REFEDS ASSURANCE FRAMEWORK (RAF) 2.0

It’s (almost) here!

Kyle Lewis

Agenda

Background

- *What is the RAF?*
- *Why 2.0?*

RAF 2.0 Orientation

- *Elements of RAF*
  - Conformance Criteria
  - Identifier Uniqueness
  - Identity Assurance Profiles
  - Attribute Freshness
- *Versioning Compatibility*
- *Relationship to other Assurance Profiles*

Pointers and Q&A

What's a RAF?

REFEDS Assurance Framework (RAF)

"To manage risks related to federated access to their services, some Relying Parties in research and education federations must decide how much confidence they need in the assertions made by the Identity Providers. This document specifies a framework for articulating such assurances and their expression by the Credential Service Provider to the Relying Party using common identity federation protocols."

RAF addresses the following components

- *Identifier Uniqueness* - a method to communicate to the RP that the user's identifier (such as a login name) is unique, and is only bound to one identity in the CSP's context.
- *Identity Assurance* - a method to communicate to the RP how certain the CSP was at enrollment time 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.
- *Attribute Assurance* - a method to communicate to the RP regarding the quality and freshness of attributes (other than the unique identifier) passed in the login assertion.

The Framework

RAF consists of a series of claims formatted as URIs

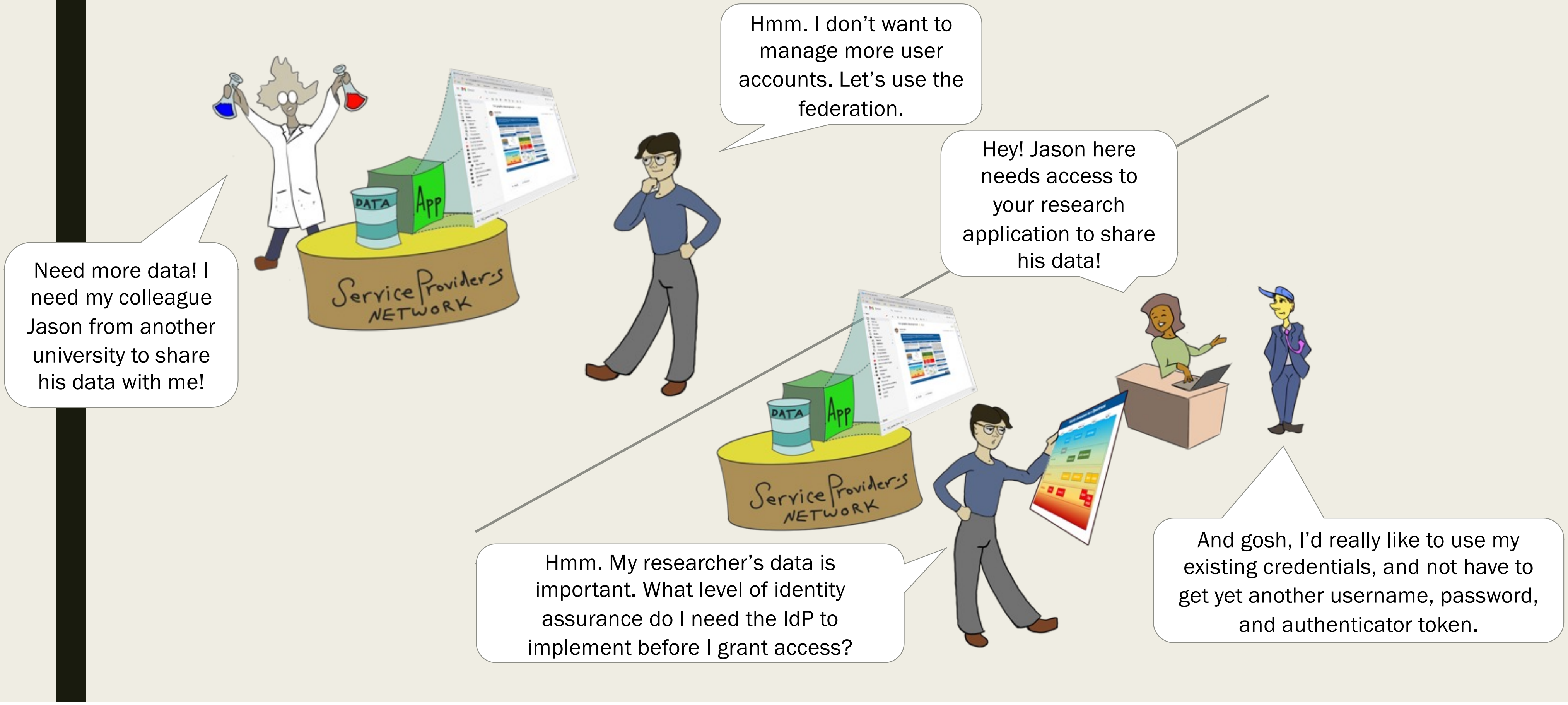
URIs are intended for inclusion in the REFEDS eduPersonAssurance attribute.

- *Example:* eduPersonAssurance: https://refeds.org/assurance

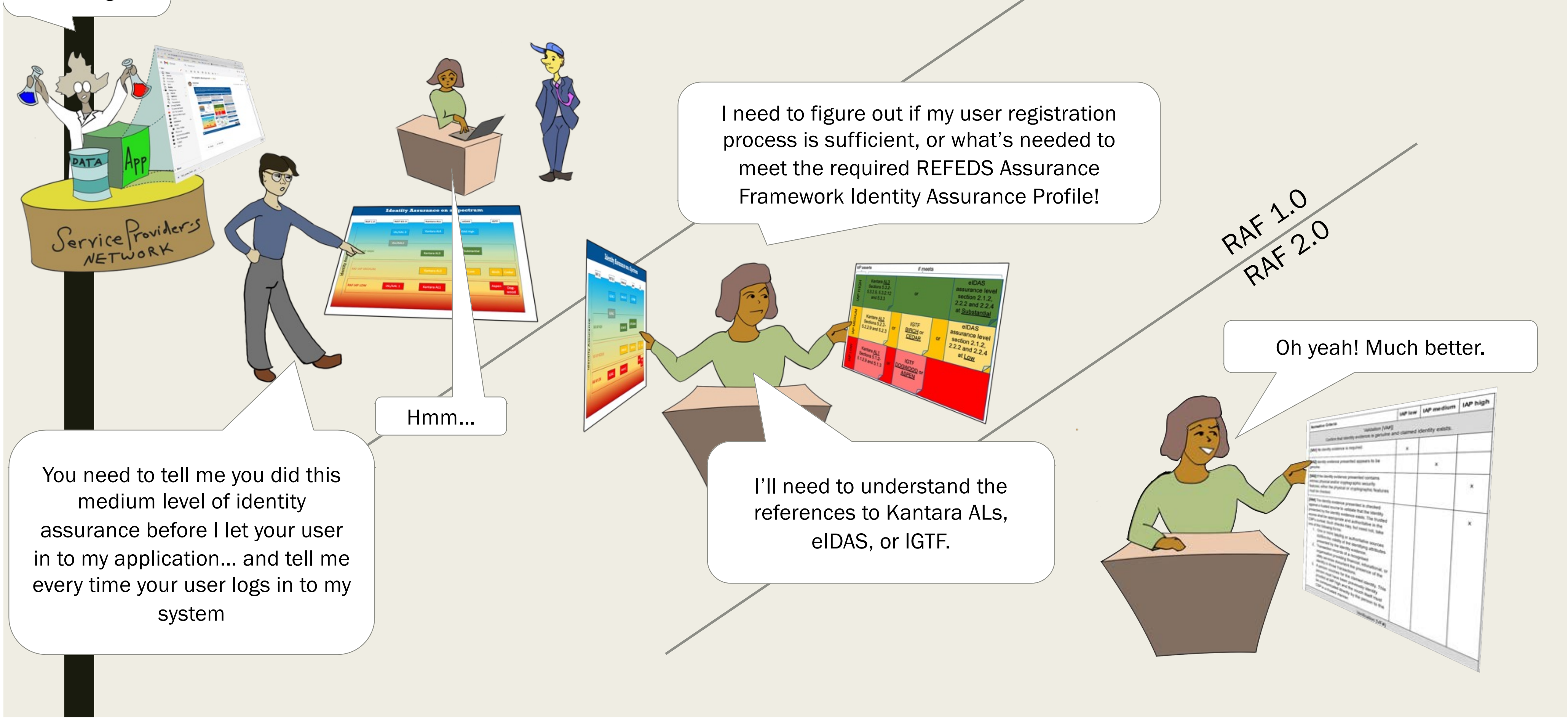
The RAF framework specifies a series of assertions, and what claims an IdP is making by including these assertions in eduPersonAssurance

The RPs can use these claims to make risk-based access decisions

Relying Party's Perspective


Need more data! I need my colleague Jason from another university to share his data with me!
DATA
App
Service Provider's NETWORK
Hmm. I don't want to manage more user accounts. Let's use the federation.
Hey! Jason here needs access to your research application to share his data!
DATA
App
Service Provider's NETWORK
Hmm. My researcher's data is important. What level of identity assurance do I need the IdP to implement before I grant access?
And gosh, I'd really like to use my existing credentials, and not have to get yet another username, password, and authenticator token.

