REFEDS Assurance Framework version 2.0

Version History: V2.0

Status: Final

Date: 2023-12-05

Abstract

In identity federations, Relying Parties (RPs) grant access to services by allowing users to use their own institutional credentials by logging in to their respective Identity Providers (IdPs), which rely on their institution's underlying Credential Service Providers (CSPs). To manage risks related to federated access to their services, some RPs in research and education federations must decide how much confidence they need in the assertions made by the IdPs. This document specifies a framework for articulating such assurances and their expression by the CSP to the RP using common identity federation protocols.

This framework splits assurance into the following independent components:

- Identifier Uniqueness
- Identity Assurance
- Attribute Assurance

To simplify matters for RPs, the components may be further collapsed into two assurance profiles (titled Cappuccino and Espresso) that encapsulate all components. This framework also specifies how to represent the defined claims using SAML 2.0 and OpenID Connect federated identity protocols.

Claims made on the basis of the original REFEDS Assurance Framework (RAF 1.0) can continue under the REFEDS Assurance Framework version 2.0 (RAF 2.0) with some exceptions for Identity Assurance Profile (IAP) process-based claims. Appendix A explains these exceptions and section 4 defines how to express IAP claims under both RAF 1.0 and RAF 2.0.

1. Purpose and Scope

This section is informative.

This document provides a framework by which a Credential Service Provider (CSP) asserts claims to a Relying Party's (RP's) service about its confidence in the values of selected user attributes.

The CSP encompasses an organisation's authentication and authorisation infrastructure where the user enrollment, credential issuance and user lifecycle are managed. In a federated environment the RP uses a federation protocol (typically SAML or OIDC) to communicate with the user's Identity Provider (IdP), which represents the CSP to the RP using the federation protocol to provide the user's authentication details and related attributes. The REFEDS Assurance Framework (RAF) addresses the following distinct components:

Identifier Uniqueness - communicates to the RP that the user's identifier (such as a login name) is unique and is bound to a single identity in the CSP's context.

Identity Assurance - communicates to the RP how confident the CSP was at the time of enrollment, of the real-world identity of the Person to whom the account was issued. This framework specifies three levels of process-based identity assurance and authenticator management (low, medium and high) and one risk-based identity assurance claim (local-enterprise).

Attribute Assurance - communicates to the RP the quality and freshness of specific attributes (other than the unique identifier) passed in the login assertion.

In a federated environment, since an RP outsources some or all of its authenticator issuance and management needs to one or more external CSPs, it must rely on those CSPs to manage associated risk. How much risk is acceptable and which security controls are applied are based on the RP organisation's assessment of the sensitivity of the information and data collected, processed, and maintained by its information systems, services, applications and infrastructure. Based on the organisation's particular needs and level of risk it is willing to accept, the organisation will require a commensurate level of confidence on understanding the CSP's assurance of the asserted identity and attributes. There are varying degrees of confidence required, with assertions about the uniqueness and timeliness of some attributes. This document presents a framework for communicating those degrees of confidence over federated

login.

Claims about authentication strength are outside the scope of this framework (for example, the REFEDS SFA Profile [REFEDS SFA] and REFEDS MFA Profile [REFEDS MFA]); however, while REFEDS Assurance Framework (RAF) claims are transmitted from the CSP to the RP with every federated login, the authentication needs to be commensurately strong enough to ensure that the claims pertain to the person logging in. For example, an RP that determines that a service it provides requires high assurance should also require MFA from the CSP.

In addition, outside the scope of this framework, an RP must also ensure that the claims from the CSP are protected and cannot be modified in transit. For example, in SAML, the assertion response is signed using a certificate known and trusted by the RP.

The purpose of producing this version 2.0 of RAF (RAF 2.0) is twofold:

1. to tighten the definitions of many claims based on field experience with RAF 1.0 (the original RAF), and
2. to provide a single set of criteria defining the IAP claims of low, medium, and high, avoiding the need for the CSP to refer to one of several external standards and also reducing the ambiguity faced by RPs who wish to have a clear understanding of what each IAP claim actually means.

2. Terms and Definitions

Term	Definition
Attribute Assurance	See Section 1.
Authenticator	A means used to perform digital authentication. A Person authenticates to a system by demonstrating possession and control of an authenticator. Examples: a password, a phone number used to receive OTP by SMS, or an MFA token.
Authenticator Binding	Establishing and maintaining the binding between an authenticator and a vetted identity.
Claimant	The Person submitting a claim of identity to

Term	Definition
	the CSP's identity proofing process.
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.
Identifier Uniqueness	See Section 1.
Identity Assurance	See Section 1.
Identity Evidence	Information or documentation provided by the applicant to support the claimed identity. Identity evidence may be physical (*e.g.* a driver licence) or digital (*e.g.* an assertion generated and issued by a CSP based on the applicant successfully authenticating to the CSP). [NIST SP 800-63-3]
Identity Proofing Process	The process by which a CSP evaluates a Claimant's claim of identity. Identity proofing processes may vary in levels of assurance, the characteristics of which are articulated in this framework.
Identity Provider (IdP)	Generally, a software component that acts as the federated interface to the CSP.

Term	Definition
Person	For the purposes of this document, a "Person" refers to a living, individual human being and not a legal entity such as a corporation or a system or shared account. This is sometimes referred to as a "natural person" as opposed to a "legal person".
Registrar	A person conducting any part of the identity proofing process on behalf of the CSP.
Relying Party (RP)	An actor that relies on an identity assertion or claim [X.1254].
Supervised Remote Proofing	An identity proofing process is considered 'supervised remote' when: 1. the Claimant does not appear in-person face to face with a Registrar, and 2. the CSP's Registrar and Claimant interact during the identity proofing process, such as over a live video chat, in such a way that the Registrar verifies the Claimant's identity.

Term	Definition
Unsupervised Remote Proofing	An identity proofing process is considered 'unsupervised remote' when: 1. the Claimant does not appear in-person face to face with the Registrar, and 2. no Registrar interacts with the Claimant during the identity proofing process. Unsupervised Remote Proofing processes may be: a. not fully-automated, in which the CSP uses a Registrar to evaluate the application and perform any checks required after the time of the Claimant's application, or b. fully-automated, where the CSP uses technology to process the claim and automate any required checks. An identity proofing process may use a combination of fully-automated and not fully-automated unsupervised remote proofing.
Validation	Checking to see that the identity evidence is genuine, and that the identity claimed by the evidence is a real identity that exists (*i.e.*, the evidence is genuine, and the identity it claims is a genuine real-world identity of a Person).
Verification	Checking to see if the Claimant is the Person to whom the validated identity belongs.

