Consultation: REFEDS Assurance Framework (RAF) v2.0

Background

Over the last two years, the REFEDS Assurance Framework (RAF) Working Group has updated the framework from RAF 1.0 to RAF 2.0. The reason for the change was two-fold: (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, moderate, 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.

Overview

Significant updates and rewrites occurred in the following areas:

1. The entirety of the document has been revised for clarity, to include expanding the definitions list.
2. Special attention was placed on a more in-depth articulation of Identity Assurance Profile (IAP) “local-enterprise”.
3. IAP profiles for low, medium, and high have been completely rewritten as self-contained in this document, rather than referring to disparate external sources. This includes a detailed table of criteria for each IAP level as normative text, and an informative “plain English” version in Appendix B.
4. A discussion on versioning; specifically, RAF 1.0 is not fully upwards compatible in all cases for the low/medium/high IAPs. The versioning particulars, including how to signal that RAF 2.0 criteria have been used, are detailed in the document. Furthermore, Appendix A includes an ‘upwards compatibility’ discussion detailing what CSPs must look at to determine if any adjustments need to be made to their identity proofing and credential issuing processes before claiming RAF 2.0.
5. An informative implementation discussion has been included in Appendix B.

In addition to reviewing the document, we invite reviewers to provide input on the following two questions:

1. The profiles espresso and cappuccino were maintained for legacy purposes, but the WG discussed they may be removed from future versions. The WG invites public feedback on the continued inclusion of these profiles.
2. Appendix A.2 refers to other compatible frameworks that, when implemented, meet or exceed certain RAF IAPs. The WG invites public feedback on other frameworks that might be listed on a future supplement (such as a wiki) as frameworks that achieve compatibility with RAF IAPs.
3. In regards to the versioning compatibility discussion and guidance in RAF 2.0, the WG invites reviewers thoughts on whether this approach (which allows RAF 1.0 and RAF 2.0 to exist simultaneously), or a more explicit depreciation of RAF 1.0, would be preferred.

A PDF for the consultation is available, RAF 2.0 Public Consultation.pdf

All comments should be made on consultations@lists.refeds.org or added to the comment log below, comments posted to other channels will not be included in the consultation review. Please consider adding an indication of your support if you have no changes to suggest.

Change Log

<table>
<thead>
<tr>
<th>comment #</th>
<th>Line / Reference #</th>
<th>Proposed Change or Query</th>
<th>Proposer / Affiliation</th>
<th>Action / Decision (please leave blank)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>150-151</td>
<td>The definition of CSP in this paragraph doesn't align well with that on page 4, and I think page 4 better represents what this document means by “CSP” (i.e., the organization's whole technical and organizational infrastructure for IAM). I suggest removing “...the central part of...” from that paragraph.</td>
<td>David Walker / Independent consultant</td>
<td>The Working Group (WG) agreed with this proposed change.</td>
</tr>
<tr>
<td>2</td>
<td>77-82</td>
<td>In the definition of &quot;low,&quot; the issue is not really on an identity is self-asserted, but rather whether it was validated and verified. I suggest rewriting the first sentence to &quot;The bearer of this claim is a Person with an identity that has not necessarily been validated and verified (i.e., a self-asserted identity).&quot;</td>
<td>David Walker / Independent consultant</td>
<td>The WG understand your perspective; however after discussion we agreed to keep the statements positive rather than mixing in negative ones, to keep the style consistent. We kept the original wording.</td>
</tr>
<tr>
<td>3</td>
<td>232</td>
<td>Thanks to the authors for your work to date. Overall, v2 is a big improvement and I think you've achieved the objectives outlined. This is both technical and abstract and I acknowledge that English is often not the author's native language. Great job! I'm going to add a lot of comments below but hopefully it will improve readability and clarity. Please don't take it as criticism.</td>
<td>John Scullen / Australian Access Federation</td>
<td>Thank you so much for the diligent feedback! The Working Group has discussed all the submitted comments, and will be posting responses to each in the upcoming days (this statement posted 29 Sep 2023). We spent time discussing each comment, and attempted to be as mindful as possible whether to accept the proposed change, keep the original wording, or if the proposed change pointed out an underlying point of confusion, we may have adjusted the text an a different way.</td>
</tr>
<tr>
<td>4</td>
<td>general</td>
<td>+1. I agree with david on both of these points.</td>
<td>John Scullen / Australian Access Federation</td>
<td>See responses to 2 and 3 above.</td>
</tr>
</tbody>
</table>
I'm not entirely happy with this redraft but suggest the following as an introductory paragraph:

"In identity federations, Relying Parties (RP) grant access to services after users successfully authenticate to their home organisation Identity Provider (IdP) using their institutional credentials. Identity Providers in turn rely on the home organisation’s Credential Service Providers (CSP) to issue and manage user credentials. Each RP has a different risk profile and different thresholds of confidence regarding assertions made by IdPs in order to address the RP’s operational risks. This REFEDS Assurance Framework specifies methods for expressing elements of identity assurance from the CSP for evaluation by the RP within research and education federations."