Credential Service Provider’s Perspective


IT Minion! What’s taking so long?
DATA
App
Service Provider’s NETWORK
You need to tell me you did this medium level of identity assurance before I let your user in to my application… and tell me every time your user logs in to my system
Identity Assurance on a spectrum
Hmm…
I need to figure out if my user registration process is sufficient, or what’s needed to meet the required REFEDS Assurance Framework Identity Assurance Profile!
I’ll need to understand the references to Kantara ALs, eIDAS, or IGTF.
RAF 1.0
RAF 2.0
Oh yeah! Much better.
IAP low
IAP medium
IAP high

Take Two to 2.0

- 2020 Fall: identified need to update RAF 1.0,
  in particular the Identity Assurance Profiles (IAPs)
- RAF 2.0 goals:
  1. *tighten definitions of many claims based on field experience with RAF 1.0*
  2. *provide a single set of criteria defining the IAP claims of low, moderate, and high*
     1. Avoid need for the CSP to refer to one of several external standards
     2. Reduce ambiguity for RPs’ understanding of what each IAP claim actually means
- 2021 Jan: RAF WG began developing RAF 2.0
- 2023 Jun-Aug: RAF 2.0 Public Consultation
- 2023 Aug-Sep: Incorporate public consultation inputs,
  make ready for REFEDS Steering Committee
- 2023 October/November: Target to release RAF 2.0

Agenda

Background

- *What is the RAF?*
- *Why 2.0?*

RAF 2.0 Orientation

- *Elements of RAF*
  - Conformance Criteria
  - Identifier Uniqueness
  - Identity Assurance Profiles
  - Attribute Freshness
- *Versioning Compatibility*
- *Relationship to other Assurance Profiles*

Pointers and Q&A

Conformance Criteria (The minimum)

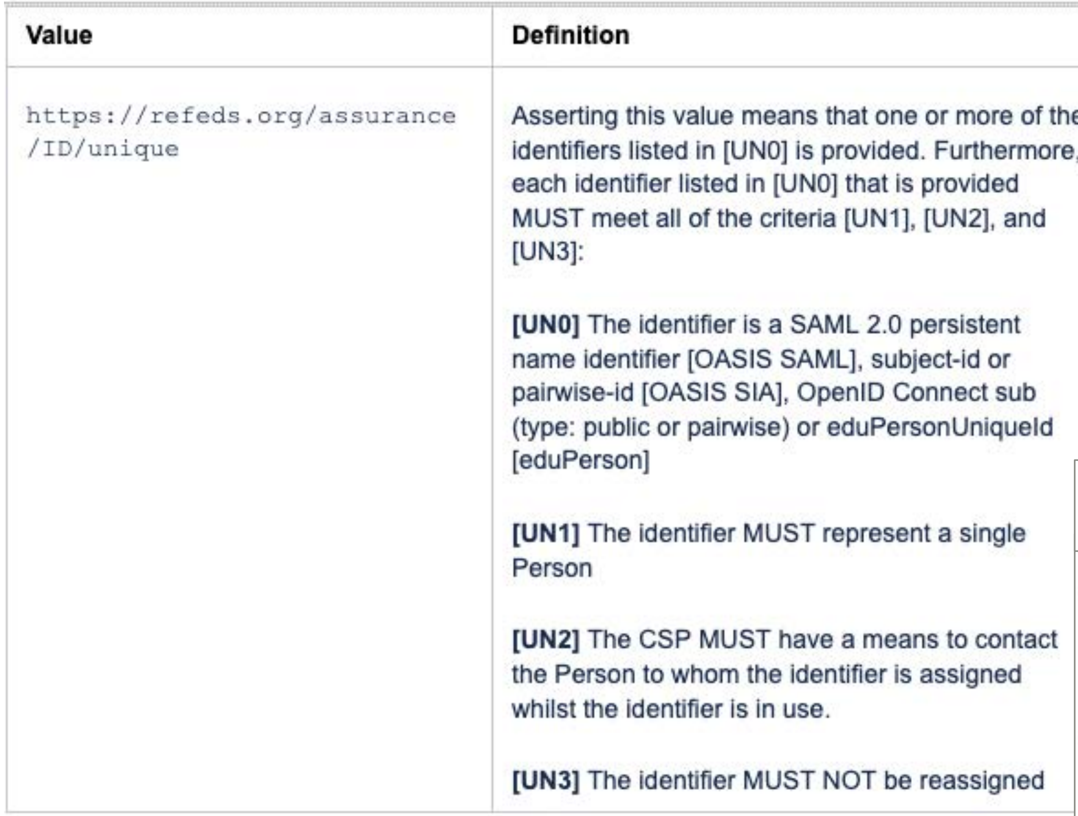
Minimum assertion: https://refeds.org/assurance

This claim means the IdP conforms to REFEDS Baseline Expectations for IdPs:

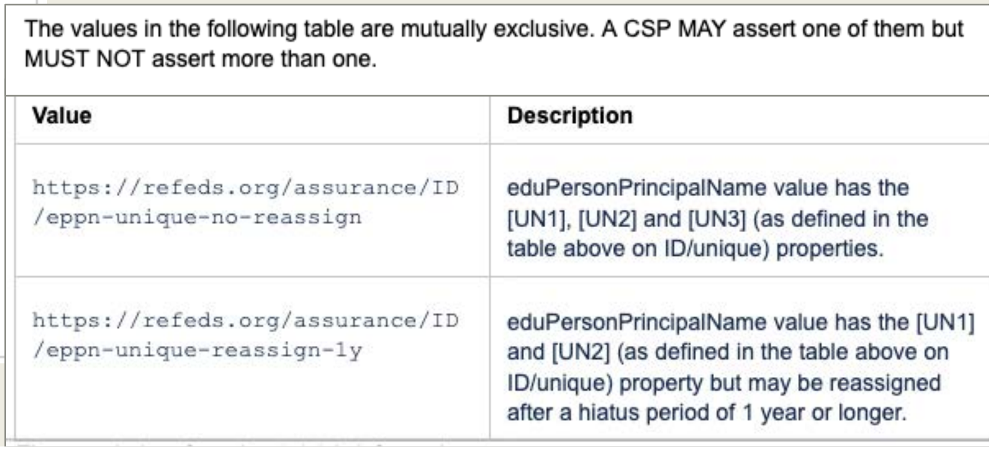
- *Your IdP operates with organizational level authority*
- *Your IdP is trusted enough to be used to access your organization's own systems*
- *You publish contact info for your IdP and respond in a timely fashion*
- *You apply security practices to protect user info, safeguard transaction integrity, and ensure timely incident response*
- *You ensure metadata registered in Federation is complete, accurate, and up to date.*

CSP may release nothing more than this. If any other values are released (detailed in upcoming slides), this claim must also be released.

Uniqueness



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



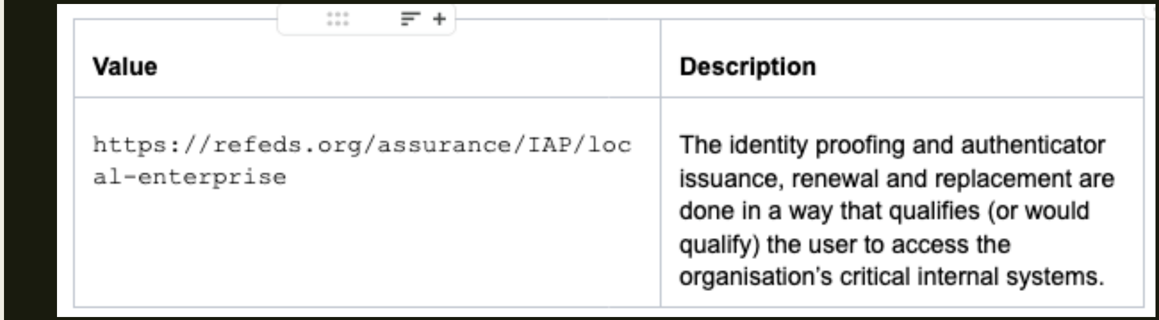
The values in the following table are mutually exclusive. A CSP MAY assert one of them but MUST NOT assert more than one.

Value	Description
https://refeds.org/assurance/ID/eppn-unique-no-reassign	eduPersonPrincipalName value has the [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.

