Document	SWAMID Person-Proofed Multi-Factor Profile
Identifier	http://www.swamid.se/policy/assurance/al2mfa
Version	V1.0
Last modified	2018-09-12
Pages	10
Status	FINAL
License	Creative Commons BY-SA 3.0

SWAMID Person-Proofed Multi-Factor Profile

Innehåll

1 Terminology and Typographical Conventions

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.

Text in Italics is non-normative. All other text is normative unless otherwise stated.

All normative parts of the profile are governed by the SWAMID Board of Trustees.

The non-normative (guidance) is maintained by the SWAMID Operations team.

1.1 Definition of terminology

Home Organisation: The SWAMID Member Organisation with which a Subject is affiliated, operating the Identity Provider by itself or through a third party.

Member Organisation: Used in this document as a synonym for Home Organisation

Subject: Any natural person, i.e. end user, affiliated with a Home Organisation, e.g. as a teacher, researcher, staff or student.

Relying Party (RP): A Service that relies upon a Subject's credentials, typically to process a transaction or grant access to information or a system. Also called a Service Provider (SP).

Identity Provider (IdP): The system component that issues Attribute assertions on behalf of Subjects who use them to access the services of Relying Party.

First factor: A knowledge-based (i.e., "something you know") or an inherent (i.e., "something you are") authentication factor used by the Subject together with a second factor to form a multi-factor. Traditionally the knowledge-based factor is the password used used for single-factor authentication. An inherent authentication factor cannot be used as a standalone single-factor.

Second factor: A independent possession-based (i.e., "something you have") authentication factor that is used in addition to the Subject's first factor in order to provide the Subject with the ability to use multi-factor authentication.

Full multi-factor: A complete new set of credentials assigned to the Subject in order to provide the Subject with the ability to use multi-factor authentication. This new set of credentials is by itself composed of at least two dependent factors (e.g. a smart card) and does not depend in any way on the normally used knowledge-based authentication factor, i.e. a password, belonging to the Subject.

2 Purpose, Scope and Summary

This profile defines how a SWAMID member organisation MUST implement a multi-factor solution in order to be certified by SWAMID for person-proofed multi-factor authentication in a federated environment. A person-proofed second factor or a person-proofed full multi-factor combines the use of multi-factor authentication with an assurance that the multi-factor authenticator is distributed to the intended Subject.

There are two levels of identity proofing methods defined for issuing multi-factors, one based on the identity proofing in SWAMID Identity Assurance Level 2 Profile (SWAMID AL2) [1] and one with a high identity assurance based on verifying the Subject with a defined set of identity cards and passports.

This SWAMID Person-Proofed Multi-Factor Profile is an extension to the REFEDS Multi-Factor Authentication (MFA) Profile (REFEDS MFA) [2].

Guidance

The intended use of this SWAMID profile is when authentication must be done with a high assurance that it is the correct Subject that is accessing a specific service.

Please note that it is possible to use Subject self-asserted multi-factor authentication in both a local environment and a federated environment in order for the Home Organisation to raise IT security, but it does not raise the identity assurance, i.e. the user is only protecting the usage of his or her own account with a multi-factor authentication. Hence this use case is not covered by this profile.

3 Compliance and Audit

Evidence of compliance with this profile MUST be part of the Identity Management Practice Statement (IMPS), maintained as a part of the SWAMID membership process. The Identity Management Practice Statement MUST describe how the organisation fulfils the normative parts of this document.

SWAMID operations, or another party approved by SWAMID Board of Trustees, conducts an initial audit of the submitted Identity Management Practice Statement. The member MUST annually confirm that their Identity Management Practice Statement is still valid. When there are changes in the identity management process or technology, a new Identity Management Practice Statement MUST be submitted for a renewed audit.

The Member organisation MUST perform a successful technical validation of their Identity Provider through the official SWAMID person-proofed multi-factor validation service to complete the audit.

Guidance

The audit routines for this profile are the same as for the SWAMID Identity Assurance Level 2 Profile with the addition of the technical validation.

SWAMID person-proofed multi-factor validation service is located at https://mfa-check.swamid.se.

4 Organisational Requirement

The purpose of this section is to define conditions regarding participating organisations responsibilities.

The Member organisation MUST be certified for SWAMID Identity Assurance Level 2 Profile.

5 Operational Requirements

The purpose of this section is to define conditions and guidance regarding use of person-proofed multi-factor authentication.

Only Subjects currently at SWAMID Identity Assurance Level 2 are allowed to authenticate themselves according to this Profile.