I think it’s better to talk about “levels of confidence” rather than “certainty”. Assurance is about collecting enough evidence to clarify some threshold related to the risks in that particular situation. It’s about having sufficient confidence rather than certainty.

John Scullen / Australian Access Federation

After discussing, the WG agreed that the word ‘confidence’ is better than ‘certainty’, and made commensurate changes.

The WG agreed and incorporated the proposed change.

The WG agreed and incorporated the proposed change.

The WG agreed and incorporated the proposed change.

The WG agreed and incorporated the proposed change.

The WG agreed and incorporated the proposed change.

The WG discussed this and felt the suggested revision too narrowly represents what is addressed in RAF 2.0 (it mentions only identity assurance). However, we agreed the existing wording might be confusing, and amended it to: “This document provides a framework by which a Credential Service Provider (CSP) asserts claims to an RP’s service about its confidence in the values of selected user attributes”

The WG discussed... while considering these revisions, we also had to look at how one revision might affect the flow with other proposed revisions. Given that for comment 12 we deleted ‘federation protocols’, the WG felt it was best to keep the original text here.

The WG agreed and incorporated the proposed change.

The WG agreed and incorporated the proposed change. WG also deleted the verbiage ‘a method to’ in lines 83, 85, and 90.

The WG agreed and incorporated the proposed change.

The WG agreed and incorporated the proposed change.

The WG agreed and incorporated the proposed change. The WG revised the text to: "Attribute Assurance communicates to the RP the quality and freshness of attributes (other than the unique identifier) passed in the login assertion."

The WG agreed in part with this. The WG revised the text to: "Attribute Assurance communicates to the RP the quality and freshness of attributes (other than the unique identifier) passed in the login assertion."

The WG discussed and ultimately voted to keep the original text. However, the WG did change the original wording of ‘certainty’ to ‘confidence’.

The WG discussed and ultimately voted to keep the original text. However, the WG did change the original wording of ‘certainty’ to ‘confidence’.

The WG agreed and incorporated the proposed change. After WG discussion, the WG decided to keep the original wording.

The WG agreed and incorporated the proposed change.
The WG discussed this for several sessions. We decided to keep the original text because it is an example in an informative piece of text. Making it more generic might have lost the purpose of providing an example, or lead to a desire to exhaust all possible examples (e.g., OCDS). The WG ultimately felt that wasn’t necessary here.

The WG discussed, but decided to keep the original text. The purpose or RAf 2.0 framework itself is larger than the purpose that drove to a revision.

The WG agreed and incorporated the proposed change.

The WG discussed this for several sessions. We decided to keep the original text because it is an example in an informative piece of text. Making it more generic might have lost the purpose of providing an example, or lead to a desire to exhaust all possible examples (e.g., OCDS). The WG ultimately felt that wasn’t necessary here.

The WG agreed, and added a "Registrar" definition, and changed 'executing' with 'carrying out'.

The WG discussed, but ultimately decided to keep the original wording.

The WG agreed and incorporated the proposed change.

The WG agreed and added a "Registrar" definition, and changed 'executing' with 'carrying out'.

The WG discussed and came to consensus that no change is needed. One point of discussion highlighted that the framework is not making claims about future behavior. [UN3] implies that ID unique declares that identifier will never be assigned to another Person - that’s more stringent than ceasing to assert ID/unique upon its reassignment. [UN3] need not imply that the identifier has always been assigned to the present Person.

The WG agreed and incorporated the proposed change.

The WG agreed and incorporated the proposed change. The purpose or RAF 2.0 framework itself is larger than the purpose that drove to a revision.

The WG agreed and incorporated the proposed change. The purpose or RAF 2.0 framework itself is larger than the purpose that drove to a revision.

The WG agreed and incorporated the proposed change. Good catch.

The WG discussed, and consensus agreed this is out of scope. There are better options, but addressing ePPN or documenting alternatives is out of scope of this framework.

The WG agreed and incorporated the proposed change.

The WG discussed, but ultimately decided to keep the original wording. The purpose or RAF 2.0 framework itself is larger than the purpose that drove to a revision.

The WG agreed and incorporated the proposed change. The purpose or RAF 2.0 framework itself is larger than the purpose that drove to a revision.