Identity Assurance Profiles (IAPs)

- Risk-Based Identity Assurance
  - *IAP/local-enterprise*
- Process-Based Identity Assurance
  - *IAP/high*
  - *IAP/medium*
  - *IAP/low*

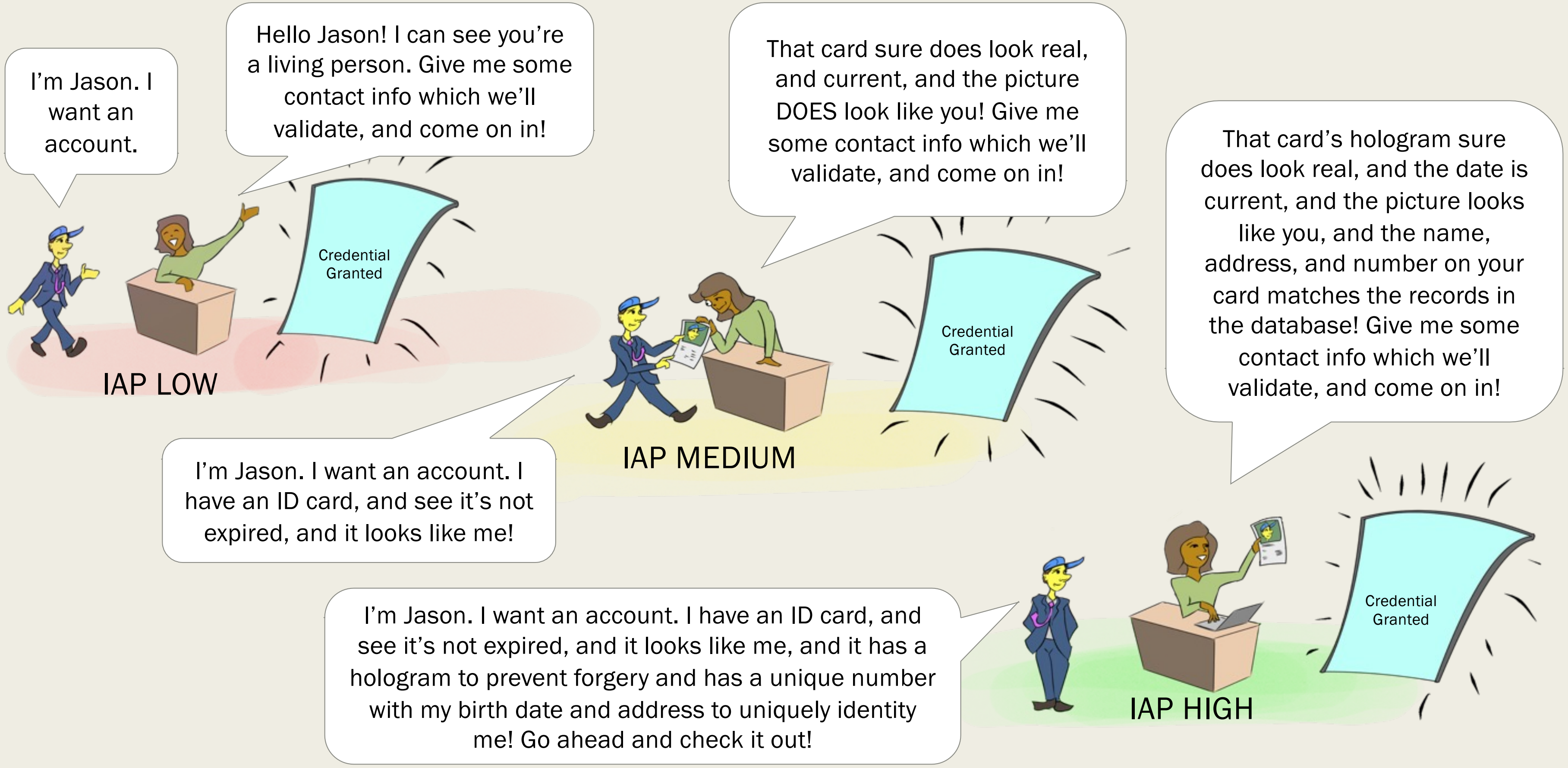
Risk-Based Identity Assurance Profile local-enterprise

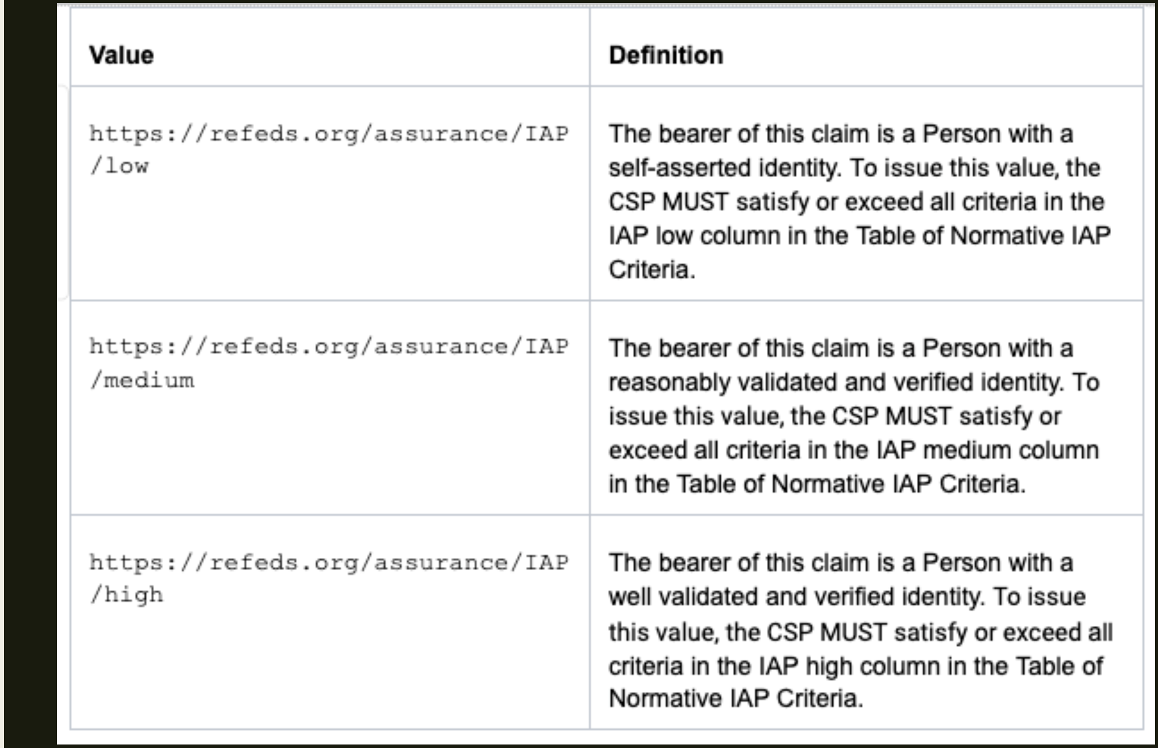


Value	Description
`https://refeds.org/assurance/IAP/local-enterprise`	The identity proofing and authenticator issuance, renewal and replacement are done in a way that qualifies (or would qualify) the user to access the organisation's critical internal systems.

- This is NOT saying the user in question has access to the organization’s critical information systems
- Examples
  - *“This student user went through the same identity checking and account issuing as our users who have access to our institution’s financial accounts.”*
  - *“We’re just as sure of this user’s identity as we are of our HR personnel who access HR records.”*
- This is an example of a kind of “transitive trust” or “reciprocity”; up to RP/SP to determine if this is sufficient

Process-based IAPs – Thumbnail Examples


I’m Jason. I want an account.
Hello Jason! I can see you’re a living person. Give me some contact info which we’ll validate, and come on in!
Credential Granted
IAP LOW
I’m Jason. I want an account. I have an ID card, and see it’s not expired, and it looks like me!
That card sure does look real, and current, and the picture DOES look like you! Give me some contact info which we’ll validate, and come on in!
Credential Granted
IAP MEDIUM
I’m Jason. I want an account. I have an ID card, and see it’s not expired, and it looks like me, and it has a hologram to prevent forgery and has a unique number with my birth date and address to uniquely identity me! Go ahead and check it out!
That card’s hologram sure does look real, and the date is current, and the picture looks like you, and the name, address, and number on your card matches the records in the database! Give me some contact info which we’ll validate, and come on in!
Credential Granted
IAP HIGH



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.

Process-based Identity Assurance Profiles

- Each level's requirements are detailed in a "car buyer's chart" type of table: the Table of Normative IAP Criteria
- Appendix B identifies that other equivalent frameworks may be used to claim IAP levels, without strict adherence to the Table of Normative IAP Criteria
  - *E.g. if you are already eIDAS's Superior or NIST 800-63a's IAL-2, you may claim IAP high without having to study the table of requirements*

