REFEDS ASSURANCE FRAMEWORK (RAF) 2.0

Current status...

Pål Axelsson

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.

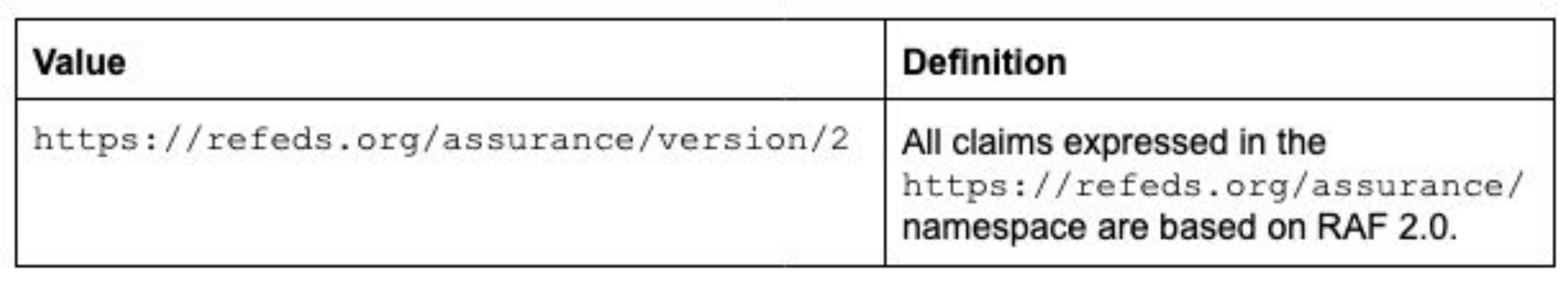
RAF’s relationship to other REFEDS assurance profiles

- 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*

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:
  - *tighten definitions of many claims based on field experience with RAF 1.0*
  - *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
  - *84 comments*
  - *no substantive disagreements with the proposed updated framework; most comments were for clarity and of editorial nature*
- 2023 Aug-Oct: Incorporate public consultation inputs, make ready for REFEDS Steering Committee
- 2023 October: WG comments on consultation is published on https://wiki.refeds.org/x/AQDOCw
- 2023 October: RAF 2.0 ready for REFEDS SC decision and later publication

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)
- Apendix B is a guide on how to interpret the IAP low, medium and high claims

Tips and Pointers for CSPs

- A CSP don’t have to assign the same IAP levels or other claims to all users
- Assess current processes and determine what claims can be made without having to change … 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

CSP stands for Credential Service Provider, i.e. the IAM system behind the IdP