The WG agreed and incorporated the proposed change. The purpose or RAF 2.0 framework itself is larger than the purpose that drove to a revision.

The WG agreed and incorporated the proposed change. The purpose or RAF 2.0 framework itself is larger than the purpose that drove to a revision.
"trusted source is defined in VA4". I don't think it's defined very well though (see also comment 37). Trusted sources seem very open to interpretation. Maybe adding some example use cases of sources that may be trusted in different contexts might help. This could probably go in an appendix with reference from the main part of the document.

John Scullen / Australian Access Federation

WG decided not to change the wording. 'Trusted source' is intentionally open to adapt to a multiplicity of cultural and national contexts.

Why are the attribute values limited to faculty, student, and member?

Revise:

Faculty is rarely asserted in Australia but we almost always see staff and often employee too. Universities here understand who their staff are but have a harder time distinguishing between faculty vs general / professional roles.

I would like to see RAF broadened to include staff and employee. I acknowledge definitions vary between countries (highlighted in section 2.5.1 of the eduPerson spec but despacing staff and to a lesser extent, employee, substantially diminishes the value of RAF in the Australian context.

John Scullen / Australian Access Federation

There was some discussion on this, but ultimately the WG agreed with the proposal. WG added 'staff' and 'employee', and also noted the difference in the versioning text.

Add: For further information see the REFEDS Multi-Factor Authentication Profile and REFEDS Single Factor Authentication Profile. (and include links to the specs)

John Scullen / Australian Access Federation

WG agrees with the underlying point... added "for example, look at..." (we chose not to link in the original spec in case the frameworks change, or titles change).

Revise to: RAF 1.0 is not deprecated. However, some RPs may require assurance using RAF 2.0 criteria over RAF 1.0 criteria.

John Scullen / Australian Access Federation

WG agrees proposed change is clearer and made the change.

below following

John Scullen / Australian Access Federation

WG agrees to change and also capitalised 'Implications' in this section.

"find itself having" need

John Scullen / Australian Access Federation

The WG agreed and incorporated the proposed change.

Revise to:

Identity evidence is any artifact that a Claimant presents to prove their identity. This includes: documentation such as a government-issued physical or digital identification document or record, and the ability to be validated and verified through a national registrar, or similar means.

John Scullen / Australian Access Federation

WG discussed, but consensus was to keep the original text. This is informative text. The WG felt that the revision might be interpreted as both parts are required, and notes that this is an example list.

Should these definitions be moved to the Terms and Definitions table (118)? They are used throughout the document and might be better placed there since they are used more widely than in the context of Appendix B. For this reason I think section 2 is a better home for them.

John Scullen / Australian Access Federation

The WG agreed, and moved these definitions to the glossary, and changed this paragraph to just list the fundamental concepts.

Revise complete sentence to:

The identity evidence presented must be valid at the time of identity proofing (e.g., unexpired), and the evidence must be: (a) issued by a nationally recognized source; nationally recognized as being valid for identification purposes, or (c) or a documented attestation of knowledge of the Claimant's identity from an authority recognized by the CSP.

John Scullen / Australian Access Federation

The WG agreed this needs revision. The WG felt original is a clear either/or construct, while the proposed revision suggests that the first 2 requirements are compounded. But, revision is warranted. Revised to "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," and formatted this as a bulleted list for reading clarity.

delete "its"

John Scullen / Australian Access Federation

WG agreed with change.

replace:

IAP high imposes one additional requirement for authenticator binding and issuance beyond the requirements in IAP medium and IAP low.

John Scullen / Australian Access Federation

WG agreed change is needed; revised to "IAP high adds one requirement".

Revise:

"achieve that assurance of Personhood."

To: "confirm the Claimant is a Person."

John Scullen / Australian Access Federation

WG agrees and adopted. This is simpler language.

Revise:

"When the process is in-person, this is a trivial requirement in that the Personhood is checked by virtue of the Registrar interacting with the Claimant face to face."

To: "Face to face interaction with the Registrar automatically fulfils the requirements for in-person processes.

John Scullen / Australian Access Federation

WG agreed this needs revision. WG felt the proposed change didn't quite capture the essence of the original text's intent, but appreciated bringing attention to clunky text in need of wordsmithing. WG revised the document to read: "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."

Revise:

"When the process is remote and unsupervised, then the CSP will need to consider how that requirement is to be fulfilled."

To: "CSSP will need to determine how to fulfill the requirements when the process is remote and unsupervised."

John Scullen / Australian Access Federation

WG agrees with this change.

"check for Personhood" "confirm the Claimant is a Person"

John Scullen / Australian Access Federation

WG agrees (ref comment 52).