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].

3. Conformance Criteria

This section is normative.

A CSP MUST conform to the following REFEDS Baseline Expectations for Identity Provider Operators [REFEDS IFBE] in order to assert any RAF claim.

1. Your Identity Provider is operated with organisational-level authority.
2. Your Identity Provider is trusted enough to be used to access your organisation's own systems.
3. You publish contact information for your Identity Provider and respond in a timely fashion to operational issues.
4. You apply security practices to protect user information, safeguard transaction integrity, and ensure timely incident response.
5. You ensure the metadata registered in Federation is complete, accurate and up to date.

A CSP SHALL indicate its conformance to these criteria by asserting the following URI: https://refeds.org/assurance

A CSP MAY choose to release only `https://refeds.org/assurance` to signal its conformance with these criteria without making any other assurance assertions.

If a CSP is releasing any other assurance values in this framework for a Person it MUST also release: `https://refeds.org/assurance`

4. Versioning

This section is normative.

With the exception of the RAF 1.0 claims for IAPs low, medium, high, each RAF 1.0 claim can continue to be expressed under RAF 2.0. Full details of these exceptions are explained in Appendix A. Further, all RAF 2.0 claims are expressed in the same manner as RAF 1.0 claims:

- Conformance (section 3 above) must be signalled with the `https://refeds.org/assurance` value of `eduPersonAssurance` [eduPerson].
- Individual RAF (1.0 or 2.0) claims are expressed as values of `eduPersonAssurance` in the `https://refeds.org/assurance/` namespace.

To make clear whether a claim is made under RAF 1.0 or RAF 2.0, an additional claim is defined.

Value	Definition
`https://refeds.org/assurance/version/2`	All claims expressed in the `https://refeds.org/assurance/` namespace are based on RAF 2.0.

If a CSP makes any process-based IAP claim (IAP low, IAP medium, or IAP high), in order to claim the RAF 2.0 version, the CSP MUST either implement the normative criteria for process-based claims in section 5.2.1, or MUST meet compatibility of an equivalent or higher assured framework as detailed in Appendix A.2. Note that this does not apply to the risk-based IAP claim of local-enterprise. RAF 1.0's claim of local-enterprise, as with other RAF 1.0 non-process-based-IAP claims, can continue to be expressed under RAF 2.0.

Thus, for example, the claim `https://refeds.org/assurance/IAP/high` is declared to be based on RAF 2.0 criteria if the `https://refeds.org/assurance/version/2` claim is also made; otherwise it refers to RAF 1.0. CSPs MUST send the version 2 claim if they also send an IAP high claim based on RAF 2.0. The specific RAF 2.0 IAP criteria which cannot be assumed to be met by RAF 1.0 IAP claims are detailed in Appendix A.

All non-process-based IAP RAF (1.0 or 2.0) claims (in section 5.2.1) have the same assurance intent whether the version 2 claim is made or not. Because RAF 2.0 makes wording changes and other clarifications in the definitions of most RAF claims, it is possible that some RPs may interpret a difference where none is intended. See Appendix A for further discussion on RAF 1.0 compatibility with RAF 2.0 compatibility.

In addition, RAF 2.0 adds accepting 'staff' and 'employee' from eduPersonPrimaryAffiliation and eduPersonScopedAffiliation to the Attribute Quality Freshness component (see section 5.3). An organisation making or requiring a freshness claim for 'staff' or 'employee' must implement RAF 2.0 instead of RAF 1.0.

Any entity implementing RAF for the first time SHOULD use the latest version.

5. Assurance Components

This section is normative.

This section introduces three assurance components which each represent a different aspect of assurance. A CSP can assert values from different components independently. The values are claims about the specific Person

represented in the assertion; different Persons may qualify for different values.

Because eduPersonAssurance ([eduPerson]) is case sensitive, and in order to maintain compatibility and avoid breaking changes with RAF 1.0, values defined in this framework (eg, `https://refeds.org/assurance/IAP/high` or `https://refeds.org/assurance/version/2`) MUST be transmitted by the CSP exactly as specified, and an RP MUST only expect them as such.

See Appendix C for a complete annotated example.

5.1. Identifier Uniqueness

This section is normative.

A unique identifier MUST represent one and only one Person in the CSP's system. A non-reassignable identifier is attached to only one Person, *i.e.*, once created, it MUST NOT be repurposed to represent another Person at any time, even when the Person associated with the identifier no longer exists in the issuing identity system.

5.1.1. Identifier Uniqueness Characteristics

This section is normative.

This component describes how a CSP expresses identifier uniqueness for a Person when it provides one or more of the set of identifiers specified in [UN0] below.

Value	Definition
https://refeds.org/assurance/ID/unique	Asserting this value means that one or more of the identifiers listed in [UN0] is provided. Furthermore, each identifier listed in [UN0] that is provided MUST meet all of the criteria [UN1], [UN2], and [UN3]: **[UN0]** The identifier is a SAML 2.0 persistent name identifier [OASIS SAML], subject-id or pairwise-id [OASIS SIA], OpenID Connect sub (type: public or pairwise) or eduPersonUniqueId [eduPerson] **[UN1]** The identifier MUST represent a single Person **[UN2]** The CSP MUST have a means to contact the Person to whom the identifier is assigned whilst the identifier is in use. **[UN3]** The identifier MUST NOT be reassigned

5.1.2. Uniqueness of eduPersonPrincipalName

This section is normative.

In addition to the identifiers listed in [UN0], eduPersonPrincipalName (ePPN, [eduPerson]) is a human-readable identifier whose reassignment practice is undefined by its specification. To support Relying Parties' use of ePPN, the following values are defined to describe a CSP's ePPN practices.

The values in the following table are mutually exclusive. A CSP MAY assert one of them but MUST NOT assert more than one.

Value	Description
https://refeds.org/assurance/ID	eduPersonPrincipalName value has the

`/eppn-unique-no-reassign`	[UN1], [UN2] and [UN3] (as defined in the table above on ID/unique) properties.
`https://refeds.org/assurance/ID/eppn-unique-reassign-1y`	eduPersonPrincipalName value has the [UN1] and [UN2] (as defined in the table above on ID/unique) property but may be reassigned after a hiatus period of 1 year or longer.

The remainder of section 5.1.2 is informative.

