Document	SWAMID Identity Assurance Level 2 Profile
Identifier	http://www.swamid.se/policy/assurance/al2
Version	V2.0
Last modified	2020-06-15
Pages	13
Status	FINAL
License	Creative Commons BY-SA 3.0

SWAMID Identity Assurance Level 2 Profile

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.

Text in green shows where there is a difference between SWAMID Identity Assurance Level 2 Profile and SWAMID Identity Assurance Level 1 Profile.

SWAMID has multiple assurance level profiles. All Identity Assurance Profiles share the same numbering scheme.

1.1. Definition of terminology

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

Subject: Any natural person affiliated with a Member Organisation, e.g. as a teacher, researcher, staff or student.

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

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 known as Service Provider (SP).

Shared secret: A piece of information that is shared exclusively between the parties involved in a secure communication.

Credential: A combination of information, cryptographic software and/or cryptographic hardware which a Subject proves possession of in order to authenticate itself in the Member Organisation's Identity Provider. This can be for example the combination of a username and password or a username and cryptographic device.

Credential issuing: The process of issuing a Subject a set of credentials which the Subject can use to authenticate itself in the Member Organisation's Identity Provider. This also includes the process when a Member Organisation issues an additional set of credentials to the same Subject.

Credential re-issuing: The process where a Member Organisation re-issues credentials to a Subject who has previously been issued credentials, i.e. by replacing a malfunctioning cryptographic device or by giving a Subject the possibility to reset a forgotten password.

Credential renewal: The process where a Subject voluntary change his or her credentials by proving possession of the current credentials, i.e. changing a password by proving knowledge of the current password.

Credential revocation: The process where a Member Organisation invalidates a set of credentials currently issued to a Subject, i.e. because the credentials are suspected to be compromised or if he or she is no longer a current Subject of the Member Organisation.

CAPTCHA: A challenge-response test used as an attempt to ensure that the response is generated by a human being, e.g. a picture with characters that a Subject must retype in a text field.

2. Purpose, Scope and Summary

This document defines the SWAMID Identity Assurance Level 2 Profile. This profile is an extension of the SWAMID Identity Assurance Level 1 Profile.

A claim at this Identity Assurance Profile implies the following:

- the subject is affiliated with the Member Organisation;
- the subject is an identified natural person;
- the subject is identified by a unique permanent user identifier; and
- the Member Organisation is responsible for the attributes/information released.

Relying parties in SWAMID may require elevated levels of assurance.

This Identity Assurance Profile is conditionally mappable to but not interchangeable with REFEDS Assurance Framework ver 1.0.

This Identity Assurance Profile is similar to but not interchangeable with the following assurance level profiles:

- Level of Assurance 2 in the sense of Swedish eID Assurance Framework (sv. Tillitsramverket för Svensk e-legitimation);
- Level of Assurance 2 in the sense of ISO/IEC Entity authentication assurance framework (ISO/IEC 29115:2013);
- Assurance Level 2 in the sense of Kantara Initiative Identity Assurance Framework: Service Assessment Criteria (Kantara IAF-1400-SAC); and
- Level of Assurance 2 in the sense of NIST Electronic Authentication Guideline (NIST SP 800-63-2).

3. Compliance and Audit

3.1 Evidence of compliance with this profile MUST be part of the Identity Management Practice Statement, 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.

3.2 SWAMID Operations, or another party approved by SWAMID Board of Trustees, conducts an audit of the submitted Identity Management Practice Statement.

The Member Organisation MUST annually confirm that their Identity Management Practice Statement is still accurate.

The Member Organisation MUST submit an updated Identity Management Practice Statement for renewed audit prior to making changes in the identity management process or technology that makes the Identity Management Practice Statement inaccurate.

Guidance: *SWAMID Operations supplies a template for the Identity Management Practice Statement.*

3.3 SWAMID Board of Trustees MAY impose an additional audit of the Member Organisation performed by SWAMID Operations, or another party approved by SWAMID Board of Trustees.