Same comments apply as for comment 35.

John Scullen / Australian Access Federation

As discussed in comment 35, the WG was intentionally broad in some language to allow for variations in how the international community and different nations' systems' implementations vary. WG appreciated bringing attention to this, and tried to revise for further clarity. WG retains VA4 to change verb 'document' to 'confirm' in the transactions case to: The Registrar confirms the presence of the claimed identity in transaction records of a recognized organisation providing financial, educational, or utility services. Also updated lines 573-575 to reflect this change in VA4.
56 580 "* *" at the end of the line
John Scullen / Australian Access Federation
WG decided not to make the change.

57 581 and 584 Number these paragraphs as 1. and 2.
John Scullen / Australian Access Federation
WG decided to reject numbering the primary paragraphs in this informative section.

58 585 and 588 Change (1) to (a) and (2) to (b) if you add numbers as recommended in comment 57. It would be a less dense paragraph if these were formatted as sub-points too.
John Scullen / Australian Access Federation
WG agreed, and made the existing numbered list into a readable bullet indented style.

59 588 Revise to: "proofing process, or; (2) use an automated..."
John Scullen / Australian Access Federation
WG agreed, and made the existing numbered list into a readable bullet indented style.

60 596-597 Revise from the comma to: "but instead articulates functional requirements in that are relevant across international contexts and as technologies evolve." John Scullen / Australian Access Federation
WG discussed, but consensus was to keep the original wording.

61 599-601 Revise to: "This section is intended to provide illustrative examples and discussion illustrating how to implement RAF. These examples and discussion points show how to interpret the normative criteria for implementation, but are not intended to be exhaustive."
John Scullen / Australian Access Federation
WG discussed, and preferred neither the original wording nor the change as proposed. This prompted discussion which led to a revision to enhance readability and clarify. Changed first sentence to: "This section is intended to provide illustrative examples and discussion of how to implement RAF.” Second sentence only changed 'exhaustive' to 'comprehensive'.

62 605 "a known and" "an" John Scullen / Australian Access Federation
WG agrees with and adopted this change.

63 606 "and" "if" John Scullen / Australian Access Federation
WG discussed, and felt that in terms of logical expression, ‘and’ is the correct operator to require both expressions to be true. WG decided to remain with original text.

64 607-608 Revise: "done by the Claimant demonstrating authentication with" To: "demonstrated through successful authentication by the Claimant using" John Scullen / Australian Access Federation
WG agrees with and adopted this change.

65 610-611 Revise: "When this approach is taken, criteria in the IE, VA, VF, and UR groups may be ignored."
John Scullen / Australian Access Federation
WG agrees with and adopted this change.

66 633-644 Revise to: "Registrars will need to consider typical service standards in their location (e.g. longer postal delivery times may be needed in some locations)."
John Scullen / Australian Access Federation
WG agrees with and adopted this change.

67 642 Delete: 'each of' John Scullen / Australian Access Federation
WG agrees with and adopted this change.

68 652 Add comma after "proofing process" John Scullen / Australian Access Federation
WG discussed, adding a comma shifts where the prepositional phrase is. However, discussion drove a revision of this part of the text. Splitting into two sentences as described below.
Line 647-657 replacement:
"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 3rd 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.

69 653 "each such service" "these services"
John Scullen / Australian Access Federation
Agreed and incorporated into edits from comment 68.

70 653-657 Revise: "These, together with 3rd parties identified in material on their Trust Status List antecede 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."
John Scullen / Australian Access Federation
Agreed and incorporated into edits from comment 68.

71 659-660 Revise first sentence to: "This framework does not explicitly require a government-issued photo ID." John Scullen / Australian Access Federation
WG agreed with proposed change, and changed follow on sentence from "The reason is simply" to "This is.”

72 660 "simply because” “that” John Scullen / Australian Access Federation
WG agreed; revision from comment 71 applies.

73 664-665 "do not implement things in the same way" "use different approaches and standards” John Scullen / Australian Access Federation
WG accepts the original language is awkward. Discussion led to the following revision: “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'.”
666-668
Revise second sentence to:
"The easiest way to meet IAP medium in-person requirements is to compare a photo on the identity evidence with the Person."

John Scullen / Australian Access Federation

WG accepts the original language is awkward. Discussion led to the following revision: 
"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."

669-671
Revise to:
"For nations that do not have robust national-level identity infrastructure, a government-issued photo ID may be the only evidence that enables the Registrar to meet all the validation and verification requirements."

John Scullen / Australian Access Federation

WG accepts the original language is awkward. Discussion led to the following revision: 
"For nations that do not have robust national-level identity infrastructure, a government-issued photo ID may be the only evidence that enables the Registrar to easily meet all the validation and verification requirements."