A Member Organisation MUST fulfil the REFEDS MFA Profile criteria.

Guidance

Original criteria repeated from REFEDS MFA Profile for convenience

By asserting the URI shown above (note: https://refeds.org/profile/mfa), 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).*
- *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.*

5.1 Credential Operating Environment

The purpose of this subsection is to ensure adequate strength of Subject credentials and protection against common attack vectors.

The selected second factor or full multi-factor technology MUST be based on the Single-Factor and Multi-Factor Authenticator Types within NIST 800-63B [3].

Second factor (used together with a knowledge-based or an inherent authentication factor)

- Single-Factor OTP Device
- Single-Factor Cryptographic Software
- Single-Factor Cryptographic Device

Full multi-factor

- Multi-Factor OTP Device
- Multi-Factor Cryptographic Software
- Multi-Factor Cryptographic Device

The selected second factor or full multi-factor technology MUST be protected against credential cloning and MUST NOT be possible to move between physical devices.

Member organisation's Identity Provider MUST support renewed multi-factor authentication if requested by the Relying Party.

Guidance

Choice of multi-factor technology should be documented together with the use of password in the IMPS, section 5.1.

Single-Factor and Multi-Factor OTP Devices have similar weaknesses to social engineering as passwords but one OTP code can only be used once and if a time based OTP (TOTP) solution is used the risk is further reduced but not negligible. The use of OTP devices will be deprecated 2025, or earlier, due to the risks with the technology.

SWAMID has published a set of valid choices for second factor and full multi-factor solutions in the SWAMID wiki.

If the Relying Party requires that the multi-factor login must not use Single-Sign On the member organisation's Identity Provider must be able to require that the Subject do a new multi-factor login even though the Subject already have a multi-factor session active with the Identity Provider.

5.2 Credential Issuing

The purpose of this subsection is to ensure that the Identity Provider has control over the issuing process of the multi-factor.

The second factor or full multi-factor must be issued to the Subjects without only using the current single factor credential, i.e. password, for identity proofing in accordance with the REFEDS MFA Profile criteria.

Subjects within an Identity Provider MAY use single factor authentication and multi-factor authentication independently of each other, i.e. all Subjects need not be issued multi-factor credentials.

Not all Subjects within an Identity Provider need to use the same credential types, some of them can only use passwords, some Person-Proofed Multi-Factors and some Person-Proofed Multi-Factors with high identity assurance. A Subject can also have multiple credentials types at the same time, but it is however important that the Home Organisation maintain a record of credential types a Subject can use and can correctly inform Relying Parties about the credential type used if requested by the Relying Party.

Person-Proofed Multi-Factor (SWAMID AL2-MFA)

A multi-factor authenticator issued and proofed to a Subject fulfilling the requirements the SWAMID Identity Assurance Level 2 Profile with additional identity proofing requirements for on-line proofing.

Person-Proofed Multi-Factor with high identity assurance (SWAMID AL2-MFA-HI)

A multi-factor authenticator issued and proofed to a Subject fulfilling the requirements the SWAMID Identity Assurance Level 2 Profile with additional identity proofing requirements based on verifying the Subject with defined identity cards or passports.

Guidance

Processes for issuing and assigning of multi-factor credentials (second factor or full multi-factor) should be documented together with the initial credential issuing in the IMPS, section 5.2.

It's not recommended for a specific Subject to have Person-Proofed Multi-Factors and a Person-Proofed Multi-Factors with high identity assurance at the same time due the importance to differentiate between them in time of authentication and attribute release.

5.2.1 Issuing a Person-Proofed Multi-Factor (SWAMID AL2-MFA)

Credential Issuing of second factor or full multi-factor fulfilling the SWAMID Identity Assurance Level 2 Profile MUST be done using one of the following methods