4. Organisational Requirement

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

4.1 Enterprise and Service Maturity

This subsection defines the organisation and the procedures that govern the operations of the identity provider.

4.1.1 The Member Organisation MUST have a Swedish Company Registration Number, e.g. be a legal entity in Sweden (sv. organisationsnummer för s.k. juridiska personer).

4.1.2 The Member Organisation MUST adhere to applicable Swedish legislation. The Member Organisation MUST conduct and maintain an analysis of applicable legislation for the Identity Provider and underlying systems.

Guidance: *An example of an analysis is provided in the SWAMID Wiki that can be used as an internal template.*

4.1.3 The Member Organisation MUST have documented procedures for data retention and protection in order to ensure the safe management of Subject information.

Guidance*: The Member Organisation must have defined decommission procedures of the Identity Provider and underlying systems for when they are replaced or decommissioned. Special considerations should be taken for decommissioned Components (e.g. hard drives, backup media and other storage media) that may contain sensitive or private Subject information, such as passwords, Swedish Personal Identity Number (sv. personnummer) etc. These components must be safely and permanently disposed of.*

4.2 Notices and User Information

The Member Organisation provides an Acceptable Use Policy (AUP) and a Service Definition including a Privacy Policy (PP) for the organisation Subjects. These policies are needed to fulfil the SWAMID Policy and the Swedish legislation including the General Data Protection Regulation (EU) No 679/2016.

4.2.1 Each Member Organisation MUST publish the Acceptable Use Policy to all Subjects including any and all additional terms and conditions.

4.2.2 All Subjects MUST indicate acceptance of the Acceptable Use Policy before use of the Identity Provider.

Guidance: *A suggested way to fulfil this requirement is to display and accept the Acceptable Use Policy at first login in the Identity Provider.*

4.2.3 All Subjects MUST indicate renewed acceptance of the Acceptable Use Policy if the Acceptable Use Policy is modified.

4.2.4 The Member Organisation MUST maintain a record of Subject Acceptable Use Policy Acceptance.

4.2.5 Each Member Organisation MUST publish the identity provider Service Definition. The Service Definition MUST at least include:

- a general description of the service;
- a Privacy Policy with reference to applicable Swedish law;
- any limitations of the service usage; and
- service desk, or equivalent, contact details.

Guidance: *SWAMIDs recommendation is to use SWAMIDs best practice policy template if none other exists.*

4.3 Secure Communications

This subsection defines how clear text passwords, private keys and shared secrets must be protected to obtain operational security.

4.3.1 Access to shared secrets MUST be subject to discretionary controls which permit access to those roles/applications needing such access.

Guidance: *Access to shared secrets should be limited to as few individuals as possible and life cycled managed.*

4.3.2 Private keys and shared secrets MUST NOT be stored in plain text form unless given adequate physical or logical protection.

Guidance: *Password files and private keys on servers must not be openly accessible but should be subject to operating system access control/restrictions.*

4.3.3 All network communication between systems related to Identity or Credential management MUST be secure and encrypted or be physically secured by other means.

Guidance: *Always use TLS or equivalent for establishing encrypted communications between endpoints and use client certificates or account authentication between services. For example, the communication between an Identity Provider and an LDAP server and the communication between a web application for account management and the identity management backend (e.g. Active Directory) must be encrypted.*

4.3.4 Relying Party and Identity Provider credentials (i.e. entity keys) MUST NOT use shorter comparable key strength (in the sense of NIST SP 800-57) than a 2048-bit RSA key

Guidance: *Keys should not be used for more than 10 years and should be changed when doing a major software upgrade or a hardware replacement*

4.4 Security-relevant Event (Audit) Records

This section defines the need to keep an audit trail of relevant systems.

4.4.1 The Member Organisation MUST maintain a log of all relevant security events concerning the operation of the Identity Provider and the underlying systems, together with an accurate record of the time at which the event occurred (timestamp). These records MUST be retained with appropriate protection and controls to ensure successful retrieval, accounting for service definition, risk management requirements, applicable legislation, and organisational policy.

