Introducing the REFEDS MFA Profile

- What is the REFEDS MFA Profile?
- Where can I find the definition of the REFEDS MFA Profile?
- What does the Profile Guarantee?
- What are the Profile’s requirements for multi-factor authentication?
- How does the MFA Profile relate to Identity Assurance Profiles such as the REFEDS Assurance Framework?
- What does "at least two of the four types" mean?
- What are the "independent" factors mentioned in the Profile?
- What constitutes an acceptable "second" factor?
- Does my IdP need to be able to perform MFA to support the REFEDS MFA Profile?
- Can you share examples where organizations require REFEDS MFA Profile?
- How do I use the Profile in SAML?
- Is this Profile SAML-specific?
- What’s the difference between the REFEDS MFA Profile <AuthnContextClassRef> value and the others I see in vendor docs or product configuration?
- Do You Provide Explicit Guidance on What Is or Isn't a Sufficient Approach to MFA?

What is the REFEDS MFA Profile?

The REFEDS Multi-Factor Authentication (MFA) Profile defines a standard signal a service provider may send to request an IdP to perform MFA during federated authentication. The IdP sends the corresponding signal in its response to indicate that MFA had occurred. The Profile also defines the criteria an IdP must meet in order to claim successful MFA using the Refeds MFA Profile.

The REFEDS MFA Profile is primarily used within SAML authentication. Its use is largely patterned from the OASIS Authentication Context for SAML.

Where can I find the definition of the REFEDS MFA Profile?

The Refeds MFA Profile specification is available at https://refeds.org/profile/mfa.

What does the Profile Guarantee?

When signaling MFA using the REFEDS MFA Profile, you (the IdP) are guaranteeing that the specific user in question has successfully authenticated with MFA in a way that meets the requirements of the Criteria defined in the Profile.

MFA provides additional safeguards for both IdPs and SPs. However, it is not the solution to mitigate all security threats. Deployers should take care to examine and address other security threat vectors when selecting appropriate approaches and technologies.

What are the Profile’s requirements for multi-factor authentication?

To claim MFA using the REFEDS MFA Profile, an Identity Provider must be using an authentication method that meets the following requirements:

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

How does the MFA Profile relate to Identity Assurance Profiles such as the REFEDS Assurance Framework?

Identity and authentication assurance are very different things. This profile is about authentication assurance (how much to trust an assertion of authentication); it is not about how much to trust the identity information being asserted. These are (or should be) entirely orthogonal concerns. Some older "approaches" to this problem tended to conflate the two, but this is less common today.

The REFEDS Assurance Framework does not reference this profile but is intended to work in parallel with it.
What does "at least two of the four types" mean?

Authentication factors are commonly grouped into 4 types: something I know (knowledge factor), something I have (possession factor), something I am (inherence factor), and something I do (behavior factor). The REFEDS MFA Profile requires the IdP to use at least 2 authentication factors during MFA. Each factor used must be of a different type from the others. This means that validating two separate passwords (something I know) is not sufficient - the second (and further) factors must use a different factor approach.

What are the "independent" factors mentioned in the Profile?

When deciding MFA factors, introducing a second authentication factor that is directly accessible using the first factor negates the security offered by using a second factor; therefore it is NOT considered a second factor. For example, a software/virtual phone that is authenticated using the enterprise password is not an appropriate second factor in a MFA transaction when the enterprise password is the first factor.

Additionally, a users may take actions that reduce the ability to treat otherwise independent factors as "independent"; for example, a user storing their software OTP generator on a network device accessible using just the "first factor" password.

To meet Refeds MFA Profile requirements, an IdP operator must take measure to ensure that its supported authentication factors must be separate from each other. The MFA profile does not enumerate specific requirements an institution must meet to maintain independence between authentication factors. Although technical controls (where feasible) and user education are highly recommended to mitigate the risks of users deploying factors in a manner that decreases their independence.

What constitutes an acceptable "second" factor?

The REFEDS MFA Profile makes no statement about the types of technologies that could be used as the second or multi factor. The InCommon MFA Interoperability Profile Working Group has prepared some useful advice on approaches that might be useful.

Does my IdP need to be able to perform MFA to support the REFEDS MFA Profile?

In a meaningful sense, yes, but in the event that you do not support MFA at all, there may be steps you can take to ensure more useful error signaling behavior by your IdP to better support services across research and education. See Guidance for Identity Provider Operators for tips and how-to's.

Can you share examples where organizations require REFEDS MFA Profile?