3 Kinds of Process-based Identity Proofing

In-Person

- ‘Simplest’ to assure

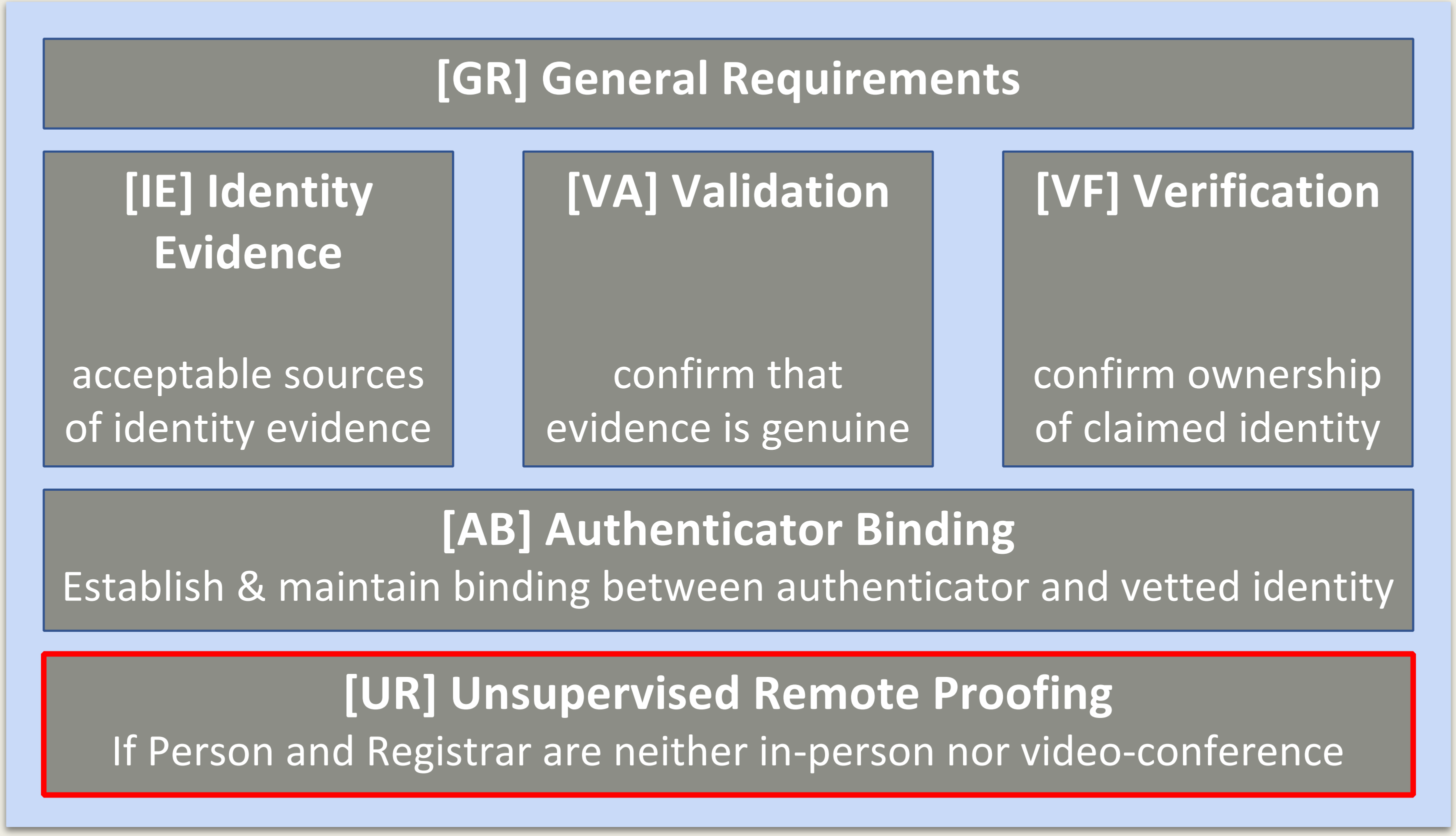
Remote Supervised

- Registrar has live agent involved in the process, in real-time or asynchronously

Remote Unsupervised

- Process is automated; account granted to successful applicant without Registrar ‘live human’ review

