Guidance for Identity Provider Operators

- What do I (the IdP) need to guarantee in order to assert use of the Profile?
- What does a "successful" response to a request for REFEDS MFA look like?
- My IdP does not support/perform MFA. How should my IdP respond when a SP requests MFA using the Profile?
- 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 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?
- How recently must MFA have been performed in order to comply with the REFEDS MFA Profile?
- 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?

What do I (the IdP) need to guarantee in order to assert use of the Profile?

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 section defined in the Profile. The use of MFA has to have occurred either directly in the fulfillment of the request from the SP in question, or as part of the overall SSO "session" maintained with the browser.

In the event that you cannot perform MFA for the user in question, take care to ensure your IdP handles errors gracefully so that external services can help guide the user to the appropriate help they may need. Questions and answers in this section contains useful tips and how-to's.

What does a "successful" response to a request for REFEDS MFA look like?

In the event that an IdP supports the profile and can fulfill a request for it, the assertion that is returned would contain the appropriate <AuthnContextClassRef> like so:

Example: Successful MFA

```xml
<samlp:Response xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
    xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">
    ...
    <samlp:Status>
    </samlp:Status>
    ...
    <saml:AuthnStatement AuthnInstant="..."
        SessionNotOnOrAfter="..."
        SessionIndex="...">
        <saml:AuthnContext>
            <saml:AuthnContextClassRef>https://refeds.org/profile/mfa</saml:AuthnContextClassRef>
        </saml:AuthnContext>
    </saml:AuthnStatement>
    ...
</samlp:Response>
```

Every SSO assertion in SAML has this kind of content; the contents of the <AuthnContext> element may vary but in the vast majority of IdPs, it will be this kind of element and only the URI in the element will vary.
My IdP does not support/perform MFA. How should my IdP respond when a SP requests MFA using the Profile?

Per the SAML 2.0 Core Specification, Section 3.3.2.2.1:

If none of the specified classes or declarations can be satisfied in accordance with the rules below, then the responder MUST return a <Response> message with a top-level <StatusCode> of urn:oasis:names:tc:SAML:2.0:status:Responder and MAY return a second-level <StatusCode> of urn:oasis:names:tc:SAML:2.0:status:NoAuthnContext.

(Note that the above document is modified by Errata approved after the original standard's approval, but the changes are largely cosmetic.)

In XML, this looks like:

```
Example: Unsuccessful MFA

<samlp:Response xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
    xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
    ...
    ...
    <samlp:Status>
        <samlp:StatusCode Value="urn:oasis:names:tc:SAML:2.0:protocol:Responder">
        </samlp:StatusCode>
    </samlp:Status>
</samlp:Response>
```

In plain English, the IdP is expected to respond to the SP and needs to return an error when it does so. There are definitely scenarios in which IdPs tend to leave the user facing challenge screens or the like because they don't offer some kind of "cancel" function or any way to continue so the IdP can respond, and this is not viewed as "wrong", merely less ideal for the SP. The important thing is that the IdP MUST NOT return any kind of successful response to the SP, as this is a violation of the standard.

It is also important that the IdP does not fail in a graceless manner (e.g., crashing with a stack trace) because that leaves the user with no recourse.

It might be more useful to the user to give instructions on what the user has to do to be able to perform MFA, such as performing some kind of initial enrollment process, though obviously if the IdP simply has no support for MFA of any kind, then this isn't possible.

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?

You may, or may not, subject to the golden rule: you must assert something that matches the request and you must assert only what it true. If the request specifies nothing, you are left with the option to assert anything that is true.

But, if the request specifies something else specific, then whether you can respond with a matching class would depend on whether the requested class was a fit for what the IdP can do in order to maintain the constraint that only what is true is acceptable. This is because of the standard's language noted above: if an SP requests an authentication context class other than REFEDS MFA, your IdP MUST respond with that context or with an error (allowing that being unable to respond at all is a possible situation). Any other behavior is simply not allowed under the standard and your IdP is broken if it does so.

For example, if part of your authentication workflow fulfills the rudimentary "PasswordProtectedTransport" context class and an SP were to request that context class, then a successful response MUST include the PasswordProtectedTransport context class, even if the user actually was forced to do more than just that process. In contrast, for example, a fingerprint check together with a hardware token does not fulfill the intent behind PasswordProtectedTransport, and asserting it would not be appropriate in response to such a request. (This edge case illustrates why SPs should rarely, if ever, request "low-value" kinds of authentication, because they may well preclude much better options from use.)
Note that in SAML, an SP may simultaneously request multiple authentication contexts. However, the IdP can only respond with one. If an SP requests multiple authentication contexts, the IdP may respond with any of the requested contexts at its discretion, as long as that one is accurate.

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 enroll 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 authenticated without MFA. What should my IdP do?

The sum total of the user's challenges across this request and any previous requests 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.

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?

Your IdP may honor the normal single sign-on behavior and reply to the SP with a successful response without triggering any new authentication, unless the ForceAuthn attribute (set to "true") was included in the request. If so, single sign-on may not be used, at least in total, and the user must be challenged in some form. It is not precisely defined which individual factor(s) must be performed, though it is fairly common for all of them to be freshly performed.

How recently must MFA have been performed in order to comply with the REFEDS MFA Profile?

The user should have authenticated within their current or in a new SSO session with the IdP using a combination of at least two distinct types of authentication factors. In other words, the user should have been challenged to complete each factor within the current IdP session's span.

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 does not address this question in detail, it is the sense of most (though not all) deployers that an MFA implementation's "Remember Me" duration should ideally be shorter or equal to the IdP's overall session length (typically 8 to 24 hours) to avoid a scenario in which a user may instantiate a new IdP session where MFA is required without actually completing the MFA challenge.

While some actually argue for even stricter 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 feature. 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?

When receiving a REFEDS MFA request, if your IdP cannot not perform MFA for a user for any reason, it must respond in accordance with the SAML requested authentication context processing rule. This behavior is sometimes described as “failing closed” rather than “failing open”. An inability to perform MFA (whatever the reason) must always be indicated to the SP using a SAML error response or without responding at all.
Because the REFEDS MFA Profile is used in signaling MFA across organizational boundaries, a local policy exempting a user from completing MFA in order to maintain business continuity does not apply when evaluating MFA compliance in a federated context.

This is however only applicable if the SP specifically requests REFEDS MFA Profile use, though many IdPs may not have an easy time making such a distinction. It would however be completely acceptable (if the IdP operator deems it so) to fail open in response to a request that does not stipulate the use of the Profile.