## Acceptable Authentication Assurance Policy

**INTRODUCTION**

In order to protect its assets, the Infrastructure needs to authenticate, identify, and trace *Users* granted access to its *Services*. The authentication and identification must be sufficient to meet the requirements of the Security Policy and any ancillary Specific Policies, bearing in mind the nature of data stored within the Infrastructure and the heterogeneous authentication options.

**DEFINITION OF APPROVED AUTHENTICATION ASSURANCE SOURCES**

In HDF we support different assurance levels explicitly. Therefore, we do not have a minimal assurance level. HDF services SHOULD filter users by their assurance level and HDF PIs (VO managers) can (under specific circumstances) take measures to elevate the assurance of users (e.g. by checking a person’s passport according to defined procedures).

HDF uses the REFEDS Assurance Framework [1] (RAF) to express assurance profiles. HDF uses additional Assurance profiles, that are described based on RAF.

As an example, the following (non exhaustive list) of Assurance profiles is supported:

* **AARC-Assam** [1]: This profile represents identities substantially derived from social media or self-signup identity providers (outside the R&E community) on which no further policy controls or qualities are placed. Identity proofing and authenticator are substantially derived from upstream credential service providers (CSPs) that are not under the control of the Infrastructure. This means that the uniqueness or persistence of IDs coming from these CSPs is not guaranteed. The Infrastructure ensures uniqueness on the identifiers based on proprietary heuristics.

The following represents how eduperson\_assurance OIDC claim for this profile can be asserted by the Infrastructure:

MUST assert:

* + <https://aarc-project.eu/policy/authn-assurance/assam>

SHOULD assert:

* + <https://refeds.org/assurance/ID/unique>, but only if the Infrastructure Proxy can comply with the requirements on this unique identifier as specified in the REFEDS RAF [2], including the single natural person and traceability requirements therein
	+ <https://refeds.org/assurance/IAP/low>, but only if the source (meaning originating CSP) complies with REFEDS IAP low requirements [2] (e.g. verified email address)
* **IGTF-Dogwood** [1, 3]: This profile represents identities with persistent non-reassigned identifier, where identity proofing is sufficient to ensure non-reassignment of the identifier for the lifetime of the CSP. May contain marginally-verified real name resemblance or identifiers clearly identifiable as pseudonyms. No anonymous credentials are permitted and issuance must be traceable at time of issuance. Authenticator is secured according to best common practice. Identity and authenticator are managed by the CSP.

The following represents how eduperson\_assurance OIDC claim for this profile can be asserted by the Infrastructure:

MUST assert:

* + <https://igtf.net/ap/authn-assurance/dogwood>

SHOULD assert, only if the Infrastructure is certain the issuing CSP complies with the requirements for each listed attribute/claim (i.e. assert only the claims that are supported):

* + <https://refeds.org/assurance/ID/unique>
	+ <https://refeds.org/assurance/IAP/low>
	+ <https://refeds.org/profile/sfa>
	+ <https://refeds.org/assurance/ATP/ePA-1m>

For example, if the Infrastructure receives <https://refeds.org/assurance/IAP/low> from the CSP, or the Infrastructure is certain CSP complies with the necessary requirements, only then it can (and SHOULD) assert that claim “downstream”. Same is required for other claims.

* **IGTF-Birch** [1, 3]: This profile represents identities with persistent, non-reassigned identifier, and where identity proofing based on in-person appearance (current or past), or remote vetting with compensatory controls, IGTF BIRCH [3] or Kantara LoA 2 [4] or better. It also includes a reasonable verified representation of the real name of the entity, and is secured using best common practices.

The following represents how eduperson\_assurance OIDC claim for this profile can be asserted by the Infrastructure:

MUST assert:

* <https://igtf.net/ap/authn-assurance/birch>

SHOULD assert, only if the Infrastructure is certain the issuing CSP complies with the requirements for each listed attribute/claim (i.e. assert only the claims that are supported):

* <https://refeds.org/assurance/ID/unique>
* <https://refeds.org/assurance/IAP/low>
* <https://refeds.org/assurance/IAP/medium>
* <https://refeds.org/profile/sfa>
* <https://refeds.org/assurance/ATP/ePA-1m>

For example, if the Infrastructure receives <https://refeds.org/assurance/IAP/medium> from the CSP, or the Infrastructure is certain CSP complies with the necessary requirements, only then it can (and SHOULD) assert that claim “downstream”. Same is required for other claims.

* **RAF-Cappuccino** [1, 2]: This profile represents identities that have a unique identifier, identity proofing and credential qualifies substantially to Kantara LoA 2 [4], IGTF BIRCH or CEDAR [3], or eIDAS low [5]. The affiliation information MUST not be older than one month at the moment of receiving such information.

The following represents how eduperson\_assurance OIDC claim for this profile can be asserted by the Infrastructure:

MUST assert, and comply fully with REFEDS RAF profile Cappuccino specification:

* <https://refeds.org/assurance/profile/cappuccino>,
* <https://refeds.org/assurance/ID/unique>
* <https://refeds.org/assurance/IAP/low>
* <https://refeds.org/assurance/IAP/medium>
* <https://refeds.org/assurance/ATP/ePA-1m>
* **RAF-Espresso** [1, 2]: This profile has a unique identifier, identity proofing and credential qualifies substantially to Kantara LoA 3 [4] or eIDAS substantial [5]. The affiliation information MUST not be older than one month.

