Obsolete MFA Profile FAQ

A new FAQ is now available.

This version of Refeds MFA Profile FAQ has been replaced with a new version. Visit the new REFEDS MFA Profile FAQ.

The following FAQ support the use of the REFEDS Multifactor Authentication Profile. This documentation is intended to be non-normative supporting information. If you have any questions about the use of the REFEDS MFA Profile, please direct them to the REFEDS mailing list (refeds@lists.refeds.org).

- What are the requirements for multifactor authentication in the profile?
- What does the Profile Guarantee?
- What constitutes an acceptable "second" factor?
- Why two of the four types?
- What do you mean by "independent" factors?
- How Does the MFA Profile relate to (level) of assurance profiles?
- Is this Profile SAML specific?
- How do I implement this in SAML?
- What Does the (SAML) SP need to do?
- How Do I Create SAML Requests?
- What are the Use Cases for Including the <RequestedAuthnContext> Element?
    - SP always requires MFA
    - SP prefers, but does not require, MFA
    - SP Requires “Step Up” MFA
- Why Reference ITU-T X.1254?
- Do You Provide Profiles for the Authentication Approaches?

What are the requirements for multifactor authentication in the profile?

In order to assert the REFEDS MFA profile, the 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.

What does the Profile Guarantee?

The Profile signals that the specific user in question is using multifactor authentication in a way that meetings the requirements shown above. Mutlifactor provides additional safeguards for both IdPs and SPs but is not completely resistant to all possible threats - this should be kept in mind when selecting appropriate approaches and technologies.

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.

Why two of the four types?

Each factor in the MFA profile must be of a different type. This means that validating two separate passwords is not sufficient - the second (and further) factors must use a different factor approach. This is to address any generic point of failure with one factor type.

What do you mean by "independent" factors?

- Implementors must work to ensure that the different factors used in the authentication process are independent, meaning that gaining access to one factor must not trivially grant access to the other factor.
- Any factor that is directly accessible using the first factor is no more secure than the single factor by itself, and so is NOT considered a second factor.
- Institutions are expected to provide safeguards to maintain the independence of their supported authentication factor.
    - a software/virtual phone that is authenticated using the enterprise password is not an appropriate second factor.
- The MFA profile does not enumerate specific requirements the institution must meet to protect against these forms of authentication dependence, but technical restrictions (where feasible) and user education are highly recommended to mitigate the risks of users deploying factors in a manner that decreases their independence.
- Processes that allow a user to immediately register a new second factor (re--registration) using only their “first factor” enterprise password are no more secure than use of the enterprise password itself.
- Implementors are expected to require greater scrutiny before allowing registration of replacement or additional second factors to prevent attackers with password access from simply registering and immediately using a new second factor. Additional second factors can use a existing second factor when registered or the same method as the first second factor.

How Does the MFA Profile relate to (level) of assurance profiles?

Many assurance profiles will include approaches to MFA within them. REFEDS Assurance Framework does not reference the REFEDS MFA Profile but is intended to work in parallel with this profile.

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.

How do I implement this in SAML?

The recommended means of representing these profiles in a SAML assertion are via the <AuthContextClassRef> element (SAML 2.0). These are expressed in SAML statements used to represent acts of authentication by the subject of an assertion. In the case of SAML 2.0, the use of the Authentication Context mechanism has the benefit of enabling signaling of requirements by a relying party in its requests to an identity provider.

Configuration examples for several identity provider technologies are available.

What Does the (SAML) SP need to do?

Most IdPs and campuses that support MFA services do not provide universal MFA coverage for their user communities. This means that even when a given IdP is capable of supporting this profile, there is a significant probability that any given user may not be able to authenticate using MFA. There is no defined mechanism at present to identify whether a given IdP is configured to assert <AuthnContextClassRef> values, and SAML itself does not rely on that knowledge; it assumes that IdPs will respond in accordance with the standard when handling a request containing requirements it cannot meet.. If the SP does not have any information about an IdP’s capabilities, it may not be able to distinguish between a case of specific users being unable to satisfy the profile, and an IdP as a whole not supporting it. Whether this distinction is relevant will depend on the SP. <AuthnContextClassRef> value is returned in SAML responses; it is not sufficient to configure an SP to request MFA and assume all responses will therefore contain the MFA context. This is because users can generally bypass an SP’s SAML request configuration using unsolicited responses from an IdP, or by handcrafting a SAML request that does not include the MFA requirement.

