REFEDS Multi-Factor Authentication Profile

Version History: V1.2 (clarification of MFA Profile V1.0: https://refeds.org/profile/mfa)
Status: community consultation draft
Date: 2023-05-16

1. Introduction

This section is informative.

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. These requirements convey a higher quality of authentication than ordinary password authentication (i.e., the authentication is sufficiently secure and trustworthy such that the subject can be strongly associated with the information presented about them). While specific methods of authentication are a factor in this calculation, the REFEDS MFA Profile does not precisely specify or constrain the exact methods used.

This profile does not encompass all forms of “higher quality” authentication and in fact some technologies that may be deemed strong (perhaps even stronger than MFA) are not included in this profile.

A service provider (SP) relying on a federated identity provider (IdP) to perform user authentication uses the signal defined within this Profile to request MFA from an IdP. If MFA is successful, the IdP sends the corresponding signal in its response to indicate that MFA has successfully occurred.

This Profile offers two messaging protocol bindings: for SAML 2.0 and for OpenID Connect.

Relationship to other assurance related issues

It should be noted that there are other assurance related issues, such as identity proofing and registration, that may be of concern to SPs when authenticating users. This Profile does not establish any requirements for these other areas; these additional assurance issues may be addressed by other REFEDS profiles **[REFEDS]**.

Relationship to institution-specific MFA signalling needs

This Profile is specifically applicable when a service provider supports the use of identity providers outside of its own organisational control and specifically requires the semantics described in Section 4.

Deployments of this Profile must adhere strictly to its requirements and cannot override them with local policy requirements. Because this Profile cannot anticipate unique organisational authentication practices and nuances, it is strongly recommended not to use the value defined in this Profile to meet intra-organizational MFA request/response needs.

2. Terms and Definitions

This section is normative.

Term	Definition
federated login	An authentication exchange in which the identity provider and service provider belong to different organisations or administrative domains.
identity provider (IdP/OP)	A party in a federated login exchange that authenticates the subject and asserts information about the subject and the authentication event. In OIDC, this component is synonymous with OpenID Provider (OP).
service provider (SP/RP)	A party in a federated login exchange that requests authentication of a subject by an identity provider and receives an assertion or token vouching for the authentication. In OIDC, this component is synonymous with Relying Party (RP) or Client.
Multi-factor authentication (MFA)	Multifactor refers to the use of an additional, non-password challenge included as part of login, typically in combination with a password.
bearer cookie	An HTTP cookie whose presentation by a user agent is considered valid without additional cryptographic proof.

*The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in **[RFC2119]**.*

3. Profile Identifier

This section is normative.

The use of this profile is identified by the following URI:

`https://refeds.org/profile/mfa`

The use of this value in specific identity protocols is defined in later sections of this document. When used, it signals a requirement for, or the use of, an authentication approach that satisfies the requirements of Section 4 of this document.

This Profile revision clarifies the behaviour expected in the original REFEDS MFA Profile. Future versions of this profile may introduce additional identifiers reflecting different requirements, but the meaning of this identifier will not change in the future.

4. Authentication Requirements

This section is normative.

When signalling MFA using the REFEDS MFA Profile, the IdP is claiming that the user has successfully signed in using a combination of authentication factors sufficient to qualify the user to access the organisation's critical internal systems.

Because this combination of factors may be implemented independently of one another and may occur at different times, this profile also includes guidance on how to communicate the time of authentication and interpret forced re-authentication requirements common to identity protocols, with notable caveats due to implementation constraints.

An IdP MUST NOT signal the use of MFA in the protocol-specific ways outlined in Section 5 unless it was actually performed in accordance with the requirements in this Section. This includes cases in which security policy allows for the bypass or omission of one or more factors for local reasons (e.g., failing "open" for reliability of local services).

> **Guidance:** As discussed in the introduction, this is a key reason why the use of this profile should be discouraged for internal use cases, so as to permit such policies if desired.

4.1 Multiple Factors

The authentication of the user's current session MUST use a combination of at least two of the four distinct types of factors, that is something an entity has (e.g. a hardware device containing a credential), something an entity knows (e.g. password), something an entity is (e.g. biometric), something an entity does (e.g. behavioural).

4.2 Factor Independence

The factors used MUST be independent; this includes processes to recover, replace, or add additional authentication factors.

The combination of the factors MUST mitigate risks related to attacks such as phishing, offline cracking, online guessing and theft of a (single) factor. Protection against active man in the middle attacks is out of scope of this Profile.