Guidance: *Audit trails are sensitive personal data and must be protected from unauthorised access. A separate log-server is recommended as best practice but not mandatory. All changes to credentials and attributes used in SWAMID must be logged.*

5. Operational Requirements

The purpose of this section is to ensure safe and secure operations of the service.

5.1 Credential Operating Environment

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

5.1.1 The Identity Provider MUST authenticate Subjects at the request of the Relying Party. The authentication MUST be performed using either Single-Factor Authentication or Multi-Factor Authentication.

Single-Factor Authentication of Subjects MUST be performed using either

- a memorised secret as defined in NIST 800-63B, i.e. a password or a passphrase with
  - at least 24 bits of entropy as defined in (the old) NIST SP 800-63-2, Appendix A; or
  - a score of at least 3 (safely unguessable) as defined by the zxcvbn password strength definition in February 2017;
- a Single-Factor Cryptographic Software as defined in NIST 800-63B;
- a Single-Factor Cryptographic Device as defined in NIST 800-63B;
- a full Multi-Factor OTP Device as defined in NIST 800-63B;
- a full Multi-Factor Cryptographic Software as defined in NIST 800-63B; or
- a full Multi-Factor Cryptographic Device as defined in NIST 800-63B.

Multi-Factor Authentication of Subjects MUST be performed using a full Multi-Factor (as defined above) or using a memorised secret (or an inherent authentication factor) in combination with either

- a Single-Factor OTP Device as defined in NIST 800-63B;
- a Single-Factor Cryptographic Software as defined in NIST 800-63B; or
- a Single-Factor Cryptographic Device as defined in NIST 800-63B.

All factors used to perform a combined Multi-Factor authentication MUST be independent.

A Subject MAY have more than one valid set of credentials, e.g. a memorised secret and one or more Single-Factor Cryptographic Devices.

Guidance 1: *Inherent authentication factors include biometric and behaviour associated with the Subject. Note that inherent authentication factors are usually considered sensitive data as defined in the General Data Protection Regulation* (EU 2016/679).

Guidance 2: *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. Member organisations are encouraged not to implement new OTP solutions.

Guidance 3: *Independent factors means that access to one factor does not by itself grant access to other factors. For example, a FIDO security key used in combination with a password may not by itself be used to perform a reset of the password.*

Guidance 4: *Details on memorised secrets and a template password policy is available in the SWAMID Wiki.*

Guidance 5*: For more information regarding the zxcvbn password strength definition see https://www.usenix.org/system/files/conference/usenixsecurity16/sec16_paper_wheeler.pdf*

Guidance 6: *By only using other credential types than memorised secrets it is possible to implement "passwordless" authentication.*

Guidance 7: *Multi-Factor Authentication support is optional.*

5.1.2 All protocols used MUST be protected against message replay.

Guidance: *ALL SWAMID technology profiles fulfil this requirement.*

5.1.3 Subjects MUST be actively discouraged from sharing credentials with other subjects either by using technical controls or by requiring users to confirm policy forbidding sharing of credentials or acting in a way that makes stealing credentials easy.

Guidance: *A strong recommendation is that the Acceptable Use Policy or Password Policy explicitly forbids Subjects to share their credentials with other subjects or re-use their memorised secrets in other systems.*

5.1.4 The organisation MUST take into account applicable system threats and apply appropriate controls to all relevant systems.

Guidance: *Example of system threats are:*

- *the introduction of malicious code;*
- *compromised authentication arising from insider action;*
- *out-of-band attacks by other users and system operators;*
- *spoofing of system elements/applications; and*
- *malfeasance on the part of Subscribers and Subjects.*

5.2 Credential Issuing

The purpose of this subsection is to ensure that the Identity Provider has control over the issuing process including issuing of credentials and binding of other information

to the Subject. Furthermore, the Identity Provider and its Subjects must be uniquely identified.

5.2.1 Each Subject assertion MUST include a unique representation of one or more administrative domain(s) owned by the Member Organisation or which the Member Organisation has delegated usage of.

