REFEDS Single Factor Authentication Profile (DRAFT 2 May 2018)

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

Version History: v0.2: this document

1. Introduction

This Single Factor Authentication (SFA) Profile specifies requirements that an authentication event must meet in order to communicate the usage of SFA. It also defines a SAML and OpenID Connect (OIDC) authentication context for expressing it. The SFA authentication context can be used by Relying Parties (RPs) to request that Identity Providers (IdPs) perform SFA as defined below and by IdPs to notify that SFA was used.

Terminology used in this document is based on NIST Special Publication 800-63B [3].

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 the REFEDS Assurance Framework [1] or other REFEDS Profiles [2].

3. Syntax

Compliance with this profile is communicated by asserting:

SAML	assertion: AuthnContextClassRef	https://refeds.org/profile/sfa
OIDC	id token: acr claim	

4. Criteria

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

- The authentication factor must fulfill the following requirements:
  - Authenticator secrets have at least the following minimum length:

Authenticator type[1]	**Secret basis**[2]	**Minimum length**
Memorized Secret	≥52 characters *(e.g. 52 letters)*	12 characters
	≥72 characters *(e.g. 52 letters + 10 digits + 10 special characters)*	8 characters
Time based OTP-Device Out-of-Band Device	10-51 characters *(e.g. 10 digits)*	6 characters
	≥52 characters *(e.g. 52 letters)*	4 characters
Look-Up Secret Sequence based OTP-Device	10-51 characters *(e.g. 10 digits)*	10 characters
	≥52 characters *(e.g. 52 letters)*	6 characters
Cryptographic Software/Device	RSA/DSA	2048 bit
	ECDSA	256 bit

  - Secrets that are transmitted must have a maximum life span according to the way of delivery.

Way of delivery	**Maximum life time**
Time based OTP Device	5 minutes
Telephone network (e.g. SMS, phone)	10 minutes
E-mail (e.g. recovery link)	24 hours
Postal mail	1 month

[1] Biometrics are excluded because of its lacking applicability as a single factor for web authentication.
[2] The secret is chosen out of the given character set or based on the specified algorithm

    - Accounts are protected against online guessing attacks (e.g. rate limiting).
    - Authentication secrets at rest and in online transit must be cryptographically protected.

- Replacement of a lost authentication factor ensures all of the following, as applicable:
    - An existing secret must not be sent to the user (e.g. a stored password).
    - The replacement procedure relies not solely on knowledge based authentication (e.g. answer a secret question).
    - Human based procedures (e.g. service desk) ensure a comparable level of assurance of the requesting user identity as the initial identity vetting.
    - In order to restore a lost authentication factor, an OTP may be sent to the users address of record. All corresponding requirements apply as though this OTP would be a Look-Up Secret, except that it may be transmitted without being cryptographically protected.
    - For authenticators which are provided to the user as a backup, all requirements of the corresponding authentication factor apply.

References

[1] REFEDS Assurance Framework:
https://wiki.refeds.org/display/GROUPS/Assurance+Working+Group

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

[3] NIST Special Publication 800-63B Digital Identity Guidelines, June 2017:
https://doi.org/10.6028/NIST.SP.800-63b