Body of RAF IAP Process Requirements



[GR] General Requirements

[IE] Identity Evidence

acceptable sources of identity evidence

[VA] Validation

confirm that evidence is genuine

[VF] Verification

confirm ownership of claimed identity

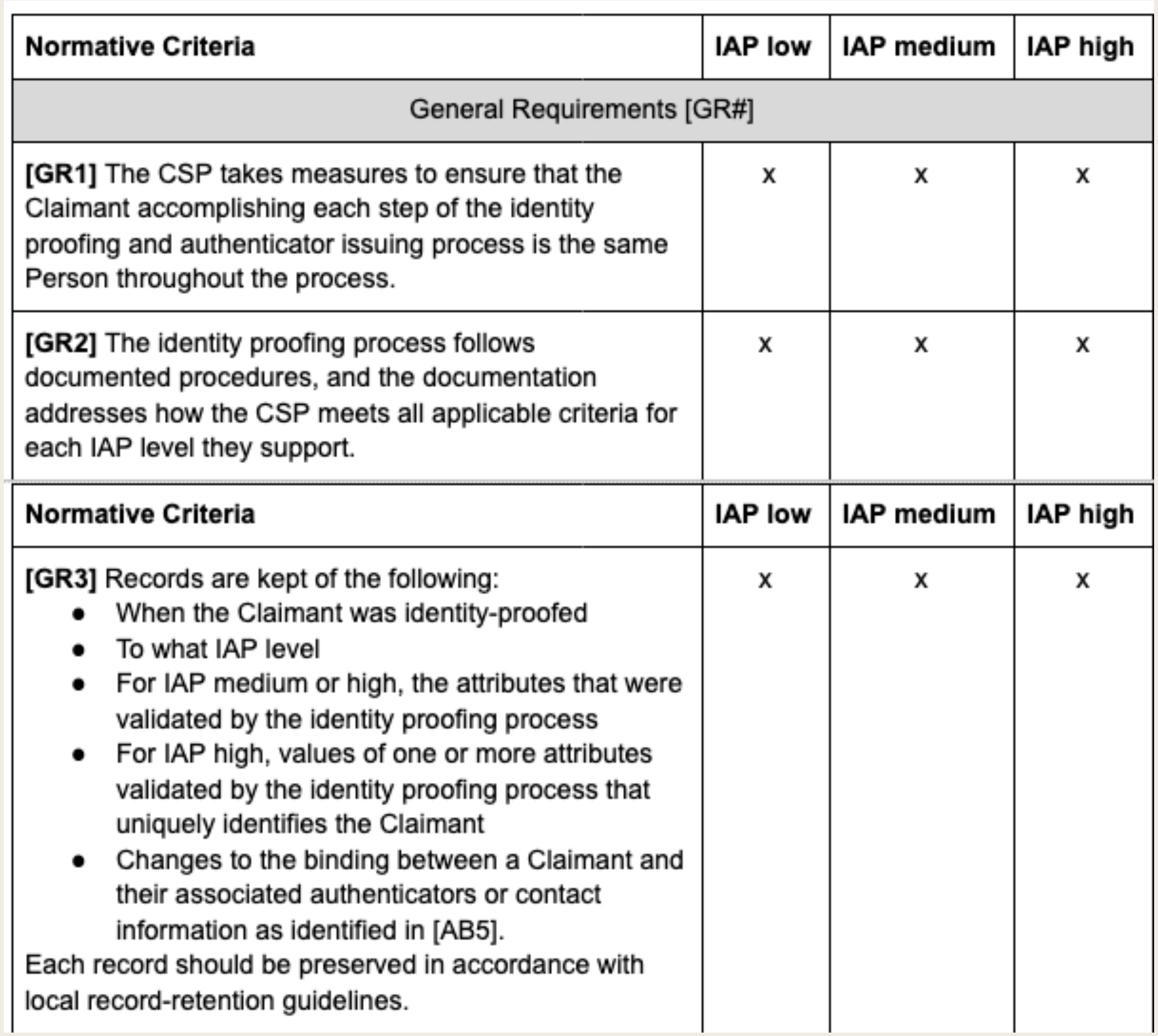
[AB] Authenticator Binding

Establish & maintain binding between authenticator and vetted identity

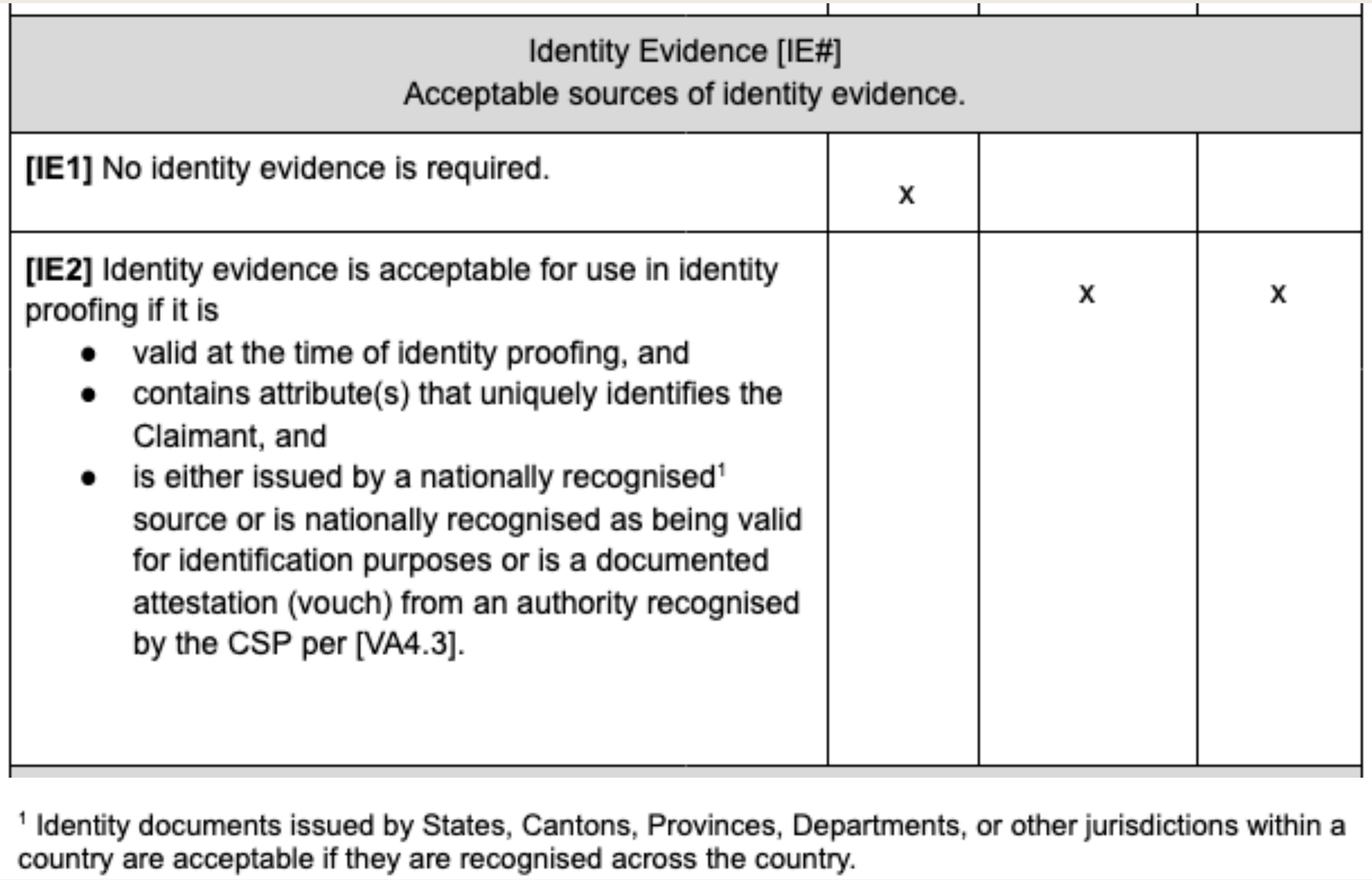
[UR] Unsupervised Remote Proofing

If Person and Registrar are neither in-person nor video-conference

Table of Normative IAP Criteria

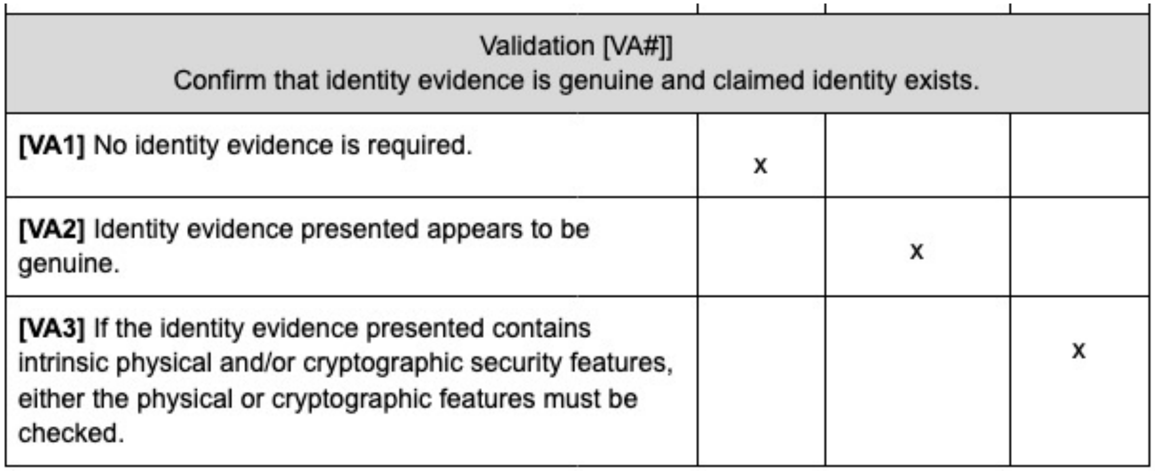


Normative Criteria	IAP low	IAP medium	IAP high
General Requirements [GR#]			
[GR1] The CSP takes measures to ensure that the Claimant accomplishing each step of the identity proofing and authenticator issuing process is the same Person throughout the process.	x	x	x
[GR2] The identity proofing process 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 ● For IAP medium or high, the attributes that were validated by the identity proofing process ● For IAP high, values of one or more attributes validated by the identity proofing process that uniquely identifies the Claimant ● Changes to the binding between a Claimant and their associated authenticators or contact information as identified in [AB5]. Each record should be preserved in accordance with local record-retention guidelines.	x	x	x

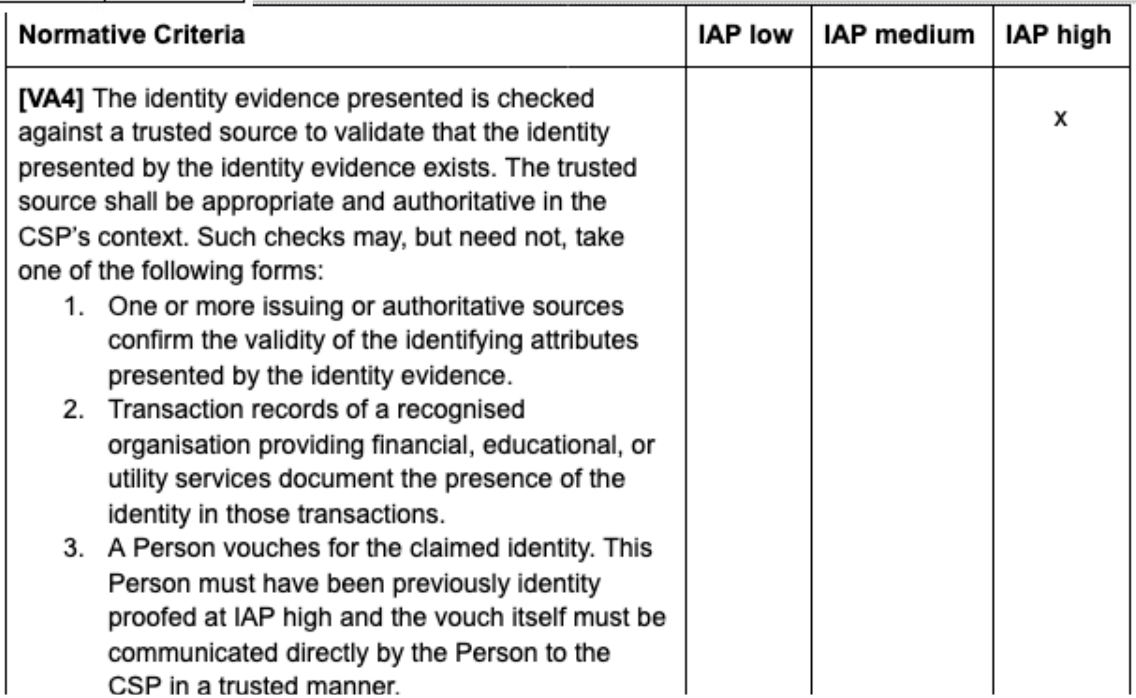


Identity Evidence [IE#] Acceptable sources of identity evidence.			
[IE1] No identity evidence is required.	x		
[IE2] Identity evidence is acceptable for use in identity proofing if it is ● valid at the time of identity proofing, and ● contains attribute(s) that uniquely identifies the Claimant, and ● is either issued by a nationally recognised[1] source or is nationally recognised as being valid for identification purposes or is a documented attestation (vouch) from an authority recognised by the CSP per [VA4.3].		x	x

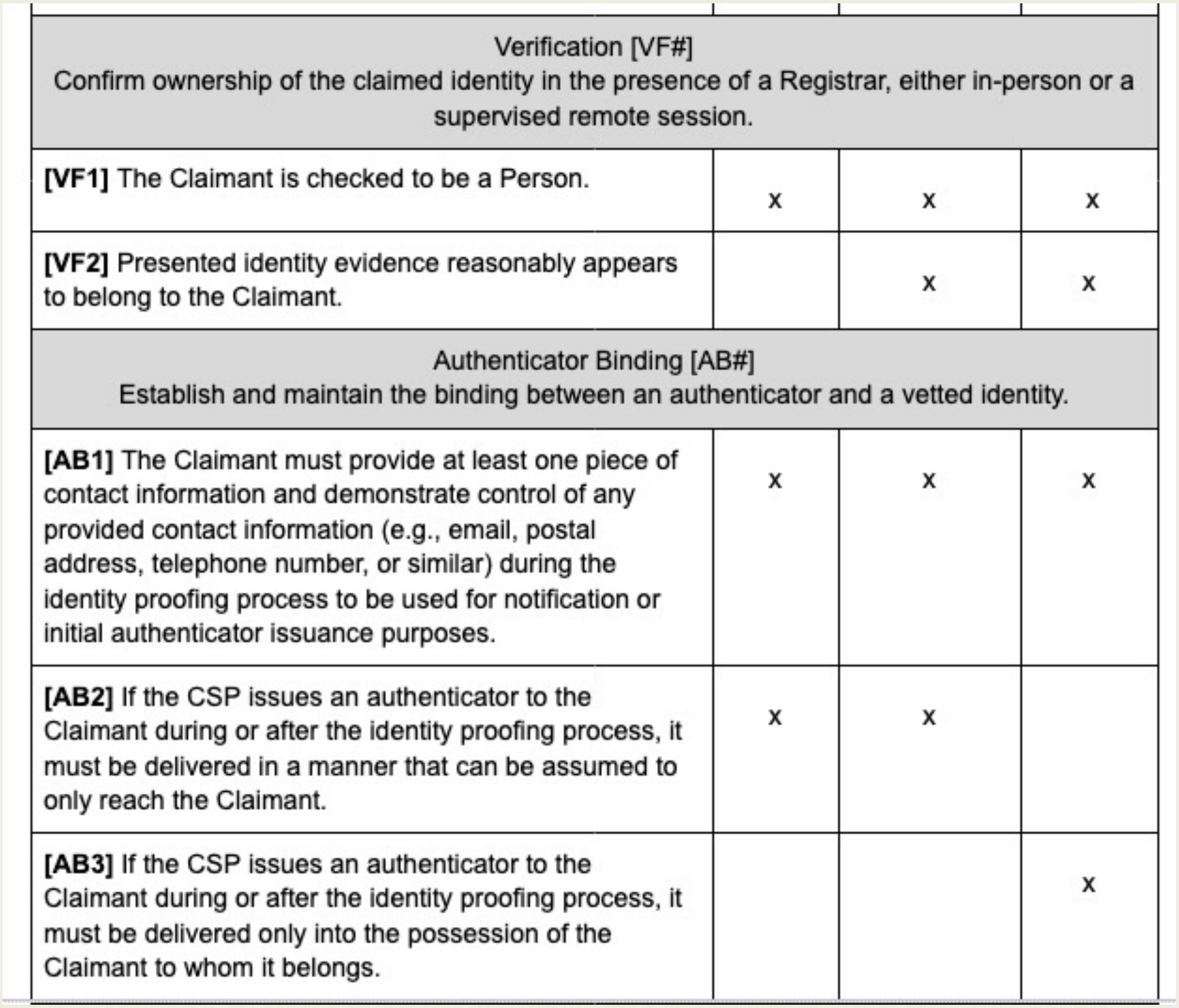
[1] Identity documents issued by States, Cantons, Provinces, Departments, or other jurisdictions within a country are acceptable if they are recognised across the country.



