REFEDS MFA Profile Recommendation

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

Version History: v0.1: this document

1. Introduction

This Multi-Factor Authentication (MFA) Profile specifies requirements that an authentication event must meet in order to communicate the usage of MFA. It also defines a SAML authentication context for expressing this in SAML.

The MFA Authentication Context can be used by Service Providers to request that Identity Providers perform MFA as defined below and by IdPs to notify SPs that MFA was used.

The Profile Recommendation is based on the OASIS Authentication Context for SAML [1] and the MFA Interop Final Report by InCommon [2].

2. Scope

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, however, does not establish any requirements for those other issues; these may be addressed by other REFEDS profiles [3].

3. Syntax

In a SAML assertion, compliance is communicated by asserting the AuthnContextClassRef:

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

4. Criteria

By asserting the URI shown above, an Identity Provider claims that:

- 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) [4].
- 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.

5. SAML Representation

The recommended means of representing these profiles in a SAML assertion are via the `<AuthnContextClassRef>` element (SAML 2.0). These are expressed in SAML statements used to represent the means of authentication by the subject of an assertion.

SPs will need to validate that the https://refeds.org/profile/mfa `<AuthnContextClassRef>` value is returned in SAML responses; it is not sufficient to configure an SP to request MFA and assume all responses will contain the MFA context.

From a technical point of view, the approach to generate a SAML authentication request with MFA is straightforward:

- Explicitly list every AuthnContextClassRef value that your SP is willing to accept in the `<RequestedAuthnContext>` element in your SAML request, listed in order of preference. The actual values you list will depend on your use case and are described in the OASIS Authentication Context for SAML [1].
- No matter how carefully you specify context class values, some IdPs may be unable to respond due to software or process limitations. Consider reissuing your SAML request with no `<RequestedAuthnContext>` element if an authentication request specifying allowable values returns a SAML error.

6. References

[1] Kemp, John at al. "Authentication Context for the OASIS Security Assertion Markup Language(SAML) V2." 15 March 2005: https://docs.oasis-open.org/security/saml/v2.0/saml-authn-context-2.0-os.pdf.

[2] Herrington, Karen et al. "Multi-Factor Authentication (MFA) Interoperability Profile Working Group Final Report." 23 June 2016: https://spaces.internet2.edu/display/MIPWG/Final+Products+of+the+MFA+Interoperability+Profile+Working+Group?preview=/98992612/98992945/MFAInteropFinalReport-3.pdf.

[3] REFEDS Profiles are listed at: https://refeds.org/specifications.

[4] International Telecommunication Union. "Series X. Data Networks, Open System Communication and Security. Cyberspace security – Identity management. Entity authentication assurance framework. Standard X.1254." September 2012: https://www.itu.int/rec/T-REC-X.1254-201209-I/en