The expected RP behaviour for observing ePPN reassignment is as follows:

- If the CSP asserts `eppn-unique-no-reassign`, the RP knows that when it observes a given ePPN value it will always be assigned to the same Person.
- If the CSP asserts `eppn-unique-reassign-1y`, the RP knows that if no assertion bearing that ePPN value as a unique identifier is received for one year, the ePPN may have been reassigned. A safe practice for the RP is to close a user account or remove the ePPN value associated with it if the user hasn't logged in for one year. The RP can also use some out-of-band mechanism to verify whether the user is still the same Person.
- If the CSP asserts neither `eppn-unique-no-reassign` nor `eppn-unique-reassign-1y`, the RP cannot rely on ePPN as a unique identifier but should use it only in combination with another identifier listed in [UN0].

Finally, the reader is reminded that they should not assume any property that goes beyond the specification of the ePPN attribute. For instance, an RP must not assume that an ePPN value can be used as the recipient of an email message.

5.2. Identity Proofing and Authenticator Issuance, Renewal and Replacement

The following is informative.

This framework supports two different approaches for making Identity Assurance related claims. The first approach is based on assessment of the identity proofing and authenticator management process(es) used by the CSP against specified criteria, and RPs determine which criteria suffice to address their risks. This approach is detailed in section 5.2.1 below. Appendix B contains informative implementation guidance for RAF 2.0 process-based IAP claims.

The second approach is based on the issuing organisation's accepted risk. In this

approach, the CSP asserts whether the organisation of which it is a part trusts its own identity proofing and authenticator management processes enough to address risk associated with their use within the local enterprise, and RPs determine if that organisation's risk acceptance suffices for themselves. This approach is detailed in section 5.2.2 below.

These approaches may be used independently or together. IAP claims are defined below for each approach.

5.2.1. Process-Based IAP Claims

The following is normative.

This Framework defines IAP values "low", "medium" and "high", which constitute an ordered set of identity proofing levels with increasing requirements. A CSP asserting an IAP value of "high" for a user MUST also assert the IAP values "medium" and "low" for that user. A CSP asserting an IAP value of "medium" for a user MUST also assert the IAP value "low" for that user.

Value	**Definition**
`https://refeds.org/assurance/IAP/low`	The bearer of this claim is a Person with a self-asserted identity. To issue this value, the CSP MUST satisfy or exceed all criteria in the IAP low column in the Table of Normative IAP Criteria.
`https://refeds.org/assurance/IAP/medium`	The bearer of this claim is a Person with a reasonably validated and verified identity. To issue this value, the CSP MUST satisfy or exceed all criteria in the IAP medium column in the Table of Normative IAP Criteria.
`https://refeds.org/assurance/IAP/high`	The bearer of this claim is a Person with a well validated and verified identity. To issue this value, the CSP MUST satisfy or exceed all criteria in the IAP high column in the Table of Normative IAP Criteria.

Table of Normative IAP Criteria

Specific criteria that define each IAP level are organised into the following groups: General Requirements, Identity Evidence, Validation, Verification, Authenticator Binding, and Unsupervised Remote Proofing.

Some jurisdictions and vendors provide identity proofing and authenticator management services that meet or exceed the criteria for a given IAP level. When a Claimant demonstrates authentication to such a third-party service, corresponding criteria in the IE, VA, VF, and UR criteria groups specified below MAY be considered satisfied at that IAP level by the CSP. When authentication to such a service is used to satisfy the corresponding criteria at IAP high, the authentication SHALL use MFA or similarly strong or stronger authentication. The CSP SHALL document which criteria are satisfied in such a manner, per [GR2] below.

Normative Criteria	**IAP low**	**IAP medium**	**IAP high**
General Requirements [GR#]			
[GR1] The CSP takes measures to ensure that the Claimant accomplishing each step of the identity proofing and authenticator issuing process is the same Person throughout the process.	x	x	x
[GR2] The identity proofing process follows documented procedures, and the documentation addresses how the CSP meets all applicable criteria for each IAP level they support.	x	x	x
[GR3] Records are kept of the following: • When the Claimant was identity-proofed • To what IAP level • Changes to the binding between a Claimant and their associated authenticators or contact information as identified in [AB5]	x	x	x

Normative Criteria	**IAP low**	**IAP medium**	**IAP high**
Each record should be preserved in accordance with local record-retention guidelines.			
[GR4] Records are also kept of the following: • The attributes that were validated by the identity proofing process Each record should be preserved in accordance with local record-retention guidelines.		x	x
[GR5] Records are also kept of the following: • The values of one or more attributes validated by the identity proofing process that uniquely identifies the Claimant Each record should be preserved in accordance with local record-retention guidelines.			x
Identity Evidence [IE#] Acceptable sources of identity evidence.			
[IE1] No identity evidence is required.	x		
[IE2] Identity evidence is acceptable for use in identity proofing if it is • valid at the time of identity proofing, and • contains attribute(s) that uniquely identifies the Claimant, and • is either issued by a nationally recognised[1] source, or is nationally recognised as being valid for identification purposes, or is a		x	x

[1] Identity documents issued by States, Cantons, Provinces, Departments, or other jurisdictions within a country are acceptable if they are recognised across the country.

Normative Criteria	IAP low	IAP medium	IAP high
documented attestation (vouch) from an authority recognised by the CSP per [VA4.3].			
Validation [VA#]] Confirm that identity evidence is genuine and claimed identity exists.			
[VA1] No identity evidence is required.	x		
[VA2] Identity evidence presented appears to be genuine.		x	
[VA3] If the identity evidence presented contains intrinsic physical and/or cryptographic security features, either the physical or cryptographic features must be checked.			x
[VA4] The identity evidence presented is checked against a trusted source to validate that the identity presented by the identity evidence exists. The trusted source shall be appropriate and authoritative in the CSP's context. Such checks may, but need not, take one of the following forms: 1. One or more issuing or authoritative sources confirm the validity of the identifying attributes presented by the identity evidence. 2. The Registrar confirms the presence of the claimed identity in transaction records of a recognized organisation providing financial, educational, or utility services. 3. A Person vouches for the claimed			x