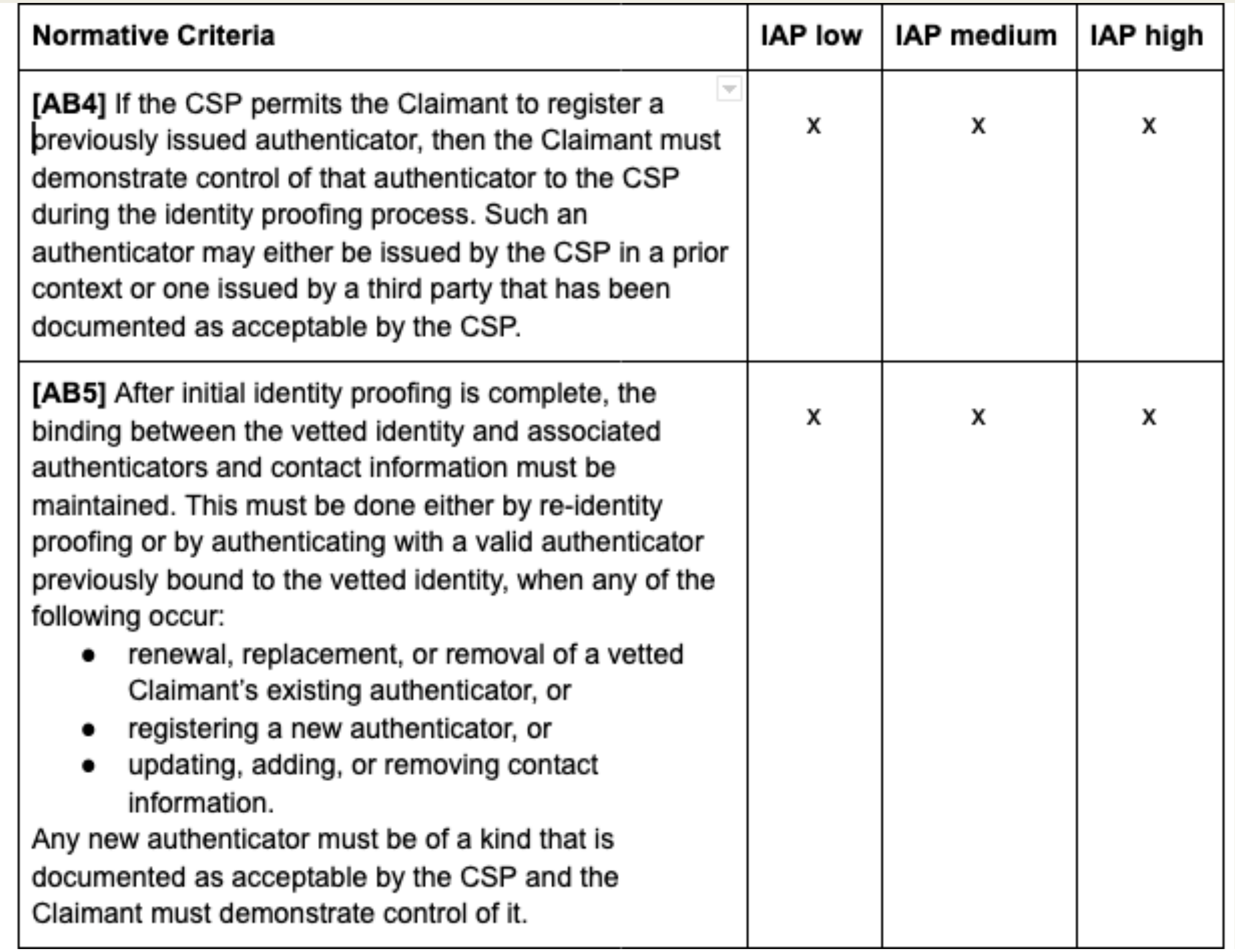
Validation [VA#]] Confirm that identity evidence is genuine and claimed identity exists.			
[VA1] No identity evidence is required.	x		
[VA2] Identity evidence presented appears to be genuine.		x	
[VA3] If the identity evidence presented contains intrinsic physical and/or cryptographic security features, either the physical or cryptographic features must be checked.			x



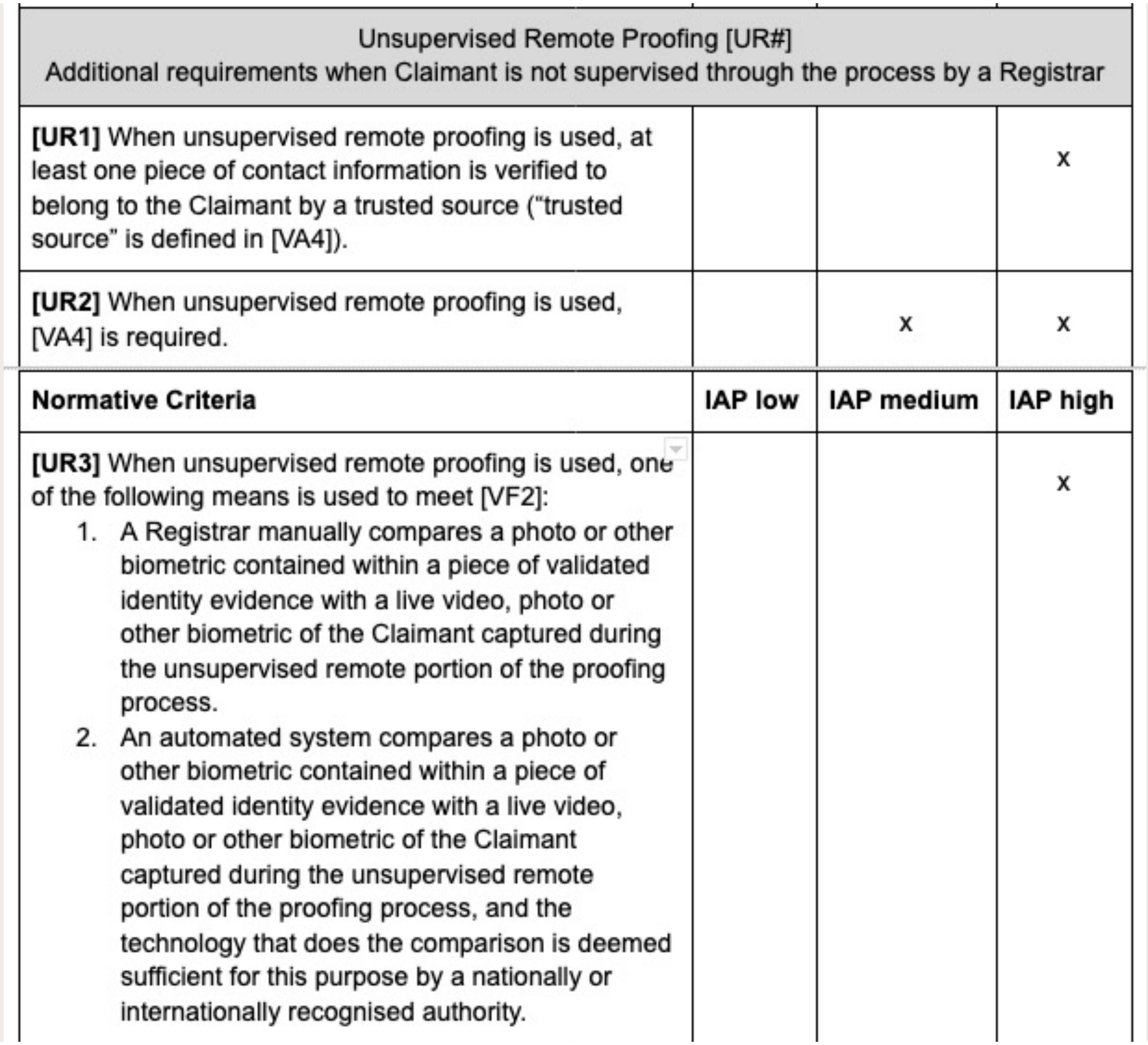
Normative Criteria	**IAP low**	**IAP medium**	**IAP high**
[VA4] The identity evidence presented is checked against a trusted source to validate that the identity presented by the identity evidence exists. The trusted source shall be appropriate and authoritative in the CSP's context. Such checks may, 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. Transaction records of a recognised organisation providing financial, educational, or utility services document the presence of the identity in those transactions. 3. A Person vouches for the claimed 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.			x