The United States National Institute of Health (NIH) announced in 2021 that it will require MFA for access to some of its resources. As part of the rollout, it is requiring federated IdPs to support Refeds MFA Profile, along with other REFEDS standards. NIH's Electronic Research Administration Portal (eRA) already requires MFA for all federated access. Most universities in the US, as well as many around the world, collaborate with NIH and/or receive grants from NIH.

The InCommon Federation maintains a Get NIH Ready wiki to help keep the community up to date and to assist with implementations.

How do I use the Profile in SAML?

The SP invokes the profile by setting a pre-defined SAML element in the request to "https://refeds.org/profile/mfa". If it is able, the IdP, on receiving this value, authenticates the user in a manner consistent with the profile. If authentication is successful, the IdP indicates REFEDS MFA was performed by setting a related value in the response to "https://refeds.org/profile/mfa". If authentication is unsuccessful, or the IdP is unable to perform MFA, it initiates an error flow.

Details

The appropriate means of representing this profile in a SAML assertion is via the <AuthContextClassRef> element. These are expressed in SAML authentication statements used to represent acts of authentication by the subject of an assertion.

The use of the Authentication Context mechanism has the benefit of enabling signaling of requirements by an SP in its requests to an IdP via the <RequestedAuthnContext> request element. The standard defines the rules for this in https://www.oasis-open.org/committees/download.php/56777/sstc-saml-core-errata-2.0-wd-07-diff.pdf in Section 3.3.2.2.1. on page 46. (Note that this revision of the standards document includes material adjusted by Approved Errata, though the clarifications in this area are minimal.)
While this mechanism has a number of advanced features, the simple form and the one that interoperates with most open source SAML IdPs and SPs is the use of the default ("exact") Comparison operator and the inclusion of one or more `<AuthContextClassRef>` elements. An IdP that receives a request containing such an element is obligated to authenticate the user in a manner that allows it to return one of the requested `<AuthContextClassRef>` values in its assertion, or fail the request.

Returning a SAML error is required in the event of a failure, though there may be some cases in which an IdP cannot guarantee such a response to the SP and may leave the user stranded on the IdP. Any other behavior by an IdP is non-compliant with the standard; in particular, it MUST NOT issue a successful response with an assertion containing a non-matching context class value.

IdP software by default would not be expected to recognize the REFEDS profile context class, and so requesting it would be expected to result in an error; this is normal. Configuration examples for several identity provider technologies are available to demonstrate how to incorporate this context class into an IdP.

**Is this Profile SAML-specific?**

The Profile is not intended to be SAML-specific and can be extended for use with other technologies, such as OIDC. This will be reviewed subject to demand in those areas and examples provided when appropriate and mature.

**What’s the difference between the REFEDS MFA Profile `<AuthnContextClassRef>` value and the others I see in vendor docs or product configuration?**

A context class “reference” is an URI that means whatever the “owner” of the URI says it means. The field was meant to be extensible by design and there was never any presumption that the only possible values would be the ones mentioned in the original SAML standard. REFEDS chose the URI https://refeds.org/profile/mfa for its clarity. The fact that the value matches the Profile’s web URL also makes the Profile easy to find.

**Details**

Originally, the creators of SAML specification thought that expressing very technically-specific information was a logical thing to do, and that it would be a common way of signaling and requesting different types of authentication. The values defined in the standard were meant to “seed” the landscape with some basic values that were thought to be useful.

This idea turned out to be fairly bad in a couple of ways.

In one respect, implementers ignored the “extensible” angle and just baked in explicit and limiting support for only the values defined originally, which was never the intent.

Further, it proved to be a bad idea to base values on specific technologies because this ties deployments to “point in time” assumptions about how things work, without allowing systems to evolve in sensible ways. This problem is particularly acute with MFA because of the vast range of technologies involved, and the rapid pace of evolution in how MFA has been deployed.

As an example, if the value in the original standard that most closely resembles RSA SecurID tokens were used, a lot of systems would be built around the idea that the TimeSyncToken URN means “MFA”.

But many new MFA technologies are a completely different kind of authentication that doesn’t comport with the meaning of TimeSyncToken at all, yet may be just as acceptable.

The point of the REFEDS MFA Profile is to abstract away the details around a value with a meaning agreed to by a relevant community of practice. This is entirely in keeping with the intent of the mechanism in SAML, but not with the original way the mechanism was expected to be used.

**Do You Provide Explicit Guidance on What Is or Isn't a Sufficient Approach to MFA?**

REFEDS is developing a Profile to flag approaches that do not provide multifactor. The scope of this is still to be decided, but this FAQ will be updated as appropriate.