REFEDS Single Factor Authentication Profile

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.

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:

1. The authentication factor must fulfill the following requirements:
    1.1. 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

    1.2. 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] See Appendix A for definitions of these authenticator types. Biometrics are excluded because of its lacking applicability as a single factor for web authentication.
[2] The secret is chosen/generated out of the given character set or based on the specified algorithm. See Appendix B for example combinations of secret basis and secret length.

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

2. Replacement of a lost authentication factor ensures all of the following, as applicable:
   2.1. An existing secret must not be sent to the user (e.g. a stored password).
   2.2. The replacement procedure does not solely rely on knowledge-based authentication (e.g. answer a secret question).
   2.3. Human based procedures (e.g. service desk) ensure a comparable level of assurance of the requesting user identity as the initial identity vetting.
   2.4. 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.
   2.5. 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

Appendix A - Terminology:

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

Memorized Secret (*something you know*):
A memorized secret is a character string typically chosen by the user, e.g. password or PIN.

OTP-Device (*something you have*):
An One-Time-Password-Device generates an OTP based on a stored secret. This applies to dedicated hardware devices as well as software like mobile phone applications. The generation of an OTP can be done either time-based or sequence based.

Out-of-Band Device (*something you have*):
An Out-of-Band Device transmits a secret via a distinct communication channel that is different from the one used for authentication, e.g. SMS.

Look-Up Secret (*something you have*):
Look-Up secrets are a physical or electronic set of character strings provided to the user in advance. Each string is used only once for a single authentication event. A common use case are recovery keys which can be used to restore a lost authentication factor.

Cryptographic Device/Software (*something you have*):
A cryptographic software uses a cryptographic key to generate an authentication secret. A cryptographic device is dedicated hardware with an embedded cryptographic key, which cannot be directly accessed. In both cases, the generated secret is used to authenticate and therefore prove possession of the authentication factor.

Appendix B - Memorized Secret Example:

There are two sizes available for the secret basis (≥52 and ≥72) of memorized secrets, on which the secret length depends.

Character set size	Example character set	Example secret
≥ 52	(a-z)(A-Z)	doHskLAnPaEb
≥ 52	(A-Z)(26 special french characters)	ÆZHéIÔMNúYPU
≥ 72	(a-z)(A-Z)(0-9)(10 special characters)	L&Qn3?hM
≥ 72	(48 greek letters)(0-9)(14 special characters)	α1Σ%β34σ

Although all other authenticator types are generated (not user chosen), the secret and secret basis are handled analogously.