Introducing the REFEDS MFA Profile

What is the REFEDS MFA Profile?

The REFEDS Multi-Factor Authentication (MFA) Profile defines a standard signal to request MFA and to respond to such a request in a federated authentication transaction.

The REFEDS MFA Profile also outlines requirements that an authentication event must meet in order to communicate the usage of MFA.

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 signalling MFA using the REFEDS MFA Profile, you (the IdP/OP) are guaranteeing that the specific user in question has successfully authenticated with MFA in a way that meets the requirements 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.

Does the REFEDS MFA Profile v1.2 replace the original REFEDS MFA Profile v1.0?

Yes, the REFEDS MFA Profile v1.2 replaces the original REFEDS MFA Profile. V1.2 adds additional clarity.

What is the difference between the v1.0 and v1.2 version?

In addition to adding clarity, the 1.2 version of the Profile offers two messaging protocol bindings: for SAML 2.0 and for OpenID Connect. It also includes guidance on how to communicate the time of authentication and interpret forced re-authentication requirements when using multiple factors, with notable caveats due to implementation constraints.

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

REFEDS MFA Profile v1.2 defines MFA requirements inline in Section 4 of the Profile.

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

See “Relationship to other assurance-related issues” in Section 1 of the Profile.

What constitutes an acceptable "second" factor/is XXX acceptable as a second factor?

The REFEDS MFA Profile does not specifically define what technical methods are acceptable as individual factors. Per Sections 4.1 and 4.2 of the profile, factors must be of different types and independent from each other.

Explore the MFA Profile FAQ

MFA Profile FAQ Home

Introducing the REFEDS MFA Profile

Guidance for Identity Provider /OpenID Provider Operators

Guidance for Service Provider /Relaying Party Operators

Dealing with Institution MFA Policies

Identity Provider/OpenID Provider product specific questions

Service Provider/Relying Party product specific questions

Additional Links

REFEDS MFA Profile

InCommon MFA Interoperability Profile
Working Group Analysis: MFA Technologies, Threats, and Usage

The InCommon MFA Interoperability Profile Working Group published some useful advice during their work on the initial InCommon MFA Profile 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 signalling behaviour by your IdP to better support services across research and education. See **Guidance for Identity Provider Operators** in this FAQ 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.

The Swedish National Administration and Information System for coordinators (Nais), https://www.nais.uhr.se/personal, requires REFEDS MFA for authenticating staff users.

The Student Information System of higher education institutions in Sweden (Ladok), https://www.start.ladok.se/, is configurable, and configured for some higher education institutions, to require REFEDS MFA step-up for some certification-related parts of the application.

The national AARC-BPA-based 'AAI as a Service' at SURF (SRAM), https://sram.surf.nl/, requires MFA for access. REFEDS MFA signalling from the IdP may be used to avoid the requirement of configuring a local TOTP in SRAM for the user.

How do I use the Profile in SAML?

See Section 5 of the profile.

Is this Profile SAML-specific?

No, the Profile is messaging protocol agnostic. V1.2 introduces bindings for both SAML and ODIC.

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

A SAML context class "reference" is a 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 the SAML specification thought that expressing very technically-specific information was a logical thing to do and that it would be a common way of signalling 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.

OIDC

While there is less practical experience with this protocol, it is likely that many of the same considerations noted above with regard to SAML's `<AuthnContext>` feature apply to OIDC's `acr` claim and related features.