> **Guidance:** Independence means that access to one factor does not by itself grant access to or allow the replacement of the other factor. For example, possession of a Single-Factor device by itself may not by itself be used to perform a reset of a "first

factor" password or the other way around. Another precluded example is where the user's "first factor" password grants access to a virtual telecom device that receives callbacks or SMS OTPs that act as the "second factor", allowing registration of additional devices without the use of MFA.

4.3 Validity Lifetime and Time of Authentication

This profile does not impose elapsed-time constraints (i.e., authentication age) between the the time of an SP's authentication request and the actual authentication time of any of the authentication factors used in the assertion. This profile also does not prohibit the use of a bearer cookie as a substitute for the re-application of one or more factors.

To support SPs making policy decisions based on authentication freshness, an IdP SHOULD set the protocol-specific field indicating the time of authentication to the earliest time within an SSO session where a user successfully satisfied any authentication challenges requiring active user intervention within a single sign-on session. See Section 5 for additional guidance.

Note that the above requirement disqualifies setting the time of authentication based on the presence of a browser cookie as a challenge bypass mechanism (e.g., using the "Remember me" feature of third party MFA products). When configuring software to support this profile, a deployer SHOULD take care to prevent such features from influencing the authentication time value in authentication responses.

5. Protocol Specific Bindings

5.1 SAML 2.0 Binding

5.1.1 REFEDS MFA Profile Authentication Context Class Reference

This section is normative.

In SAML 2.0, signalling authentication requirements and outcome is accomplished via the Authentication Context feature of the standard **[SAMLAuthnContext]**. Specifically, the `<AuthnContextClassRef>` element carries a URI referencing how authentication must be, or was, performed.

cvThe REFEDS MFA Profile defines the identifier `https://refeds.org/profile/mfa` as its Authentication Context Class Reference value.

When this value is used (listed/presented) in the `<RequestedAuthnContext>` element in an SP's request (Section 3.4.1 of **[SAMLCore]**), the SP indicates a requirement that the IdP MUST authenticate the subject in accordance with the requirements in Section 4.

When this value is used (listed/presented) in the `<AuthnContext>` element in an IdP assertion (Section 2.7.2 of **[SAMLCore]**), the IdP asserts that the subject was authenticated in accordance with the requirements in Section 4.

The remainder of Section 5.1 provides additional implementation guidance when using this Profile with SAML 2.0. This guidance shall not be interpreted to imply behaviours that are contrary to the SAML 2.0 standard.

5.1.2 IdP Considerations

This section is normative.

5.1.2.1 Signalling Time of Authentication

An IdP responding with the REFEDS MFA Profile context class reference SHOULD set `AuthnInstant` (Section 2.7.2 of **[SAMLCore]**) to the earliest time at which the user was authenticated with any of the factors used to satisfy the MFA requirements. However, any authentication factor referenced to set the `AuthnInstant` timestamp must have required active intervention by the user.

5.1.2.2 Forced Authentication

Upon receiving a SAML authentication request with the `ForceAuthn` flag set to true, an IdP responding with the REFEDS MFA Profile context class reference SHOULD immediately authenticate the user using all required authentication factors. The authentication factors used to satisfy this MFA challenge must each require active intervention by the user.

If the IdP is unable to process the immediate and explicit authentication challenges described above, the IdP SHOULD return an error response to the SP when responding to a SAML authentication request with `ForceAuthn` set to true.

5.1.2.3 Error Handling

IdPs that are unable to meet the requirements of this profile either in whole or for a specific transaction SHOULD ensure whenever possible that an error response is returned to the SP rather than leaving the user stranded. This is necessary to allow for proper error handling by SPs in a variety of scenarios.

5.1.3 SP Considerations

This section is informative.

5.1.3.1 AuthnContextClassRef Usage

The most reliable way for an SP to signal requirement of REFEDS MFA is to include only one `<AuthnContextClassRef>` element (containing the REFEDS MFA Profile Authentication Context Class Reference value).

> **Background:** A SAML request may contain more than one `<AuthnContextClassRef>` element. When an SP sends a request containing multiple `<AuthnContextClassRef>` elements it is signalling that it will accept any of the requested authentication types. An IdP may satisfy any one of the requested authentication methods; it need not satisfy all of them. SAML also allows the request to contain no `<AuthnContextClassRef>` values, which allows the IdP to authenticate the subject using any authentication method it chooses.

5.1.3.2 RequestedAuthnContext Comparison

The SAML specification allows the `Comparison` XML Attribute in the `<RequestedAuthnContext>` element, when present, may be set to values other than the default value of `"exact"`. However, the use of other values requires a shared understanding of the relationship between `<AuthnContextClassRef>` values that is beyond the scope of this Profile and is therefore not recommended.