Normative Criteria	**IAP low**	**IAP medium**	**IAP high**
identity. This Person must have been previously identity proofed at IAP high and the vouch itself must be communicated directly by the Person to the CSP in a trusted manner.			
Verification [VF#] Confirm ownership of the claimed identity in the presence of a Registrar, either in-person or a supervised remote session.			
[VF1] The Claimant is checked to be a Person.	x	x	x
[VF2] Presented identity evidence reasonably appears to belong to the Claimant.		x	x
Authenticator Binding [AB#] Establish and maintain the binding between an authenticator and a vetted identity.			
[AB1] The Claimant must provide at least one piece of contact information and demonstrate control of any provided contact information (e.g., email, postal address, telephone number, or similar) during the identity proofing process to be used for notification or initial authenticator issuance purposes.	x	x	x
[AB2] If the CSP issues an authenticator to the Claimant during or after the identity proofing process, it must be delivered in a manner that can be assumed to only reach the Claimant.	x	x	

Normative Criteria	IAP low	IAP medium	IAP high
[AB3] If the CSP issues an authenticator to the Claimant during or after the identity proofing process, it must be delivered only into the possession of the Claimant to whom it belongs.			x
[AB4] If the CSP permits the Claimant to register a previously issued authenticator, then the Claimant must demonstrate control of that authenticator to the CSP during the identity proofing process. Such an authenticator may either be issued by the CSP in a prior context or one issued by a third party that has been documented as acceptable by the CSP.	x	x	x
[AB5] After initial identity proofing is complete, the binding between the vetted identity and associated authenticators and contact information must be maintained. This must be done either by re-identity proofing or by authenticating with a valid authenticator previously bound to the vetted identity, when any of the following occur: • renewal, replacement, or removal of a vetted Claimant's existing authenticator, or • registering a new authenticator, or • updating, adding, or removing contact information. Any new authenticator must be of a kind that is documented as acceptable by the CSP and the Claimant must demonstrate control of it.	x	x	x

Normative Criteria	**IAP low**	**IAP medium**	**IAP high**
Unsupervised Remote Proofing [UR#] Additional requirements when Claimant is not supervised through the process by a Registrar			
[UR1] When unsupervised remote proofing is used, at least one piece of contact information is verified to belong to the Claimant by a trusted source ("trusted source" is defined in [VA4]).			x
[UR2] When unsupervised remote proofing is used, [VA4] is required.		x	x
[UR3] When unsupervised remote proofing is used, one of the following means is used to meet [VF2]: 1. A Registrar manually compares a photo or other biometric contained within a piece of validated identity evidence with a live video, photo or other biometric of the Claimant captured during the unsupervised remote portion of the proofing process. 2. An automated system compares a photo or other biometric contained within a piece of validated identity evidence with a live video, photo or other biometric of the Claimant captured during the unsupervised remote portion of the proofing process, and the technology that does the comparison is deemed sufficient for this purpose by a nationally or internationally recognised authority.			x

Appendix B contains a narrative presentation of these criteria.

5.2.2 Risk-based IAP Claim

This section is normative.

In contrast to the approach in section 5.2.1, in which claims are made about some of the CSP's processes, in this section a claim, called "local-enterprise", is made about the demonstrated risk acceptance of an organisation the CSP supports. If the organisation deems the level of identity assurance good enough for accessing their critical internal systems, then it might also be judged good enough for accessing some external resources.

The organisation MUST have made a risk-based decision on requirements that must be satisfied by CSP accounts before they may be granted access to their critical internal systems. That is, the organisation has demonstrated through its satisfaction with on-going operations that it accepts whatever residual risk is inherent in potential misuse of any of their critical internal systems by an authorised authenticator.

All of the organisation's users whose identity is proofed by the same or better processes, and who possess authenticators that are managed by the same or better processes, can have the local-enterprise claim asserted with their federated logins.

Organisations may have several internal systems with varying risk levels, and hence various identity assurance level requirements. Those deemed "critical internal systems" in this specification MUST satisfy one or more of the following criteria:

- The system manages some of the organisation's expenditures
- The system manages employment-related personal data
- The system manages student-related personal data
- The system manages some aspect of the organisation's regulatory or legal compliance obligations
- The system is vital to the functioning of the organisation

A CSP MAY assert the following value independent of the other IAP values defined above in section 5.2.1:

Value	**Description**
`https://refeds.org/assurance/IAP/local-enterprise`	The identity proofing and authenticator issuance, renewal and replacement are done in a way that qualifies (or would qualify) the user to access the organisation's critical internal systems.

5.3. Attribute Quality and Freshness

This section is normative.

This section describes the requirements for the quality and freshness of the attributes (other than the unique identifier) that 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, staff, employee and member. Other values and attributes are out of scope.

Here "freshness" refers to the latency between the time when one of these affiliations is changed in the organisation's associated system of record and the time when the organisation's Identity Provider accurately reflects the change.

The freshness of eduPersonAffiliation, eduPersonScopedAffiliation and eduPersonPrimaryAffiliation is intended 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 `https://refeds.org/assurance/ATP/ePA-1d` MUST also assert `https://refeds.org/assurance/ATP/ePA-1m` for a given user.

Value	Description
`https://refeds.org/assurance/ATP/ePA-1m`	Appearance of "faculty", "student", "staff", "employee" or "member" in any of eduPersonAffiliation, eduPersonScopedAffiliation or eduPersonPrimaryAffiliation attributes accurately reflect the user's affiliation(s) in associated systems of record within the previous 31 calendar days.
`https://refeds.org/assurance/ATP/ePA-1d`	Appearance of "faculty", "student", "staff", "employee" or "member" in any of eduPersonAffiliation, eduPersonScopedAffiliation or eduPersonPrimaryAffiliation attributes

Value	Description
	accurately reflect the user's affiliation(s) in associated systems of record within the previous 1 working day.

The remainder of this section is informative.

This specification imposes no particular requirements on the organisational business policies and practices regarding the start or end of an affiliation between the user and the organisation. For example:

- In some organisations, a faculty loses their organisational role and privileges the day their employment ends. In other organisations, there is a defined grace period during which they maintain their faculty privileges.
- In some universities, a student loses their organisational role and privileges the day they graduate. In other universities, the student role and privileges remain effective until the end of the next semester.
- In some organisations, a new faculty appointee is given faculty access privileges some time before the start of their contract term. In other organisations, faculty access privileges commence on the first day of their contract term.
- In some organisations, particularly during busy times-of-year, data entry in responsible offices (eg, HR or Registrar) may be backed-up on either the incoming or outgoing end and affiliations may be "back-dated" to reflect actual start or end dates.

None of these situations have any bearing on the value of the freshness claim. The timeframe being claimed only refers to the time from when the business process updates the relevant system of record, not when the action is time-stamped (which may be backdated as per the example above).