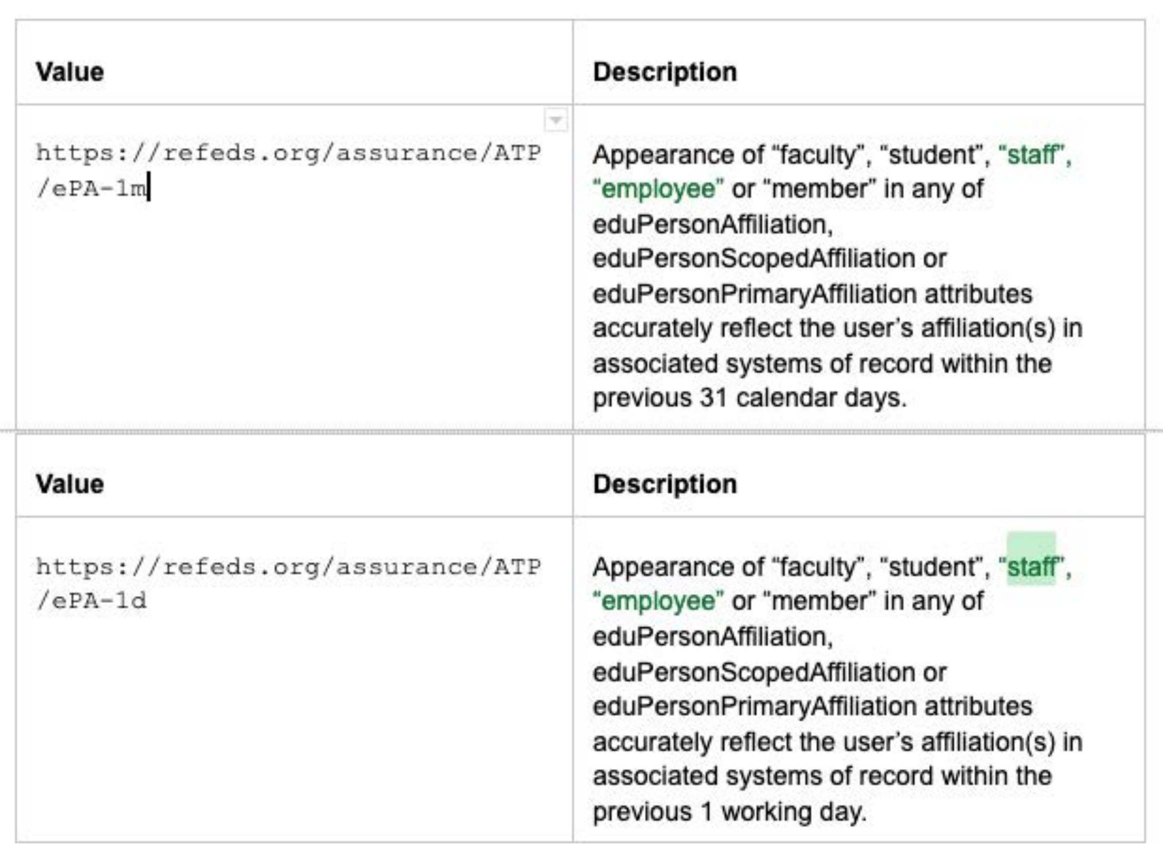
Verification [VF#] Confirm ownership of the claimed identity in the presence of a Registrar, either in-person or a supervised remote session.			
[VF1] The Claimant is checked to be a Person.	x	x	x
[VF2] Presented identity evidence reasonably appears to belong to the Claimant.		x	x
Authenticator Binding [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	
[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



Normative Criteria	IAP low	IAP medium	IAP high
[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



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
Normative Criteria	**IAP low**	**IAP medium**	**IAP high**
[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



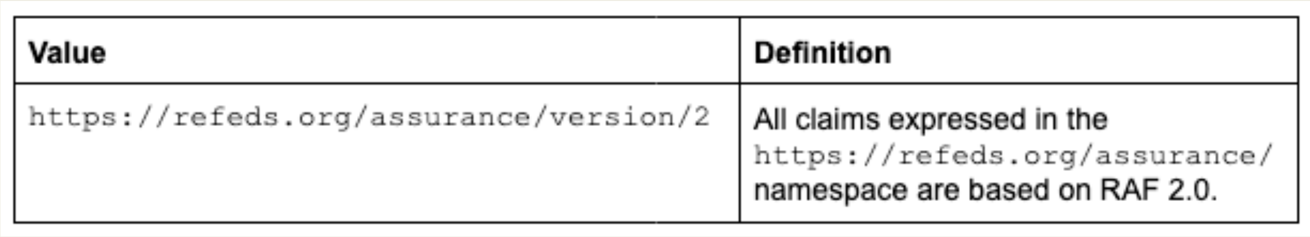
Value	Description
https://refeds.org/assurance/ATP/ePA-1m	Appearance of "faculty", "student", "staff", "employee" or "member" in any of eduPersonAffiliation, eduPersonScopedAffiliation or eduPersonPrimaryAffiliation attributes accurately reflect the user's affiliation(s) in associated systems of record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

Value	Description
https://refeds.org/assurance/ATP/ePA-1d	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 1 working day.

Attribute Quality and Freshness

- No change from 1.0 to 2.0 other than to expand to 'employee' and 'staff'
- 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)

Versioning Compatibility



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

- RAF 1.0 claims are ‘upward compatible’ with RAF 2.0, except IAPs low, medium, and high
  - *Example: Under RAF 1.0, a CSP could claim IAP High based on the Kantara specs… and have a remote automated proofing session with no biometric (or equivalent) check … this specific case does not meet RAF 2.0*
- Appendix A has a detailed ‘risk gap’ discussion on the version differences, in order to aid RPs risk-based decisions on whether to require 2.0 or not
- Appendix A has a “transition” guide for CSPs who currently implement RAF 1.0, in order to help the CSP determine if they already qualify for RAF 2.0, or which additional steps they need to add… based on how they implemented RAF 1.0 (eIDAS, Kantara, or IGTF)

RAF’s relationship to other assurance profiles

- RAF makes claims about the attributes themselves (quality and freshness), and the identity proofing included in the account issuance process as a single point in time…
- …assurance at account issuing is preserved with strong authentication methods, in order to protect ownership of the account throughout it’s lifecycle.
  - *These other frameworks are out of scope for RAF, but should be implemented in concert*
  - *Example: REFEDS MFA Profile*

Agenda

Background

- *What is the RAF?*
- *Why 2.0?*

RAF 2.0 Orientation

- *Elements of RAF*
  - Conformance Criteria
  - Identifier Uniqueness
  - Identity Assurance Profiles
  - Attribute Freshness
- *Versioning Compatibility*
- *Relationship to other Assurance Profiles*

Pointers and Q&A

Tips and Pointers for CSPs

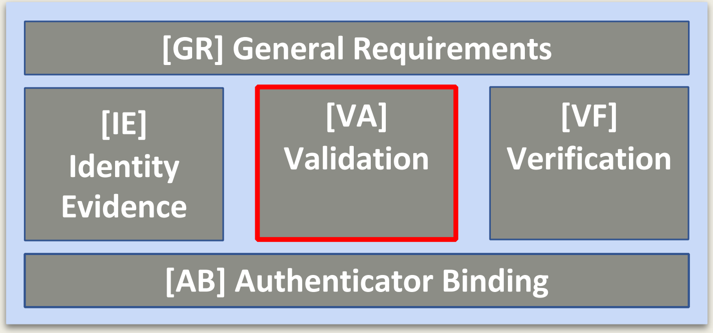
- You don’t have to assign the same IAP levels or other claims to all users
- Assess your current process and determine what claims can be made without having to change processes … Assign existing user community to each claim already achieved
- Develop an ‘upgrade’ path if users need to qualify for a higher IAP level
- Tweak existing processes for future new users as appropriate
- If you’re in InCommon, you can assert the Conformance Criteria today!

Q&A / DISCUSSION

BACKUP SLIDES

Identity Evidence, Validation & Verification

low:	no evidence documents
medium:	seems genuine
high:	checked to be genuine & against trusted source

