Guidance for Identity Provider/OpenID Provider Operators

- My IdP performs MFA for all requests. Should I signal REFEDS MFA use even when the SP does not explicitly request MFA using the Profile?
- An SP is requesting MFA for a user. My IdP supports MFA, but the user in question has not activated or enrolled in my MFA solution. How should the IdP behave?
- An SP has requested MFA for a user. That user already has a valid IdP session, but is authenticated without MFA. What should my IdP do?
- When an SP requests MFA using the REFEDS MFA Profile, and the user already has a valid SSO session with the IdP that has been authenticated via MFA, what should the IdP do?
- My MFA implementation has a “Remember Me” feature to allow less frequent challenges. How should my IdP respond to an MFA request if a user logs in with the first factor and a “remembered” second factor?
- How should my IdP respond to an MFA request when my IdP is unable to perform MFA because the service (e.g., Duo or another third-party solution) is unavailable?

My IdP performs MFA for all requests. Should I signal REFEDS MFA use even when the SP does not explicitly request MFA using the Profile?

Presuming that you meet the requirements of the profile, you can only signal REFEDS MFA if the SP does not request any other AuthnContext class reference or requested acr claim in its request. If the SP requests one or more specific values, you cannot respond with the REFEDS MFA signal unless the SP includes it among them.

That does not imply that performing MFA itself is disallowed; this would depend on the meaning of the other values requested and whether performing MFA would allow the IdP to assert one of the requested values.

The golden rule: you must assert something that matches the request and you must assert only what is true. If the request specifies nothing, you are left with the option to assert anything that is true, including REFEDS MFA.

An SP is requesting MFA for a user. My IdP supports MFA, but the user in question has not activated or enrolled in my MFA solution. How should the IdP behave?

A key goal of federated access is to facilitate trustworthy and streamlined access to collaboration resources. Your IdP might inform the user that the resource they are attempting to access requires MFA, and they should enrol in MFA before continuing. You could then optionally trigger MFA enrollment if you have a self-service online MFA enrollment mechanism.

However, none of this is strictly mandated; all that you MUST do is either leave the user somewhere sensible or return them to the SP with an error response.

An SP has requested MFA for a user. That user already has a valid IdP session, but is authenticated without MFA. What should my IdP do?

The sum total of the user challenges associated with their SSO "session" must comply with the Profile. It is the IdP’s choice whether every factor must be performed at once (possibly repeating earlier challenges), or whether only the “missing” steps needed to satisfy the Profile are performed. The latter is an example of so-called “step-up authentication” and many IdPs may do this automatically when configured correctly.

Note, per Section 4.3 in the profile, if the “step-up authentication” approach is used, it is recommended that the AuthnInstant or auth_time communicated for the SSO session be that of the oldest challenge the user has completed.

When an SP requests MFA using the REFEDS MFA Profile, and the user already has a valid SSO session with the IdP that has been authenticated via MFA, what should the IdP do?

If the user’s current SSO session meets the requirements of the MFA REFEDS Profile, your IdP can reply to the SP with a successful response without triggering any challenges, unless the ForceAuthn or prompt/max-age features are enabled and included in the request. If ForceAuthn or prompt/max-age is included in the request, an existing SSO session should not be used, at least in total, and the user should be challenged in some form. It is not precisely defined which individual factor(s) must be performed, though it is fairly common (and most understandable) for all of them to be freshly performed. See sections 5.1.2.2 (SAML) and 5.2.2.2 (OIDC) in the profile for more on this.
How recently must MFA have been performed in order to comply with the REFEDS MFA Profile?

See Section 4.3 of the Profile.

The Profile does not mandate any specific limit on the actual lifespan during which previous challenges may be reused, and the only mitigation for this is the use of the AuthnInstant attribute or auth_time claim by the SP to enforce its own view of how long is “too long”. This is why it is suggested and hoped that IdPs will populate this value as conservatively as possible by setting it to the oldest appropriate value and not the newest, but this is not a requirement of either SAML or OIDC, so it is a recommendation only.

My MFA implementation has a “Remember Me” feature to allow less frequent challenges. How should my IdP respond to an MFA request if a user logs in with the first factor and a “remembered” second factor?

While the Profile explicitly does allow for such features to be used and does not stipulate limits on the period of time involved, it does stipulate that such features should never, when used alone, cause the authentication timestamp communicated to the SP to be updated. In practice, this implementation constraint may be difficult to meet and it is therefore a recommendation and not a mandatory requirement.

While some argue for strict constraints on the feature, note that SSO itself is ultimately a form of “Remember Me” functionality anyway, so constraining it further overlaps quite strongly with the use of the ForceAuthn, and related, features. Generally, SPs that require truly fresh authentication challenges are advised to use that option, but should also understand that many IdPs may not support it well, so interoperability may be impacted.

How should my IdP respond to an MFA request when my IdP is unable to perform MFA because the service (e.g., Duo or another third-party solution) is unavailable?

See Section 4 of the Profile. Failing “open” is not allowable.