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.

6. Assurance Profiles

This section is normative.

The following describes a simplified way to bundle claims by collapsing the components presented in sections 3 and 5 into two assurance profiles:

`cappuccino` and `espresso`.

The CSPs who populate the assurance assertions presented in the section 5 SHOULD also populate all assurance profiles to which they qualify.

The table below defines the following assurance profiles:

- Assurance profile Cappuccino for low-risk research use cases (`https://refeds.org/assurance/profile/cappuccino`)
- Assurance profile Espresso for use cases requiring verified identity (`https://refeds.org/assurance/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**
`https://refeds.org/assurance`	X	X
`https://refeds.org/assurance/ID/unique`	X	X
`https://refeds.org/assurance/ID/eppn-unique-no-reassign`		
`https://refeds.org/assurance/ID/eppn-unique-reassign-1y`		
`https://refeds.org/assurance/IAP/low`	X	X
`https://refeds.org/assurance/IAP/medium`	X	X
`https://refeds.org/assurance/IAP/high`		X
`https://refeds.org/assurance/IAP/local-enterprise`		
`https://refeds.org/assurance/ATP/ePA-1m`	X (*)	X (*)
`https://refeds.org/assurance/ATP/ePA-1d`		

(*) The CSP can omit this requirement if it doesn't populate and release the attribute values defined in section 5.3 for this Person.

For instance, if a user qualifies for all values required according to the column "Espresso" the CSP SHOULD assert `profile/espresso` for this user.

Notice that these assurance profiles do not cover the authentication assurance of the user session. The deployers are encouraged to use these profiles in conjunction with specifications focusing on authentication, such as the REFEDS Multi-Factor Authentication [REFEDS MFA] and REFEDS Single-Factor Authentication [REFEDS SFA] profiles.

Also note that cappuccino and espresso represent an ordered set. If a CSP signals espresso, the CSP MUST signal *both* cappuccino and espresso.

7. Representation on Federated Protocols

This section is normative.

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

In SAML 2.0, this assurance framework is to be represented using the multivalued `eduPersonAssurance` attribute, as defined in [eduPerson].

In OIDC, this assurance framework is to be represented using the multivalued `eduperson_assurance` claim, as defined in [REFEDS OIDCre].

8. 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	Interoperable Global Trust Federation 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. KIAF-1420 Operational -63r2 Service Assessment Criteria. Version 1.0. Publication Date 2018-03-21. https://kantarainitiative.org/confluence/display/LC/Identity+Assurance+Framework
Kantara TSL	Kantara Initiative Trust Status List. https://kantarainitiative.org/trust-status-list/
NIST SP 800-63-3	https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-3.pdf
OASIS SAML	Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0. OASIS Standard. 15 March 2005. https://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf
OASIS SIA	SAML V2.0 Subject Identifier Attributes Profile Version 1.0. 16 January 2019. https://docs.oasis-open.org/security/saml-subject-id-attr/v1.0/saml-subject-id-attr-v1.0.pdf
REFEDS IFBE	REFEDS Identity Federation Baseline Expectations. https://refeds.org/baseline-expectations
REFEDS OIDCre	OpenID Connect for Research and Education Working Group. Mapping SAML attributes to OIDC Claims. Referenced 9 February 2018. https://wiki.refeds.org/display/GROUPS/OpenID+Connect+SAML+mapping
REFEDS MFA	REFEDS Multi-Factor Authentication Profile. https://refeds.org/profile/mfa
REFEDS SFA	REFEDS Single-Factor Authentication Profile. https://refeds.org/profile/sfa
RFC2119	Bradner, S. Key words for use in RFCs to Indicate Requirement Levels. RFC2119.

	https://www.ietf.org/rfc/rfc2119.txt
UKGDS	How to prove and verify someone's identity, updated 9 January 2023, UK Government Digital Service. Referenced 23 March 2023. https://www.gov.uk/government/publications/identity-proofing-and-verification-of-an-individual/how-to-prove-and-verify-someones-identity
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

Appendix A: Compatibility of RAF Versions and Other Frameworks

This appendix is informative.

A.1 Guidance Regarding Upwards Compatibility of RAF 1.0 to RAF 2.0

The following sections are intended to clarify the differences between RAF 1.0 and RAF 2.0 IAP claims in order to help RPs decide what to require, and to help CSPs transition to RAF 2.0 if required. These details are different depending on which external framework (IGTF, Kantara "Classic", or eIDAS) the CSP used to justify its RAF 1.0 IAP claim. Note that if the CSP made no process-based IAP claims at all, the CSP can add `https://refeds.org/assurance/version/2` and be fully RAF 2.0 compliant; any future process-based IAP claims would need to be implemented according to the criteria in Section 5.2.1 of this document.

Under the REFEDS Assurance Framework (version 1.0, denoted RAF 1.0 when clarity is needed), IAP levels low, medium, and high were assigned to selections of one or more external identity proofing standards. By contrast, IAP levels under the present REFEDS Assurance Framework version 2.0 are assigned based on meeting associated criteria explicitly defined within the Framework.

The reason RAF 2.0 explicitly defines IAP criteria within the framework is due to the challenge posed by RAF 1.0 IAP criteria referring to three different external sources, stating that any one of those three sources can be used to meet RAF 1.0 IAP levels. That reliance on external sources made RAF 1.0 more difficult to understand, forcing the CSP to study the external sources and make a determination which "route" they would use. The three sources were IGTF, selections from Kantara "Classic", and selections from eIDAS for IAP low and IAP medium. IAP high only referred to Kantara "Classic" and eIDAS.

From an RP's perspective, the presence of three different referenced frameworks made it difficult to determine the practical level of risk the IAP claims addressed. The guaranteed risk had to be the lowest common denominator between all three frameworks (two frameworks for IAP high), for the simple reason there was no way for an RP to know by which framework the CSP arrived at a particular IAP claim.

The authors of RAF 2.0 attempted to find the common ground between the sources and crystalize what the IAP levels inherently mean, within the document itself. Thus, RAF 2.0 IAP criteria are derived from the RAF 1.0 sources. Through the course of the analysis, the differences between the three source systems revealed themselves. The authors considered weakening the RAF 2.0 criteria to maintain full upwards compatibility from RAF 1.0. However, given that risks to

identity proofing have evolved since RAF 1.0 was authored, the RAF 2.0 authors decided not to weaken the framework, and instead adopt a version claim.