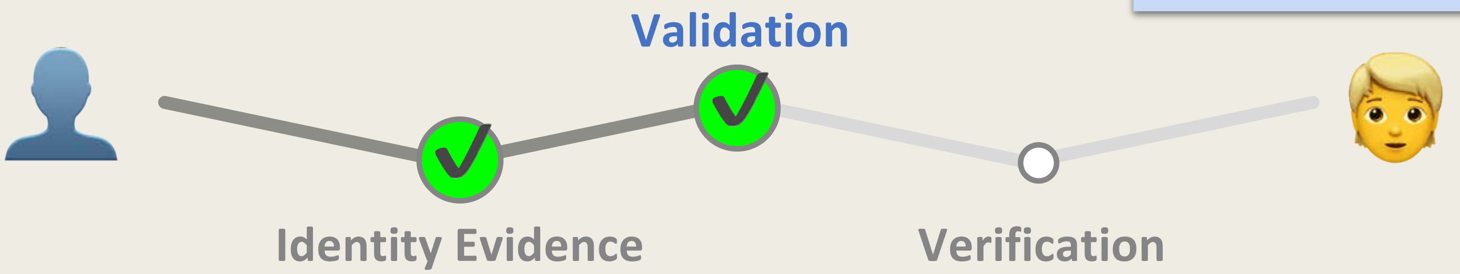

[GR] General Requirements

[IE] Identity Evidence

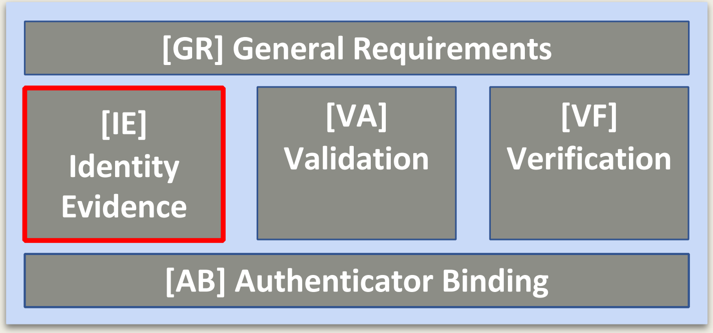
[VA] Validation

[VF] Verification

[AB] Authenticator Binding



Identity Evidence, Validation & Verification



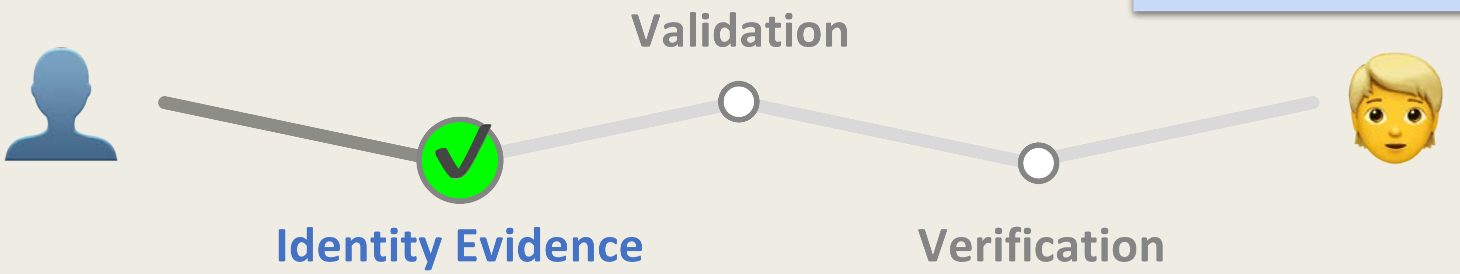
[GR] General Requirements

[IE] Identity Evidence

[VA] Validation

[VF] Verification

[AB] Authenticator Binding



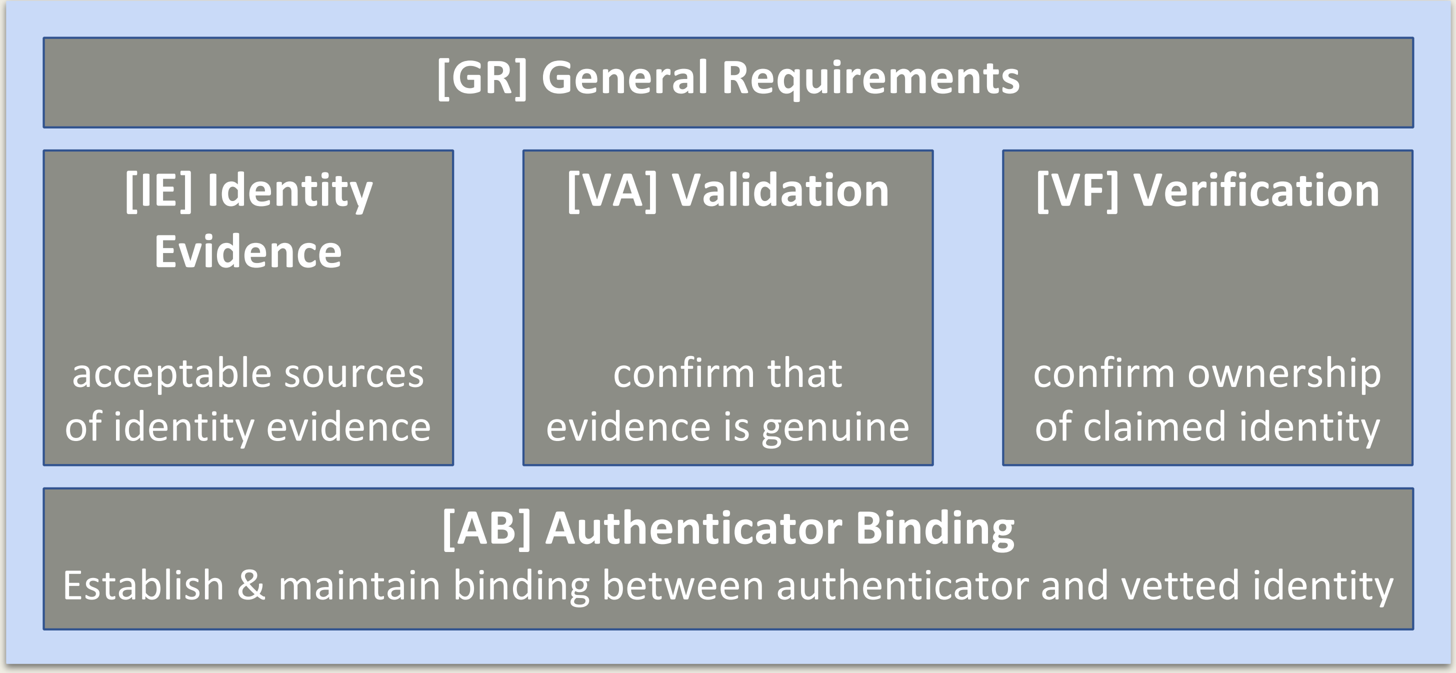
Validation

Identity Evidence

Verification

low:	no evidence
medium:	valid & recognised
high:	valid, recognised & security features

In Person & Supervised Remote Proofing



[GR] General Requirements

[IE] Identity Evidence

acceptable sources of identity evidence

[VA] Validation

confirm that evidence is genuine

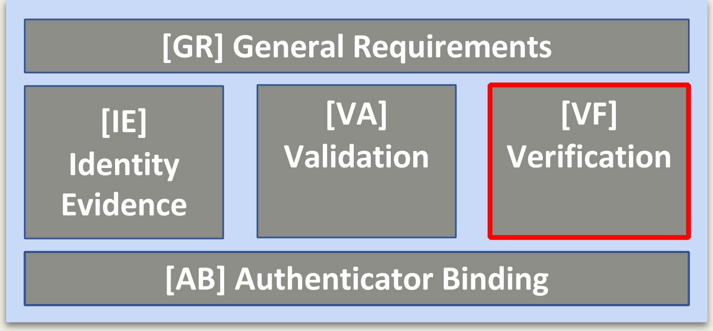
[VF] Verification

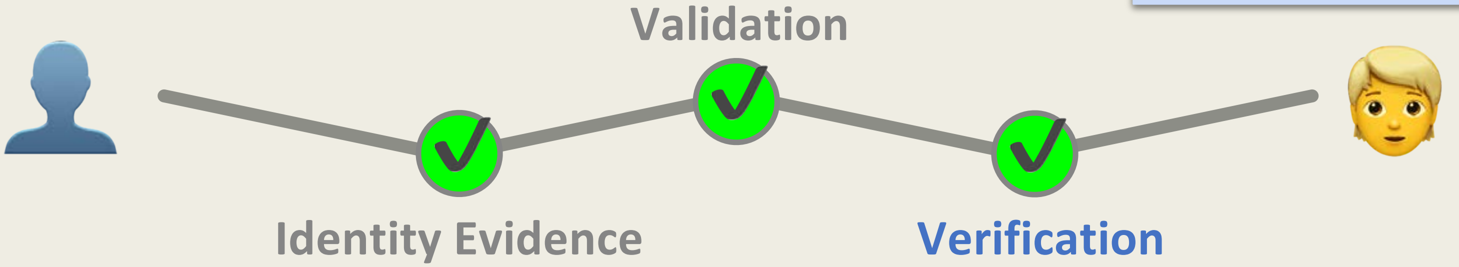
confirm ownership of claimed identity

[AB] Authenticator Binding

Establish & maintain binding between authenticator and vetted identity

Identity Evidence, Validation & Verification



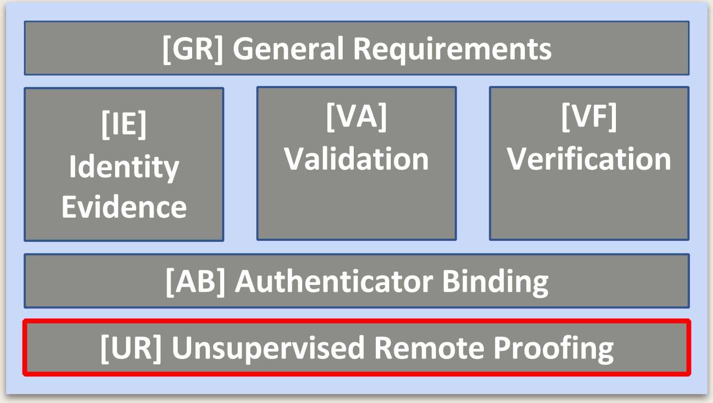


low: Claimant is a Person

medium/ high: Claimant is a Person & identity evidence reasonably belongs to Claimant

Unsupervised Remote Proofing

- e.g. fully automated proofing process
- Additional measures to accomplish IAP medium and high



[GR] General Requirements

[IE] Identity Evidence

[VA] Validation

[VF] Verification

[AB] Authenticator Binding

[UR] Unsupervised Remote Proofing

BUT, only implement [UR] if you have such process in place!

→ I.e., [UR] is not required to claim one of the IAP levels