5.1.3.3 Forced Authentication

In a federated authentication transaction, an SP trusts the IdP to perform user authentication This includes trusting the IdP to determine the appropriate methods and frequency of authentication. The IdP, in turn, relies on this ability to manage authentication frequency to offer the user a smooth single sign-on experience. Setting `ForceAuthn` to true in a SAML authentication request disrupts a user’s single sign-on experience.

This profile recognizes that an SP may require explicit user interaction during a request in order to meet regulatory or risk management requirements. To assist with this need, Section 5.1.2 of this profile provides IdP guidance on how to process the `ForceAuthn` option and set the `AuthnInstant` timestamp when used in conjunction with the REFEDS MFA Profile. If adhered to, these clarifications enable an SP to accurately determine when a complete multi-factor authentication challenge last took place. An SP can therefore make an informed decision as to whether to accept a response, or return the user to the IdP to authenticate again with `ForceAuthn` set to true.

5.1.3.4 Error Handling

Finally, an SP must always be prepared to handle a SAML response that contains an error status rather than an assertion (see third example in Section 5.1.4 for SAML response indicating failure). This is particularly true when making use of the `<RequestedAuthnContext>` element, as the standard mandates that an IdP unable to satisfy the requirements expressed return an error if it responds.

In addition, some exception conditions may prevent an IdP from being able to issue a response at all, so the user agent may be left interacting with an error response from the IdP.

5.1.4 Examples

This section is informative.

An SP issuing a request requiring use of this profile:

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

An edited response indicating the use of this profile:

```
<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:status:Success"/>
  </samlp:Status>
  <saml:Assertion>
    <saml:AuthnStatement ...>
      <saml:AuthnContext>
        <saml:AuthnContextClassRef>
          https://refeds.org/profile/mfa
        </saml:AuthnContextClassRef>
      </saml:AuthnContext>
    </saml:AuthnStatement>
  </saml:Assertion>
  ...
</samlp:Response>
```

An edited response indicating the IdP was unable to authenticate the subject using this profile:

```
<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:status:Responder">
      <samlp:StatusCode
          Value="urn:oasis:names:tc:SAML:2.0:status:NoAuthnContext">
    </samlp:StatusCode>
  </samlp:Status>
</samlp:Response>
```

5.2 OIDC 1.0 Binding

5.2.1 REFEDS MFA Profile `acr` Claim

This section is normative.

In OpenID Connect **[OIDC]**, signalling authentication requirements and use is accomplished with the `acr` claim, which stands for Authentication Context Reference, and was modelled after the similarly-named SAML 2.0 feature (see Section 5.1.1 above). Use of URIs is a recommended practice.

The REFEDS MFA Profile defines the identifier `https://refeds.org/profile/mfa` as an `acr` claim value.

When this value is used (listed/presented) in an RP's request (Section 5.5 of **[OIDC]**), the RP indicates a requirement that the OP MUST authenticate the subject in accordance with the requirements in Section 4.

An RP's `claims` parameter can be sent as an explicit HTTP request parameter or as a claim within a JWT-formatted request object. The former is URL-encoded as a form parameter while the latter is serialised as a JWT **[RFC7519]**.

The use of the `acr_values` parameter MUST NOT be used for this purpose, because it signals a non-essential or voluntary claim requirement, and cannot cause the OP to enforce the use of the Profile.

When this value is used (listed/presented) as a claim value in an OP's ID token (Section 2 of **[OIDC]**), the OP asserts that the subject was authenticated in accordance with the requirements in Section 4.

The use of the `amr` claim is unspecified by this profile. It may be used to signal finer-grained details about how authentication was performed.

The remainder of Section 5.2 provides additional implementation guidance when using this Profile with OpenID Connect. This guidance shall not be interpreted to imply behaviours that are contrary to the OIDC specification.

5.2.2 Additional OP Guidance

This section is normative.

5.2.2.1 Signalling Time of Authentication

An OP responding with the REFEDS MFA Profile `acr` claim value SHOULD set the `auth_time` claim (when including it) to the earliest time at which the user was authenticated with any of the factors used to satisfy the MFA requirements. However, any authentication factor referenced to set the `auth_time` claim must have required active intervention by the user.

5.1.2.2 Forced Authentication

An OP receiving the `prompt=login` key and value in a request and responding with the REFEDS MFA Profile `acr` claim SHOULD immediately authenticate the user using all required authentication factors. The authentication factors used to satisfy this MFA challenge must each require active intervention by the user.

Further, use of the `max-age` option should be enforced similarly, such that any factor applied at a time older than the specified value SHOULD be re-applied in a manner that requires active intervention by the user.