If an application intends to provide limited services to non MFA authenticated users, the actual <AuthnContextClassRef> value returned to the SP will need to be evaluated dynamically by the application to determine the appropriate access to provide to the user.

How Do I Create SAML Requests?

From a technical standpoint, when generating a SAML authentication request where the MFA profile is desired, the approach is fairly straightforward:

1. Explicitly list every AuthnContextClassRef value that your SP is willing to accept in the <RequestedAuthnContext> element in your SAML request. The actual values you list will depend on your use case (see “Use Cases” below for some general guidance).
2. No matter how carefully you specify context class values, some IdPs may be unable to respond due to software or process limitations. (This issue is not specific to the MFA profile but affects any requests that includes explicit <RequestedAuthnContext> elements). If you want to support IdPs that are not able to support the values you list, then on receiving a SAML error you can try reissuing your SAML request with <RequestedAuthnContext> element.

What are the Use Cases for Including the <RequestedAuthnContext> Element?

SP always requires MFA

This use case is most relevant if the SP operator knows that the IdP in question supports this profile. To require that all users must authenticate using MFA, a SAML authentication request
should include:

```
<samlp:RequestedAuthnContext Comparison="exact">
<saml:AuthnContextClassRef>
https://refeds.org/profile/mfa
</saml:AuthnContextClassRef>
</samlp:RequestedAuthnContext>
```

That is, MFA is the (only) requested value.

Even if an IdP supports the MFA Profile, it can only respond successfully to such a request if MFA is actually performed. If the user can authenticate to the IdP, but is not able to use MFA, the IdP must respond with an error, and the SP will not receive any information about the user who tried to authenticate. If this distinction is important, and it's important to know the identity of the user even if MFA is not possible, consider one of the later uses case of preferring MFA, but accepting less. Application error messages when using this model should explicitly note that MFA is required to access the SP's services.

SP prefers, but does not require, MFA

In some cases, an SP may prefer that users authenticate with MFA but is willing to accept non-MFA authentication. Some scenarios where this approach would make sense:

- Applications that can implement a local scheme to do "stronger authentication" of specific users but prefer to allow users to use familiar campus mechanisms when available.
- Applications that will allow access to some services to all users, but have other services that are limited to those that authenticate using MFA.
- Applications that wish to offer their own opt-in feature for users to elect to use MFA for that service.
- An application that only allows access to users who authenticate with MFA, but wants to personalize error messages to users who do not use MFA as part of the authentication process.

In this scenario it is recommended that the SP request not just the REFEDS MFA Profile, but also any other standard or common <AuthnContextClassRef> values that are acceptable and frequently encountered. A
recommended request that should cover most of these use cases would include:

<samlp:RequestedAuthnContext Comparison="exact">
<saml:AuthnContextClassRef>
https://refeds.org/profile/mfa
</saml:AuthnContextClassRef>
<saml:AuthnContextClassRef>
urn:oasis:names:tc:SAML:2.0:ac:classes:X509
</saml:AuthnContextClassRef>
<saml:AuthnContextClassRef>
urn:oasis:names:tc:SAML:2.0:ac:classes:Kerberos
</saml:AuthnContextClassRef>
<saml:AuthnContextClassRef>
urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport
</saml:AuthnContextClassRef>
<saml:AuthnContextClassRef>
urn:oasis:names:tc:SAML:2.0:ac:classes:Password
</saml:AuthnContextClassRef>

The actual list of AuthnContextClassRef values to support is up to the SP, but this list is likely to address the majority of IdPs. To support arbitrary IdPs, it may still be necessary to respond to SAML errors by issuing a separate SAML request that includes no <RequestedAuthnContext> element.

SP Requires "Step Up" MFA

If a user was initially authenticated without MFA then depending on the identity of the user or the services the user is accessing, the SP may want to "elevate" the user's authentication profile as a prerequisite to allowing further access. To do this, a new SAML authentication request must be generated that includes only https://refeds.org/profile/mfa. This request would be equivalent to the requests generated under the "SP always requires MFA" section, above.

Why Reference ITU-T X.1254?

The REFEDS Multifactor Authentication Profile references ITU-T X.1254 as it references four different factors for authentication in a well described way. Other frameworks define 3 factors, which is more limiting for implementors. These four areas are:

- something an entity has (e.g., device signature, passport, hardware device containing a credential, private key);
- something an entity knows (e.g., password, PIN);
- something an entity is (e.g., biometric characteristic);
- something an entity typically does (e.g., behaviour pattern).

Please note that this reference is purely to the good definitions used by ITU-T X.1254 for authentication factors - there is no other relationship between the MFA Profile and this, or any other, assurance framework at this time.

