

83

84

85

86

87 88

89

90

91

92

93

94 95 96

97 98

99

100

101

102

103

104

105

106

107

108

109

110 111

112

113

- 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]).
- If the Home organisation asserts unique only, an ePPN value released by it is not assumed to fulfill the uniqueness property.
- A user may have more than one ePPN at one time or over time, but non reassignment means that the same ePPN value shall never refer to two different users.

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

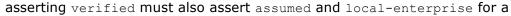
- If the Home organisation asserts no-eppn-reassign, the Relying party knows that when it observes a given ePPN value it will always belong to the same individual.
- If the Home organisation asserts eppn-reassign-1y, the Relying party knows that if an ePPN holder doesn't show up for one year, the ePPN 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.
- If the Home Organisation asserts neither no-eppn-reassign nor eppnreassign-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 ePTID, SAML2 persistent nameID or ePUID).

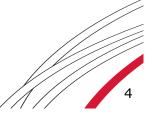
2.2 Identity proofing and credential issuance, renewal and replacement

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 MUST also assert all preceding values (i.e. a CSP asserting assumed must also assert local-enterprise and a CSP







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 <code>assumed</code> 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 - 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]
<pre>\$PREFIX\$/IAP/verif ied</pre>	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]

116

2.3 Authentication

117118119

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

120121

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

122123

2.4 Attribute quality and freshness

124125

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

126127

128 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 member². Other values and attributes are out of scope.

133134

135

136

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

137

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

138139

140

"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:

141142143

144

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.

145146147

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.

148 149

150

151

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.

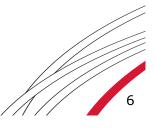
152153154

155

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].





157

3. Conformance criteria

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

160 161

1. The Identity Provider is operated with organizational-level authority.

162163

2. The Identity Provider is trusted enough to be used to access the organization's own systems.

164

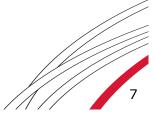
3. Generally-accepted security practices are applied to the Identity Provider.

165166

4. Federation metadata is accurate, complete, and includes site technical, admin, and securitybcontacts, MDUI information.

167

168 A CSP indicates its conformance to this profile by asserting prefix.





170

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.

173174

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

175176177

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

179180

178

The table below defines the following assurance profiles:

181 182

 Assurance profile Cappuccino for low-risk research use cases (\$PREFIX\$/profile/cappuccino)

183 184

• Assurance profile Espresso for use cases requiring verified identity and two factor authentication (\$PREFIX\$/profile/espresso)

185 186

Value	Cappuccino	Espresso
\$PREFIX\$/ID/unique	Х	Х
<pre>\$PREFIX\$/ID/no-eppn-reassign</pre>		
<pre>\$PREFIX\$/ID/eppn-reassign-1yr</pre>		
<pre>\$PREFIX\$/IAP/local-enterprise</pre>	Х	Х
\$PREFIX\$/IAP/assumed	Х	Х
\$PREFIX\$/IAP/verified		Х
<pre>\$PREFIX\$/AAP/good-entropy</pre>	Х	
https://refeds.org/profile/mfa		Х
\$PREFIX\$/ATP/ePA-1m	Х	Х

187 188

189

190

191

192

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

193 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.

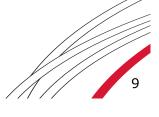
5.1. Security Assertion Markup Language 2.0 (SAML)

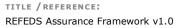
The table below presents how this assurance profile is represented using the SAML framework. Following presentations are used:

- **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]

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

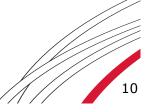
The CSPs are expected to populate the <code>\$PREFIX/AP/cappuccino</code> and <code>\$PREFIX/AP/espresso</code> metadata entity attributes if they are capable of fulfilling those profiles at least for a subset of their users. The Relying Parties can make use of that information to manage their list of 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.



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

ePSA Cormack, A., Linden, M. REFEDs ePSA usage comparison, version 0.13.

Comparison 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+

<u>Framework</u>

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)

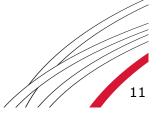
V2.0. OASIS Standard. http://docs.oasis-

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





220

229230

231

232

233234

235

236

237

238

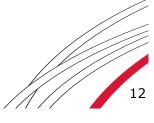
239

Appendix A: Local enterprise -- Good enough for 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 accessing some external resources, too. It is assumed that the Home Organisation 226 227 has made a risk based decision on what exactly are the assurance level requirements 228 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

241	Example on assertion	S
242	A university who quarantees	t

- A university who guarantees that its faculty members:
- 243244

240

- 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
 249 Providers
- 250 Will assert to its faculty members the following multi-valued assurance assertion:
- **251** \$PREFIX\$
- \$PREFIX\$/ID/unique
 - \$PREFIX\$/IAP/local-enterprise
- \$PREFIX\$/IAP/assumed
- \$PREFIX\$/AAP/good-entropy
- \$PREFIX\$/ATP/ePA-1m
 - \$PREFIX\$/profile/cappuccinoExamples on SAML authentication contexts
- 259 The XML namespaces used in the examples:
- - saml="urn:oasis:names:tc:SAML:2.0:assertion"
 - Example 1: An SP requests good-entropy
- 264

253

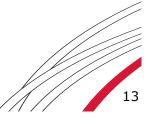
257

258

261

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

- https://refeds.org/assurance/AAP/good-entropy
- 269 </saml:AuthnContextClassRef>
- 270 </samlp:RequestedAuthnContext>
- 271
- 272 An IdP responds good-entropy:
- 273 <saml:AuthnContext>
- 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



Value="urn:oasis:names:tc:SAML:2.0:status:NoAuthnContext"/>



282

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