1. On-line authenticating the Subject using a **Person-Proofed Multi-Factor**, or higher, using an external Identity Provider compliant with the SWAMID Person-Proofed Multi-Factor Profile,
2. On-line authenticating the Subject using a multi-factor issued according to the Swedish E-identification system using an external Identity Provider compliant with the the Swedish E-identification Level of Assurance 2 or higher,
3. On-line authenticating the Subject using a **Person-Proofed Multi-Factor**, or higher, already issued to the Subject in the Home Organisation's Identity Provider,
4. In-person visit at a service desk in combination with identity proofing as defined by the Swedish Tax Agency for issuance of the Swedish Tax Agency identity card,
5. In-person visit at a service desk in combination with identity proofing with an international passport fulfilling ICAO Doc 9303, an EU/EES national identity card fulfilling the European Commission Regulation No 562/2006 or an EU/EES driving license fulfilling the European Parliament and the Council of European Union Directive 2006/126/EC,
6. Off-line using a postal **registered address** (sv. folkbokföringsadress) in combination with a time-limited one-time activation password/pin code,
7. Off-line using a copy of the same identification token as described in 4 or 5 above and a copy of a utility bill, not older than 3 months, in combination with a time-limited one-time activation password/pin code sent to the postal address on the utility bill,
8. Off-line using a postal **registered address** (sv. folkbokföringsadress) with a preregistered device, unique for the Subject, that will be considered as a Person-Proofed Multi-Factor on first use,
9. Off-line using a copy of the same identification token as described in 4 or 5 above and a copy of a utility bill, not older than 3 months, with a preregistered device, unique for the Subject, sent to the postal address on the utility bill that will be considered as a Person-Proofed Multi-Factor on first use, or
10. Other identity proofing method deemed equivalent by SWAMID Board of Trustees.

Guidance

Observe that not all Identity Providers within the Swedish E-identification system can be used for online identity proofing due to their Identity Provider usage policies.

If you are using Identity Providers within the Swedish E-identification system you must also accept authentication via eIDAS with assurance level low, substantial or high if you can bind the identity of the Subject.

Allowing the Subject to add multiple multi-factors (3 above) by proving proof of possession increase the flexibility for the Subjects, i.e. allow multiple devices or software cryptographic keys tied to the same Subject.

Time-limited one-time passwords/pins used in 6 & 7 should be valid only as long as needed for postal delivery. By copy in 7 means either a scanned, photo of or hardcopy of the identity card/passport.

5.2.2 Issuing a Person-Proofed Multi-Factor with high identity assurance (SWAMID AL2-MFA-HI)

Credential Issuing of second factor or full multi-factor for fulfilling the SWAMID Identity Assurance Level 2 Profile and with high identity assurance MUST be done using one of the following methods

1. On-line authenticating the Subject using a **Person-Proofed Multi-Factor with high identity assurance** using an external Identity Provider compliant with the SWAMID Person-Proofed Multi-Factor Profile,
2. On-line authenticating the Subject using a multi-factor issued according to the Swedish E-identification system using an external Identity Provider compliant with the the Swedish E-identification Level of Assurance 3 or higher,
3. On-line authenticating the Subject using a **Person-Proofed Multi-Factor with high identity assurance** already issued to the Subject in the Home Organisation's Identity Provider,
4. In-person visit at a service desk in combination with identity proofing as defined by the Swedish Tax Agency for issuance of the Swedish Tax Agency identity card,
5. In-person visit at a service desk in combination with identity proofing with an international passport fulfilling International Civil Aviation Organization (ICAO) Doc 9303 Machine Readable Travel Documents [4], an EU/EES national identity card fulfilling the Regulation (EU) 2016/399 of the European Parliament and of the Council [5] or an EU/EES driving license fulfilling the Directive 2006/126/EC of the European Parliament and of the Council of 20 December 2006 on driving licences [6],
6. Off-line using a postal **certified mail** (sv. rekommenderat brev med personlig utlämning) in combination with a time-limited one-time activation password/pin code, or
7. Off-line using a postal **certified mail** (sv. rekommenderat brev med personlig utlämning) with a preregistered device, unique for the Subject, that will be considered as a Person-Proofed Multi-Factor with high identity assurance on first use.

Guidance

Observe that not all Identity Providers within the Swedish E-identification system can be used for online identity proofing due to their Identity Provider usage policies.

If you are using Identity Providers within the Swedish E-identification system you must also accept authentication via eIDAS with assurance level substantial or high if you can bind the identity of the Subject.

Allowing the Subject to add multiple multi-factors (3 above) by proving proof of possession increase the flexibility for the Subjects, i.e. allow multiple devices or software cryptographic keys tied to the same Subject.

Time-limited one-time passwords/pins used in 6 should be valid only as long as needed for postal delivery of certified mail.

5.2.3 Multiple Multi-Factor Identity Proofing levels within one Identity Provider

A SWAMID Member Organisation MAY implement both **Person-Proofed Multi-Factor** and **Person-Proofed Multi-Factor with high identity assurance** within one Identity Provider.

The Member Organisation MUST maintain a record of all Subjects' Credentials and identity proofing level used to issue them.

5.3 Credential Renewal and Re-issuing

Renewal of credentials occur when the Subject changes its credential using normal password reset. Re-issuing occurs when credentials have been invalidated.