Do You Provide Profiles for the Authentication Approaches?

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.

The following FAQ support the use of the REFEDS Multifactor Authentication Profile. This documentation is intended to be non-normative supporting information. If you have any questions about the use of the REFEDS MFA Profile, please direct them to the REFEDS mailing list (refeds@lists.refeds.org).

- What does the Profile Guarantee?
- What constitutes an acceptable "second" factor?
- Why two of the four types?
- What do you mean by "independent" factors?
- How Does the MFA Profile relate to (level) of assurance profiles?
- Is this Profile SAML specific?
- How do I implement this in SAML?
- What Does the (SAML) SP need to do?
- How Do I Create SAML Requests?
- What are the Use Cases for Including the <RequestedAuthnContext> Element?
    - SP always requires MFA
    - SP prefers, but does not require, MFA
    - SP Requires “Step Up” MFA
- Why Reference ITU-T X.1254?
- Do You Provide Profiles for the Authentication Approaches?

What are the requirements for multifactor authentication in the profile?

In order to assert the REFEDS MFA profile, the 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.

What does the Profile Guarantee?

The Profile signals that the specific user in question is using multifactor authentication in a way that meetings the requirements shown above. Mutlifactor provides additional safeguards for both IdPs and SPs but is not completely resistant to all possible threats - this should be kept in mind when selecting appropriate approaches and technologies.

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.

Why two of the four types?

Each factor in the MFA profile must be of a different type. This means that validating two separate passwords is not sufficient - the second (and further) factors must use a different factor approach. This is to address any generic point of failure with one factor type.

What do you mean by "independent" factors?

- Implementors must work to ensure that the different factors used in the authentication process are independent, meaning that gaining access to one factor must not trivially grant access to the other factor.
- Any factor that is directly accessible using the first factor is no more secure than the single factor by itself, and so is NOT considered a second factor.
- Institutions are expected to provide safeguards to maintain the independence of their supported authentication factor.
    - a software/virtual phone that is authenticated using the enterprise password is not an appropriate second factor.
- The MFA profile does not enumerate specific requirements the institution must meet to protect against these forms of authentication dependence, but technical restrictions (where feasible) and user education are highly recommended to mitigate the risks of users deploying factors in a manner that decreases their independence.
- Processes that allow a user to immediately register a new second factor (re--registration) using only their “first factor” enterprise password are no more secure than use of the enterprise password itself.
- Implementors are expected to require greater scrutiny before allowing registration of replacement or additional second factors to prevent attackers with password access from simply registering and immediately using a new second factor. Additional second factors can use a existing second factor when registered or the same method as the first second factor.

How Does the MFA Profile relate to (level) of assurance profiles?

Many assurance profiles will include approaches to MFA within them. REFEDS Assurance Framework does not reference the REFEDS MFA Profile but is intended to work in parallel with this profile.

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.

How do I implement this in SAML?

The recommended means of representing these profiles in a SAML assertion are via the <AuthContextClassRef> element (SAML 2.0). These are expressed in SAML statements used to represent acts of authentication by the subject of an assertion. In the case of SAML 2.0, the use of the Authentication Context mechanism has the benefit of enabling signaling of requirements by a relying party in its requests to an identity provider.

Configuration examples for several identity provider technologies are available.

What Does the (SAML) SP need to do?

Most IdPs and campuses that support MFA services do not provide universal MFA coverage for their user communities. This means that even when a given IdP is capable of supporting this profile, there is a significant probability that any given user may not be able to authenticate using MFA. There is no defined mechanism at present to identify whether a given IdP is configured to assert <AuthnContextClassRef> values, and SAML itself does not rely on that knowledge; it assumes that IdPs will respond in accordance with the standard when handling a request containing requirements it cannot meet.. If the SP does not have any information about an IdP's capabilities, it may not be able to distinguish between a case of specific users being unable to satisfy the profile, and an IdP as a whole not supporting it. Whether this distinction is relevant will depend on the SP. <AuthnContextClassRef> value is returned in SAML responses; it is not sufficient to configure an SP to request MFA and assume all responses will therefore contain the MFA context. This is because users can generally bypass an SP's SAML request configuration using unsolicited responses from an IdP, or by handcrafting a SAML request that does not include the MFA requirement.

If an application intends to provide limited services to non MFA authenticated users, the actual <AuthnContextClassRef> value returned to the SP will need to be evaluated dynamically by the application to determine the appropriate access to provide to the user.

How Do I Create SAML Requests?