The following represents how eduperson\_assurance OIDC claim for this profile can be asserted by the Infrastructure:

MUST assert, and comply fully with REFEDS RAF profile Espresso specification:

* <https://refeds.org/assurance/ID/unique>
* <https://refeds.org/assurance/IAP/low>
* <https://refeds.org/assurance/IAP/medium>
* <https://refeds.org/assurance/IAP/high>
* <https://refeds.org/assurance/ATP/ePA-1m>

**EXAMPLES FOR IDENTITY VETTING**

The following examples represent acceptable procedures for Identity Vetting corresponding to profiles IGTF-BIRCH and RAF-Cappuccino (i.e. <https://refeds.org/assurance/IAP/medium>):

* In-person vetting, and recording the number of the government issued ID, or a copy of the same.
* Remote vetting, sending the notarized copy of the government issued ID, together with the remote video interview during which the government issued ID must be shown (the same one which copy is sent).
* Remote vetting, where a copy of the government issued ID is sent, a remote video interview is conducted during which the government issued ID must be shown (the same one which copy is sent), together with attestation to one of the following:
	+ Telephone service account, followed by the demonstration of possession (demonstrated ability to send or receive SMS)
	+ Utility service account number (e.g. electricity, gas, water) for an address matching that in the government issued ID
	+ Financial account number (e.g. credit card, bank account)
	+ An employee or student ID
* Vetting based on a current and ongoing relationship with the applicant, that must be verified through the exchange of a previously exchanged shared secret (e.g. PIN or password) that meets or exceeds best practice requirements, provided that identity was originally established with the degree of rigour equivalent to that required above and an ongoing relations exists sufficient to ensure the Applicant’s continued personal possession of the shared secret.

The example of Identity Vetting procedure corresponding to profile RAF-Espresso can already include examples from RAF-Cappuccino, but in addition must conduct a record check of such received credentials (e.g. in addition to in-person vetting, they must conduct processes to validate that the document is genuine and represents the claimed identity and steps have been taken to minimise the risk of a lost, stolen, suspended, revoked or expired document).

**EXAMPLES FOR AUTHENTICATION ASSURANCE**

In addition to these criteria, additional information can be presented regarding authentication assurance, expressed through RAF Single-Factor Authentication, RAF SFA [6] (and expressed as <https://refeds.org/profile/sfa> claim) and RAF Multifactor Authentication, RAF MFA [7] (and expressed as (<https://refeds.org/profile/mfa> claim).

RAF SFA must comply with following requirements:

|  |  |  |
| --- | --- | --- |
| **Authenticator type** | **Secret basis** | **Minimum length** |
| Memorized Secret  | >= 52 characters(e.g. 52 letters) | 12 characters |
| >=72 characters (e.g. 52 letters + 10 digits + 10 special characters) | 8 characters |
| Time based OTP-Device Out-of-Band Device  | 10-51 characters(e.g. 10 digits) | 6 characters |
| >=52 characters(e.g. 52 letters) | 4 characters |
| Look-Up SecretSequence based OTP-Device | 10-51 characters(e.g. 10 digits) | 10 characters |
| >=52 characters(e.g. 52 letters) | 6 characters |
| Cryptographic Software/Device  | RSA/DSA | 2048 bit |
| ECDSA | 256 bit |

|  |  |
| --- | --- |
| **Way of delivery** | **Maximum life time** |
| Time based OTP Device | 5 minutes |
| Telephone network (e.g. SMS, phone) | 10 minutes |
| E-mail (e.g. recovery link) | 24 hours |
| Postal mail | 1 month |

For MFA, the following additional criteria must be followed:

* The authentication of the user’s current session used a combination of at least two of the four distinct types of factors defined in ITU-T X.1254: Entity authentication assurance framework, section 3.1.3, authentication factor (something you know, something you have, something you are, something you do) [8].
* The factors used are independent, in that access to one factor does not by itself grant access to other factors.
* The combination of the factors mitigates single-factor only risks related to non-real-time attacks such as phishing, offline cracking, online guessing and theft of a (single) factor.

**OPERATIONAL MATTERS**

Assurance will be propagated with the user’s authentication token for relying services to include in Authorisation decisions

Only users conforming to one of the approved authentication assurance profiles shall be granted access to the Infrastructure.

**REFERENCES:**

[1] - Exchange of specific assurance information between Infrastructures - <https://aarc-project.eu/guidelines/aarc-g021/>

[2] - [https://wiki.refeds.org/display/ASS/REFEDS+Assurance+Framework+ver+1.0](https://wiki.refeds.org/display/ASS/REFEDS%2BAssurance%2BFramework%2Bver%2B1.0) and <https://refeds.org/assurance> and

[3] - <https://www.igtf.net/ap/authn-assurance/>

[4] - Kantara Initiative. Kantara Identity Assurance Framework. KIAF-1420 Operational -63r2 Service Assessment Criteria. Version 1.0. Publication Date 2018-03-21. [https://kantarainitiative.org/confluence/display/LC/Identity+Assurance+Framework](https://kantarainitiative.org/confluence/display/LC/Identity%2BAssurance%2BFramework)

[5] - 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>

[6] - REFEDS Single Factor Authentication Profile (SFA) - <https://refeds.org/profile/sfa>

[7] - REFEDS Multi-Factor Authentication Profile (MFA) - <https://refeds.org/profile/mfa>

[8] - International Telecommunication Union. “Series X. Data Networks, Open System Communication and Security. Cyberspace security – Identity management. Entity authentication assurance framework. Standard X.1254.” September 2012: <https://www.itu.int/rec/T-REC-X.1254-201209-I/en>