RAF 1.0 is not deprecated. However, some RPs may require assurance using RAF 2.0 criteria over RAF 1.0 criteria. For this reason, all implementations of RAF 2.0 must also signal `https://refeds.org/assurance/version/2`. The absence of the RAF version 2 claim but presence of `https://refeds.org/assurance` indicates that any IAP low, medium, or high claim is RAF 1.0, and it is up to the RP to decide if that is sufficient. The sections below provide additional guidance to assist the RP in making this determination.

If an RP requires RAF 2.0, this has implications for CSPs who have already, or are considering, implementation of RAF 1.0. In order to meet RP requirements, the CSP may need to transition to RAF 2.0 from RAF 1.0.

Implications for CSPs Using eIDAS for RAF 1.0 Transitioning to RAF 2.0

This section only addresses RAF 1.0 implementations where the organisation has internally established a process using the eIDAS paragraphs explicitly referenced by RAF 1.0. This section does not address the situation when the CSP's identity proofing process leverages a national electronic ID that has already been identity proofed.

Assurance Gaps Involved:

If the CSP made a RAF 1.0 IAP process-based claim using the cited eIDAS paragraphs from 1.0, then it's possible the CSP made such a claim without satisfying [AB4] in RAF 2.0.

eIDAS is silent on additional requirements for Unsupervised Remote processes, specifically [UR3]. Therefore, if the CSP has used the specific eIDAS paragraphs referenced by RAF 1.0 to make RAF 1.0 IAP claims, and is using an Unsupervised Remote process, the CSP needs to check that the implementation satisfies the [UR3] requirement. Please also note Appendix A.2: if the CSP is leveraging users' eIDs, then these checks need not be done.

Transition Guidance for CSP:

If an RP levies a requirement for RAF 2.0, the CSP must first ensure that, if it allows the binding of third-party credentials, [AB4] is implemented. Once [AB4] is satisfied or determined not applicable, then the CSP may add the claim `https://refeds.org/assurance/version/2`

Implications for CSPs Using Kantara "Classic" for RAF 1.0 Transitioning to RAF 2.0

Assurance Gaps Involved:

If the CSP made a RAF 1.0 IAP claim using Kantara, then it's possible the CSP made such a claim without satisfying [AB4] or [UR1].

Transition Guidance for CSP:

If an RP levies a requirement for RAF 2.0, the CSP needs to:

- Confirm whether it allows the binding of third party authenticators. If so, the CSP must meet [AB4]. If not, there is no issue.
- For claims of IAP high, confirm whether it allows unsupervised remote proofing. If so, the CSP must meet [UR3]. If not, there is no issue.

Once these two criteria are met, the CSP may add the claim `https://refeds.org/assurance/version/2`

Implications for CSPs Using IGTF for RAF 1.0 Transitioning to RAF 2.0

Assurance gaps involved:

If the CSP claims IAP low or IAP medium based on the IGTF framework as described in RAF 1.0, it's possible that [IE2], [AB1] or [AB4] is not met.

Transition Guidance for CSP:

If an RP levies a requirement for RAF 2.0, the CSP needs to:

- For IAP claims of low and medium, confirm whether it requires contact information for the Claimant, with demonstration of proof of control of that contact information [AB1].
- For IAP claims of medium, confirm whether the identity evidence it uses is issued by a source nationally recognised for such purposes [IE2].
- Confirm whether it allows the binding of third party authenticators. If so, the CSP must meet [AB4]. If not, there is no issue.

Once these three criteria are met, the CSP may add the claim `https://refeds.org/assurance/version/2`

Implications for the RP

Because RAF 1.0 does not inform the RP by which source framework (RAF 1.0 refers to selected sections of IGTF, eIDAS, and Kantara "Classic") the CSP made its IAP claim, the RP has to consider the following risk gaps for IAP claims without the RAF 2.0 version claim (i.e., RAF 1.0 IAP claims). Specifically, the

CSP may have implemented these, but the RP cannot be sure they are implemented based solely on a RAF 1.0 claim:

- IAP low: [AB1], [AB4]
- IAP medium: [IE2], [AB1], [AB4]
- IAP high: [AB4], [UR3]

Which source framework has which gap is detailed in the "implications" sections above.

Because [AB4] is a potential gap across all three of the source frameworks for RAF 1.0 claims of IAP low, IAP medium, or IAP high, if the RP permits use of authenticators bound to the vetted identity that are not issued by the CSP making those IAP claims, then the RP should require `https://refeds.org/assurance/version/2`

Note that if the RP does not require process-based IAP claims, then the RP need not require the RAF 2.0 version claim for the other claims in this framework, as those claims are fully upwards compatible.

Finally, any CSP implementing RAF 2.0 would be fully backwards compatible in this regard, and an RP choosing not to require RAF 2.0 will still be able to accept RAF 2.0 claims. (There is no case where RAF 2.0 weakens any claim).

A.2 Compatibility of Equivalent or Higher Assurance Frameworks

This Appendix provides a mapping of selections of external identity proofing standards which suffice to meet or exceed a corresponding IAP level. This appendix is not comprehensive; it provides examples. If any CSP has implemented one of these equivalent frameworks, the CSP may make IAP claims without having to further analyse the IAP criteria in Section 5.

If a CSP has already implemented IGTF standards and wants to adopt RAF 2.0, refer to A.1 above for notes on what criteria must be checked before the RAF 2.0 version claim can be asserted.

If a CSP follows the EU's eIDAS specifications:

- If a CSP implements **eIDAS Substantial or High**, they may assert IAP high, IAP medium and IAP low.
- If a CSP implements **eIDAS Low**, they may assert IAP medium and IAP low.

If a CSP follows the U.S.'s NIST 800-63-3 standards:

- If a CSP implements **NIST SP 800-63-3 IAL2 or IAL3**, they may assert IAP high, IAP medium and IAP low.
- Note that **NIST SP 800-63-3 IAL1**, does not qualify for IAP low unless

the CSP adds a measure to check if the Claimant is a Person.

Appendix B: Implementation Discussion

This Appendix is informative.

B.1 Narrative of IAP Criteria

The following section details requirements for the identity proofing and authenticator issuing process the Credential Service Provider (CSP) must meet to claim the IAP levels of low, medium, and high.

The identity proofing process involves several fundamental concepts in addition to some general requirements: Identity Evidence, Validation, Verification and Authenticator Binding (see Terms and Definitions).

B.1.1 In Person and Supervised Remote Proofing

The following describes the requirements for an In-Person or Supervised Remote Proofing process to be able to claim IAP low, medium or high. Additional requirements for an Unsupervised Remote proofing process are specified in the next session.