From a technical standpoint, when generating a SAML authentication request where the MFA profile is desired, the approach is fairly straightforward:

1. Explicitly list every AuthnContextClassRef value that your SP is willing to accept in the <RequestedAuthnContext> element in your SAML request. The actual values you list will depend on your use case (see "Use Cases" below for some general guidance).
2. No matter how carefully you specify context class values, some IdPs may be unable to respond due to software or process limitations. (This issue is not specific to the MFA profile but affects any requests that includes explicit <RequestedAuthnContext> elements). If you want to support IdPs that are not able to support the values you list, then on receiving a SAML error you can try reissuing your SAML request with <RequestedAuthnContext> element.

What are the Use Cases for Including the <RequestedAuthnContext> Element?

SP always requires MFA

This use case is most relevant if the SP operator knows that the IdP in question supports this profile. To require that all users must authenticate using MFA, a SAML authentication request
should include:

```
<samlp:RequestedAuthnContext Comparison="exact">
<saml:AuthnContextClassRef>
https://refeds.org/profile/mfa
</saml:AuthnContextClassRef>
</samlp:RequestedAuthnContext>
```

That is, MFA is the (only) requested value.

Even if an IdP supports the MFA Profile, it can only respond successfully to such a request if MFA is actually performed. If the user can authenticate to the IdP, but is not able to use MFA, the IdP must respond with an error, and the SP will not receive any information about the user who tried to authenticate. If this distinction is important, and it's important to know the identity of the user even if MFA is not possible, consider one of the later uses case of preferring MFA, but accepting less. Application error messages when using this model should explicitly note that MFA is required to access the SP's services.

SP prefers, but does not require, MFA

In some cases, an SP may prefer that users authenticate with MFA but is willing to accept non-MFA authentication. Some scenarios where this approach would make sense:

- Applications that can implement a local scheme to do "stronger authentication" of specific users but prefer to allow users to use familiar campus mechanisms when available.
- Applications that will allow access to some services to all users, but have other services that are limited to those that authenticate using MFA.

- Applications that wish to offer their own opt-in feature for users to elect to use MFA for that service.
- An application that only allows access to users who authenticate with MFA, but wants to personalize error messages to users who do not use MFA as part of the authentication process.

In this scenario it is recommended that the SP request not just the REFEDS MFA Profile, but also any other standard or common <AuthnContextClassRef> values that are acceptable and frequently encountered. A
recommended request that should cover most of these use cases would include:

<samlp:RequestedAuthnContext Comparison="exact">
<saml:AuthnContextClassRef>
https://refeds.org/profile/mfa
</saml:AuthnContextClassRef>
<saml:AuthnContextClassRef>
urn:oasis:names:tc:SAML:2.0:ac:classes:X509
</saml:AuthnContextClassRef>
<saml:AuthnContextClassRef>
urn:oasis:names:tc:SAML:2.0:ac:classes:Kerberos
</saml:AuthnContextClassRef>
<saml:AuthnContextClassRef>
urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport
</saml:AuthnContextClassRef>
<saml:AuthnContextClassRef>
urn:oasis:names:tc:SAML:2.0:ac:classes:Password
</saml:AuthnContextClassRef>

The actual list of AuthnContextClassRef values to support is up to the SP, but this list is likely to address the majority of IdPs. To support arbitrary IdPs, it may still be necessary to respond to SAML errors by issuing a separate SAML request that includes no <RequestedAuthnContext> element.

SP Requires “Step Up” MFA

If a user was initially authenticated without MFA then depending on the identity of the user or the services the user is accessing, the SP may want to “elevate” the user’s authentication profile as a prerequisite to allowing further access. To do this, a new SAML authentication request must be generated that includes only https://refeds.org/profile/mfa. This request would be equivalent to the requests generated under the “SP always requires MFA” section, above.

Why Reference ITU-T X.1254?

The REFEDS Multifactor Authentication Profile references ITU-T X.1254 as it references four different factors for authentication in a well described way. Other frameworks define 3 factors, which is more limiting for implementors. These four areas are:

- something an entity has (e.g., device signature, passport, hardware device containing a credential, private key);
- something an entity knows (e.g., password, PIN);
- something an entity is (e.g., biometric characteristic);
- something an entity typically does (e.g., behaviour pattern).

Please note that this reference is purely to the good definitions used by ITU-T X.1254 for authentication factors - there is no other relationship between the MFA Profile and this, or any other, assurance framework at this time.

Do You Provide Profiles for the Authentication Approaches?

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.