If unable to provide such guarantees, then OPs SHOULD ensure that a request containing these options results in an error response returned to the RP.

5.1.2.3 Error Handling

OPs that are unable to meet the requirements of this profile either in whole or for a specific transaction SHOULD ensure whenever possible that an error response is returned to the RP rather than leaving the user stranded. This is necessary to allow for proper error handling by RPs in a variety of scenarios.

5.2.3 Additional RP Guidance

This section is informative.

5.2.3.1 `acr` Usage

The most reliable way for an RP to signal requirement of REFEDS MFA is to include only one `acr` requested claim value (containing the REFEDS MFA Profile value).

> **Background:** An OpenID request may contain more than one `acr` requested claim value. When an RP sends a request containing multiple requested `acr` claim values it is signalling that it will accept any of the requested authentication types. An OP may satisfy any one of the requested authentication methods; it need not satisfy all of them. OpenID also allows the request to contain no requested `acr` claim values, which allows the OP to authenticate the subject using any authentication method it chooses.

5.2.3.2 Forced Authentication

In a federated authentication transaction, an RP trusts the OP to perform user authentication This includes trusting the OP to determine the appropriate methods and frequency of authentication. The OP, in turn, relies on this ability to manage authentication frequency to offer the user a smooth single sign-on experience. Using the `prompt=login` or `max-age` options in a request disrupts a user’s single sign-on experience.

This profile recognizes that an RP may require explicit user interaction during a request in order to meet regulatory or risk management requirements. To assist with this need, Section 5.2.2 of this profile provides OP guidance on how to process these options and populate the `auth_time` claim when used in conjunction with the REFEDS MFA Profile. If adhered to, these clarifications enable an RP to accurately determine when a complete multi-factor authentication challenge last took place. An RP can therefore make an informed decision as to whether to accept a response, or return the user to the OP to authenticate again with one of these options.

5.2.3.3 Error Handling

Finally, an RP must always be prepared to handle an OP response that contains an error status rather than a code or token. This is particularly true when requesting an essential `acr` claim, as the standard mandates that an OP unable to satisfy the requirements expressed return an error if it responds (see Section 5.5.1.1 of **[OIDC]**).

In addition, some exception conditions may prevent an OP from being able to issue a response at all, so the user agent may be left interacting with an error response from the OP.

5.2.4 Examples

This section is informative.

An RP issuing a request requiring use of this profile using a parameter:

```
{
  "claims":
    {
      "id_token":
      {
       "acr": {
         "essential": true,
         "values": ["https://refeds.org/profile/mfa"]
        }
      }
    }
}
```

An RP issuing a request requiring use of this profile using a request object:

```
{
  "iss": "s6BhdRkqt3",
  "aud": "https://server.example.com",
  "response_type": "code id_token",
  "client_id": "s6BhdRkqt3",
  "redirect_uri": "https://client.example.org/cb",
  "scope": "openid",
  "state": "af0ifjsldkj",
  "nonce": "n-0S6_WzA2Mj",
  "max_age": 86400,
  "claims":
    {
      "id_token":
      {
       "acr": {
         "essential": true,
         "values": ["https://refeds.org/profile/mfa"]
        }
      }
    }
}
```

An ID token example issued by an OP using this profile:

```
 {
   "iss": "https://server.example.com",
   "sub": "24400320",
   "aud": "s6BhdRkqt3",
   "nonce": "n-0S6_WzA2Mj",
   "exp": 1311281970,
   "iat": 1311280970,
   "auth_time": 1311280969,
   "acr": "https://refeds.org/profile/mfa"
  }
```

A response indicating the OP was unable to authenticate the subject using this profile:

```
HTTP/1.1 302 Found
Location: https://client.example.org/cb?
   error=invalid_request
   &error_description=Unsupported%20acr%20value
   &state=af0ifjsldkj
```

6. References

[SAMLAuthnContext] Authentication Context for the OASIS Security Assertion Markup Language (SAML) V2.0, https://docs.oasis-open.org/security/saml/v2.0/saml-authn-context-2.0-os.pdf

[SAMLCore] Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0, https://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf

[OIDC] OpenID Connect Core 1.0. November 2014. https://openid.net/specs/openid-connect-core-1_0.html

[**RFC2119**] Key words for use in RFCs to Indicate Requirement Levels, https://datatracker.ietf.org/doc/rfc2119/

[RFC7519] JSON Web Token (JWT), https://datatracker.ietf.org/doc/html/rfc7519

[REFEDS] Listing of REFEDS Specifications and Profiles; https://refeds.org/specifications.