IAP low

GENERAL REQUIREMENTS: During the overall identity proofing and authenticator issuing process, the CSP ensures that the Person accomplishing each step of the process is the same Person throughout the process. The CSP also ensures that the proofing process's procedures are documented and followed, and that the documented procedures address how the CSP meets all applicable criteria for each IAP level supported.

The CSP maintains records of the identity proofing and authenticator issuing process each time it is enacted, to include recording: when the Person was identity-proofed, who was proofed, and at what IAP level the proofing was done. Each record should be preserved in accordance with local record-retention guidelines.

EVIDENCE, VALIDATION, AND VERIFICATION: At IAP low, a Claimant's self-assertion of their identity is acceptable and the Claimant need not present any identity evidence. Without presented evidence and given that the identity is self-asserted, there is no *validation* of evidence nor *verification* of ownership of the identity by the Claimant required at low. To satisfy the requirement that the Claimant is verified to be a Person, the Registrar may accomplish this by visually seeing the Claimant (e.g., face to face for In Person proofing and over a live video feed for Supervised Remote Proofing).

AUTHENTICATOR BINDING AND ISSUANCE: The Claimant must provide at least one piece of contact information. The Claimant must demonstrate control of any and all contact information provided during the identity proofing process, whether it is to be

used for notification purposes or is used in authenticator binding processes. If the CSP issues an authenticator to the Claimant during or after the identity proofing process, it must be delivered in a manner that can be assumed to have reached only the Claimant. Furthermore, if the CSP permits the Claimant to register a previously issued authenticator (either issued by the CSP in a prior context or by a third party that has been documented as acceptable by the CSP), then the Claimant must demonstrate control of the authenticator during the identity proofing process. Finally, the binding between the vetted identity and associated authenticators must be maintained in any follow-on authenticator management processes, such as: renewal, replacement, or removal of a vetted Person's existing authenticator; registering a new authenticator; or updating, adding, or removing contact information. In such cases, the binding is maintained by either re-accomplishing the full identity proofing process or by authenticating with a valid authenticator previously bound to the vetted identity.

IAP medium

In addition to the measures described in low, the following measures are required to achieve medium.

GENERAL REQUIREMENTS: At IAP medium, the Claimant-identifying attributes that were validated by the identity proofing process are also recorded.

EVIDENCE, VALIDATION, AND VERIFICATION: At IAP medium, the Claimant submits identity evidence to the Registrar. The identity evidence presented must be valid (i.e., unexpired) at the time of identity proofing. The evidence presented must be either:

(a) issued by a nationally recognized source,

(b) or a document nationally recognized as being valid for identification purposes,

(c) or a documented attestation of knowledge of their identity from an authority recognized by the CSP.

To validate that the evidence is genuine, IAP medium is satisfied with the registrar visually inspecting the evidence to check that it reasonably appears to be authentic. In order to verify that the Person owns the claimed identity, the presented identity evidence reasonably appears to belong to the Claimant.

IAP high

In addition to the measures described in medium, the following measures are required to achieve high.

GENERAL REQUIREMENTS: At IAP high, records are also kept of the values of one or more of the attributes that were validated and that uniquely identify the Claimant.

EVIDENCE, VALIDATION, AND VERIFICATION: At IAP high, as in IAP medium, the Claimant submits identity evidence to the Registrar. If the submitted evidence contains intrinsic security features, such as holograms, watermarks, electronically validated certificates, or other similar feature that meets the same anti-tamper/anti-forgery risk-reduction intent, then the Registrar checks them to validate genuineness. The Registrar further validates the evidence by checking with a trusted source that the identity claimed in the evidence exists and the evidence is still valid. Such validation checks may, but need not, take one of the following forms: an issuing or authoritative source confirms the validity of the identity evidence; transaction records of a recognized organisation providing financial, educational or utility services documents the existence of the claimed identity by confirming the identity's presence in those transactions; or the Registrar is able to directly obtain through secure means a written attestation of their knowledge of the identity from a separate person who has been previously identity proofed at a level of IAP high. Once the evidence is validated, no additional measures beyond medium are required to verify ownership of the claimed identity.

AUTHENTICATOR BINDING AND ISSUANCE: IAP high adds one requirement for authenticator binding and issuance beyond the requirements in IAP medium and IAP low: if the CSP issues an authenticator during or after the identity proofing process, it must be delivered only into the possession of the Claimant to whom it belongs.

B.1.2 Adjustments for Unsupervised Remote Proofing

For Unsupervised Remote Proofing, the following measures must be applied to the proofing process in addition to the measures described for in-person and remote supervised proofing.

CSPs may need to consider additional implementation measures on how to accomplish the requirements. For example, IAP low requires that the CSP ensure that the Claimant is a Person. This requirement does not change in the Unsupervised Remote context, but the CSP may need to add measures to confirm the Claimant is a Person. When the process is in-person, this is a trivial requirement in that the Registrar's interaction with the Claimant face to face confirms the Claimant is a Person. CSPs will need to determine how to fulfil the requirements when the process is remote and unsupervised.

IAP low

There are no additional requirements for IAP low beyond what is required for In-Person or Supervised Remote for an Unsupervised Remote process. However, CSPs will need to add implementation solutions to confirm the Claimant is a Person (such as a "robot check" or similar solution).

IAP medium

In addition to IAP medium in-person requirements, an Unsupervised Remote process requires that the Registrar further validate the evidence by checking with a trusted source that the identity claimed in the evidence exists and is not revoked. Such validation checks may, but need not, take one of the following forms: an issuing or authoritative source confirms the validity of the identity evidence; the Registrar confirms the presence of the claimed identity in transaction records of a recognized organisation providing financial, educational, or utility services; or the Registrar is able to directly obtain through secure means a written attestation of their knowledge of the identity from a separate person who has been previously identity proofed at a level of IAP high.

IAP high

In addition to IAP high in-person requirements, the following measures are required when the process is Unsupervised Remote.

In addition to the requirement for the Claimant to demonstrate control of any provided contact information, at least one piece of contact information must be verified by the Registrar to belong to the Claimant by a trusted source.