Guidance

Processes for replacement of second factors or full multi-factors should be documented in the IMPS, section 5.3.

5.4 Credential Renewal

All Subjects MUST be able change a software-based second factor.

Subjects MUST demonstrate possession of credentials by doing a multi-factor authentication before being allowed to replace a second factor or full multi-factor.

Guidance

By doing a multi-factor authentication according to this profile a Subject can replace the currently issued multi-factor or add a second multi-factor at the same identity proofing level as the Subject's currently issued multi-factor as long as the used multi-factor authentication is on the same level or higher.

Even though there are no special criteria for a Subject changing password when a second multi-factor is in use it is recommended that the Subject proof possession of both password and second factor when the Subject changes the password.

5.5 Credential Re-issuing

Re-issuing of second factor or full multi-factor MUST be done using the same methods as listed in 5.2.1 or 5.2.2 depending on level of identity assurance for Credential Issuing.

5.6 Credential Revocation

The purpose of this subsection is to ensure that credentials can be revoked.

Guidance

Processes for revocation of second factors or full multi-factors should be documented in the IMPS, section 5.4.

5.6.1 The Member Organisation's ability to Revoke Credentials

The Member Organisation MUST be able to revoke a Subject's second factor or full multi-factor in order to

- Stop the Subject's ability to use multi-factor authentication, and
- Allow the Subject to replace the second factor or full multi-factor.

5.6.2 The Member Organisation's obligation to Revoke Credentials

The Member Organisation MUST revoke the Subject's ability to use multi-factor authentication according to the SWAMID Person-Proofed Multi-Factor Profile if the Subject's Credentials is known to be compromised or misused.

Guidance

If a Subject's second factor or full multi-factor has been misused or compromised the multi-factor should be revoked and the Subject should not be able to a create a new one until the Subject is formally informed why the multi-factor was revoked.

If an individual is no longer affiliated with a Home Organisation, i.e. no longer a Subject, all of the Credentials belonging to that should be revoked in order to avoid a situation where only the username and password are inactivated and later re-activated with a second token becoming active without a re-issuing of the second factor.

6 Syntax

If a member organisation's Identity Provider is approved for **Person-Proofed Multi-Factor** the Identity Provider is tagged in the SWAMID metadata with the assurance certification attribute http://www.swamid.se/policy/authentication/swamid-al2-mfa.

If a member organisation's Identity Provider in addition is approved for **Person-Proofed Multi-Factor with high identity assurance** the Identity Provider is also tagged in the SWAMID metadata with the assurance certification attribute http://www.swamid.se/policy/authentication/swamid-al2-mfa-hi.

In accordance with REFEDS MFA Profile:

- In a SAML assertion, in compliance with this **Person-Proofed Multi-Factor Profile** or **Person-Proofed Multi-Factor with high identity assurance**, a performed multi-factor authentication is communicated by that the Identity Provider is asserting the AuthnContextClass https://refeds.org/profile/mfa.
- In a SAML authentication request a Relying Party can request multi-factor authentication by adding AuthnContextClassRef https://refeds.org/profile/mfa to the authentication request.

When a Subject performs a multi-factor authentication based on the **Person-Proofed Multi-Factor with high identity assurance** the Identity Provider MUST add the value http://www.swamid.se/policy/authentication/swamid-al2-mfa-hi to the attribute eduPersonAssurance of the Subject in order for the Relaying Party to be able to distinguish between the two identity proofing levels of multi-factor authentication.

Guidance

The eduPersonAssurance value for Person-Proofed Multi-Factor with high identity assurance should only be released if a multi-factor authentication occurred at that authentication assurance level.

SWAMID will provide configurations examples in the SWAMID wiki for the most used Identity Provider software.

7 References

[1] SWAMID Identity Assurance Level 2 Profile: http://www.swamid.se/policy/assurance/al2
[2] REFEDS Multi-Factor Authentication (MFA) Profile: https://refeds.org/profile/mfa
[3] NIST Special Publication 800-63B - Digital Identity Guidelines - Authentication and Lifecycle Management: https://doi.org/10.6028/NIST.SP.800-63b
[4] International Civil Aviation Organization (ICAO) Doc 9303 Machine Readable Travel Documents: https://www.icao.int/publications/pages/publication.aspx?docnum=9303
[5] Regulation (EU) 2016/399 of the European Parliament and of the Council: http://data.europa.eu/eli/reg/2016/399/oj
[6] Directive 2006/126/EC of the European Parliament and of the Council of 20 December 2006 on driving licences: http://data.europa.eu/eli/dir/2006/126/oj