672-673
Revise to:
"Presented evidence" implies the Claimant must present the evidence themselves.

John Scullen / Australian Access Federation

WG discussed and consensus was the proposed change breaks the logical flow of the paragraph; decided to keep original wording.

674
"have implemented" -> "adopt"

John Scullen / Australian Access Federation

WG discussed and consensus was to delete the word 'implemented', given that if they have a solution, it implies they have already implemented or adopted it.

676
Revise heading to:
"Appendix C: Example assurance values"

John Scullen / Australian Access Federation

WG agreed and incorporated the change; also made the heading into Title Case.

690
In the "Reason" column it might be a good idea to cross referencing 5.2 to also include references to the GR, IE, VA, VF, AB and UR criteria where appropriate.

John Scullen / Australian Access Federation

WG discussed at length, but ultimately decided to reject the proposed change. Summary of discussion is: "adding the granular requirements makes this table too awkward, where the issue proposed is for just the identity proofing portion. Reference to 5.2 should direct reader to the 'car chart' for details (on identity proofing). Reference to 5.2 is a non-sequitur for all but three of the criteria, and implementing High (as in this example) essentially sources nearly every requirement in the 'car chart'."

19
"IAP" Spell out on first use then abbreviate.

Nick Rossow / Australian Access Federation

WG agrees with change.

244/GR1
GR1 requires that "The CSP takes measures to ensure that the Claimant accomplishing each step of the identity proofing and authentication/issuing process is the same Person throughout the process."

It is not clear how that can be fully achieved - there could be steps where another Person could act on behalf of the Claimant - if they shared credentials, this would be impossible to detect.

Vlad Menc / Tuukka / README

WG discussed and decided to keep the original text. WG agreed this is a potential concern (especially if users are sharing credentials), but this is out of scope of this framework. This is also why we emphasise that if an RP requires IAP High, they should also be requiring complementary assurances such as MFA (non-shareable credentials), as indicated in lines 102-107.

244/UR1
It is not clear what it means for contact information to "belong to the Claimant". Would it be stronger then being "in control of" the contact channel? Such as for a phone number, not only to be able to receive messages, but also be listed in a public phone directory as the owner? Or for email, having it listed in institutional directory as belonging to the user? Perhaps this should be made clearer.

Vlad Menc / Tuukka / README

Thanks for bringing this to attention. The WG discussed in depth, and ultimately decided not to make a change. In developing RAP 2.0, the WG decided to avoid completely define 'trusted source'; it is intentionally left to adapt to a multiplicity of cultural and national contexts (see comment #40). It is left to the CSP to include what is the trusted source in its process documentation. The trusted source as described in VA4 checks against ownership, not control (given that a phone, for example, could be stolen and not owned). "Belonging to" (verified ownership) is stronger than being "in control of". WG agrees that a public phone directory or institutional directory for email can be a trusted source to verify 'ownership' of the contact information.

244/UR3 + 394-397
I'm not sure if eIDAS is really built around an 'in-person' principle. If a claimant is identified by an (IoGov-approved) eID-Sever using an eID Token which is notified as eIDAS LoA High, why would a CSP ever require an additional in-person check? Such a requirement would run completely counter to the basic idea of eIDAS (IMO, of course). I doubt that any German university would ever be able to assert IAP high...

Wolfgang Pempke / DFN-AAI

Thank you for pointing this out. WG discussed this at length. eIDAS is silent on additional requirements for Unsupervised Remote proofing, so we inferred an in-person requirement. Furthermore, in RAP 1.0, the WG had considered the possibility that an institution might use eIDAS standards to do their own ID proofing rather than leverage the eIDAS national infrastructure itself. We agreed this needs revision because the original text communicates an incorrect assumption. WG revised to a version of the following idea (subject to final edits prior to release): "eIDAS is silent on additional requirements for Unsupervised Remote processes, specifically (UR3). Therefore, if the CSP has used the specific eIDAS paragraphs referenced by RAP 1.0 to make RAP 1.0 IAP claims, and is using 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. "WG removed the text claiming that "eIDAS was built around an in-person principle"

244/GR3
Are there any means by which the records can be requested in case of an incident?

Anders Sjöström / NoC / PuHuuri

WG discussed and confirmed that this security incident response is out of scope of this framework. There is another framework addressing security incident response and cooperation in federations; REFEDS Sirtfi (https://refeds.org/sirtfi). How records are requested and with whom they are shared will likely be governed by internal policies in addition to national requirement for privacy protect. Those things are important, but not in scope of RAP.