Furthermore, to satisfy the in-person requirement that the presented identity evidence reasonably appears to belong to the Claimant, the Registrar must accomplish one of the following:

> (a) a manual comparison of a photo or other biometric contained within a piece of validated identity evidence against a live video, photo or other biometric of the Claimant captured during the unsupervised remote portion of the proofing process; or
>
> (b) use an automated system to compare a photo or other biometric contained within a piece of validated identity evidence with a live video, photo or other biometric of the Claimant captured during the unsupervised remote portion of the proofing process, and the technology that does the comparison is deemed sufficient for this purpose by a nationally or internationally recognised authority.

B.2 Implementation Considerations

This section is informative.

The Table of normative IAP criteria does not prescribe implementation details or specific tools and technologies, but instead articulates requirements in a functional way in order to remain meaningful across international contexts and as technologies evolve over time.

This section is intended to provide illustrative examples and discussion of how to implement RAF. These examples and discussion points show how certain aspects

of the normative criteria can be interpreted for implementation, but are not intended to be comprehensive.

Building on a Third Party's Identity Assurance Claim

The CSP may base its IAP claim on a comparable or better level of identity proofing of the Claimant performed by a third party known to be sufficient for this purpose, such as a nationally accepted identity proofing service or an accepted third-party identity proofing solution that meets or exceeds RAF standards, and the CSP's process securely links the Claimant with the subject of that third party's identity assurance claim. Typically, this secure linkage is demonstrated through successful authentication by the Claimant using an authenticator provided by that third party. If the third party authenticator is to be the basis for an IAP high claim, then the authentication must use MFA or be otherwise comparably strong. Criteria in the IE, VA, VF, and UR groups may be ignored when this approach is used.

Appendix A.2 above may be useful in determining whether a third party identity proofing claim meets or exceeds a corresponding RAF IAP claim.

Demonstrating Control of Contact Information

Criterion [AB1] specifies that the Claimant must demonstrate control of any contact information provided during the identity proofing process. Examples of contact information include but are not limited to: an email address, a phone number, a text or social media account, or physical mailing address. Demonstration of control may be accomplished by the Registrar sending a confirmation code or link to that address, and having the Claimant confirm by being able to retrieve and provide the code, or click on the provided link. Another example that could be used in an in-person identity proofing process for a phone number could be for the Registrar to call or SMS to the provided number and the Claimant demonstrate control of the phone number (for example by repeating a phrase or passcode communicated). The Registrar need not follow these specific examples, and may develop other ways of validating Claimant's control of the contact information provided.

Different contact methods (email, phone number, postal address, direct message, etc) may have different expected timelines. If a confirmation code is sent, the Registrar will need to consider the expiration timeframe for that confirmation code. What may make sense for an SMS text or email (minutes) does not make sense for a code sent through the postal service (days).

Recommended expiration times for validation codes based on various contact methods:

- Postal Mail: <=10 days

- Electronic Means (via whatever mechanism): <=10 minutes

Registrars will need to consider typical service standards in their location (e.g. longer postal delivery times may be needed in some locations).

Validating Intrinsic Security Features of Identity Evidence

In [VA3], the Registrar is required to check the validity of intrinsic security features if any are present. Examples of intrinsic security features range from physical anti-tamper characteristics such as holograms, watermarks, laser etching, etc. to digital anti-tamper characteristics such as an embedded chip containing a cryptographically signed form of the presented identity data that can be checked against the issuing source.

The UK Government Digital Service published "How to prove and verify someone's identity" [UKGDS], which provides practical guidance on several aspects of identity proofing. Each of its sections describe how to achieve progressively more stringent checks, assigning scores of 1-4 accordingly. The section "Check the evidence is genuine or valid" is a good compilation of means to validate identity evidence, either in-person or remotely. Achieving a score of 2 satisfies [VA3].

Validation and verification during an unsupervised remote identity proofing session may need to rely on special purpose systems designed to perform validation checks of identity evidence and to verify that the Person being proofed matches a photo on a piece of validated identity evidence. Such systems are becoming increasingly available in some jurisdictions.

For example, in the US, the Kantara Initiative assesses commercial providers of such services Kantara's Trust Status List [Kantara TSL] identifies these services. These, together with third parties identified in supporting material on which some of them rely in turn, provide a starting point for US based organisations thinking about implementing unsupervised remote identity proofing at IAP high. Some of those providers also operate outside of the US.

Identity Evidence and Photo IDs

This framework does not explicitly require a "government-issued photo ID". This is because not every nation uses photo ID cards as their primary means of identification. Furthermore, technology has evolved such that a government issued card may be verified via other cryptographic or biometric means that may exceed the requirements in RAF. Given that technology evolves and different nations may have different approaches and standards, the RAF framework attempts to state "what" is required at an assurance level without prescribing "how".

However, a CSP's implementation may require a government-issued photo ID.

For example, in most in-person cases, the simplest way to meet IAP medium requirements is to compare a government-issued Photo ID with the Person. In some locations a government-issued photo ID may be the only evidence that enables the Registrar to easily meet all the validation and verification requirements.

Finally, a point about "presented evidence", which implies the Claimant must present the evidence themselves. While this is likely to be the case, there may be instances where CSPs have solutions where the evidence is presented through other means. It is not the intent of this framework to limit creative solutions that meet or exceed the criteria.

Appendix C: Example Assurance Values

This section is informative.

A University that guarantees that its faculty members (as defined in [eduPerson])

1. have unique non-reassignable identifier values,
2. are ID-proofed face-to-face using a government-issued photo-ID and the attributes on the photo-ID are checked against an authoritative source, and
3. are authorised to upload grades to their student information system,

and for which the institution

4. promptly reflects departure or role change into eduPerson affiliation value(s),
5. uses an identity management system which qualifies to the baseline expectations for Identity Providers, and
6. implements an identity proofing process which conforms to RAF 2.0 process-based criteria

will assert the following claims for its faculty members as multiple values of the eduPersonAssurance attribute:

Claim	**Reason**
`https://refeds.org/assurance/version/2`	(6) above**,** Section 4
`https://refeds.org/assurance`	(5) above, Section 3

https://refeds.org/assurance/ID/unique	(1) above
https://refeds.org/assurance/IAP/local-enterprise	(3) above
https://refeds.org/assurance/IAP/high	(2) above, Section 5.2.1
https://refeds.org/assurance/IAP/medium	Section 5.2.1
https://refeds.org/assurance/IAP/low	Section 5.2.1
https://refeds.org/assurance/ATP/ePA-1d	(4) above
https://refeds.org/assurance/ATP/ePA-1m	Section 5.3
https://refeds.org/assurance/profile/cappuccino	Section 6
https://refeds.org/assurance/profile/espresso	Section 6