***Guidance**: Normally the DNS top level domain of the Member Organisation is used to provide scope to all scoped attributes, e.g. eduPersonPrincipalName and eduPersonScopedAffiliation.*

5.2.2 Each Identity Provider instance MUST have a globally unique identifier

***Guidance**: ALL SWAMID technology profiles fulfil this requirement, for example entityID in SAML and radius server DNS name in eduroam.*

5.2.3 Each Subject MUST be represented by one or more globally unique identifiers.

Subject identifiers MUST NOT be re-assigned.

***Guidance:** Multiple Subject identifiers (i.e. usernames) for the same Subject can be used to represent different affiliations (for example both employee and student) at the same Member Organisation.*

5.2.4 If the Subject have more than one unique identifier within the Identity Provider the Subject MUST be able to choose which one to be used at login.

5.2.5 Identity proofing MUST be done in order to issue credentials.

Credential issuing or renewed identity proofing MUST be done using one of the following methods:

1. Online authenticating the Subject at SWAMID Identity Assurance Level 2 Profile, or higher, using an Identity Provider compliant with SWAMID Identity Assurance Profiles;
2. Online authenticating the Subject at Swedish E-identification Level of Assurance 3, or higher, using an Identity Provider compliant with the Swedish E-identification System;
3. Online authenticating the Subject at eIDAS regulation (EU) No 910/2014 assurance level substantial, or higher, using an Identity Provider compliant with the eIDAS EU regulation;
4. In-person visit at a service desk in combination with identity proofing with approved forms of identification documents, as defined by the Swedish police for issuance of the Swedish passport;
5. In-person visit at a service desk in combination with identity proofing with an international passport fulfilling ICAO Doc 9303 or an EU/EES national identity card fulfilling the European Commission Regulation No 562/2006;
6. Off-line using a registered address (sv. folkbokföringsadress) in combination with a time-limited one-time 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 in combination with a time-limited one-time password/pin code sent to the postal address on the utility bill; or
8. Other equivalent identity proofing method.

During first-time and all subsequent credential issuing, any pre-registered identifiers used to identify the Subject MUST be identical to the identifiers provided by the identity proofing.

Guidance 1: *Initial adding of a second factor in a combined Multi-Factor token or a Full Multi-Factor by a Subject can be done by authenticating the Subject in the Member Organisation's own Identity Provider (item 1 above) with a username and password in combination with an Assurance Level check. After initial addition of a second factor the Subject cannot be allowed to remove or modify the second factor only by the use of username and password in order to preserve the independence of the factors involved.*

Guidance 2: *Pre-registered identifiers available by proofing method are:*

1. *Swedish Personal Identity Number or eduPersonPrincipalName*
2. *Swedish Personal Identity Number*
3. *eIDAS unique identifier or a risk assessed combination of name, date of birth and issuing country*
4. *Swedish Personal Identity Number*
5. *A combination of passport number and issuing country or a risk assessed combination of name, date of birth and issuing country*
6. *Swedish Personal Identity Number*

Guidance item 1, 2 and 3: *Single sign-on authentication must be disabled during the credential issuing process.*

5.2.6 The Member Organisation MUST maintain a record of all changes regarding Assurance Level of Subjects.

5.2.7 The Subject MUST be able to update stored self-asserted personal information.

Guidance: *This follows by the General Data Protection Regulation (EU) No 679/2016, i.e. if the Subject has provided a private email address, he/she must be able to update it.*

5.2.8 To be authorised to perform identity proofing at this Identity Assurance Profile, the Registration Authority itself MUST be using credentials at this Identity Assurance Profile or higher.

Guidance: *System administrators, personnel at helpdesks and other Registration Authorities must be proofed at this Identity Assurance Profile or higher. The recommendation is to be proofed at SWAMID Identity Assurance Level 3 Profile or higher.*

5.3 Credential Renewal and Re-issuing

The purpose of this subsection is to ensure that Subjects can change their credential and get new credentials when lost or expired.

5.3.1 All Subjects MUST be allowed to renew their credentials.

5.3.2 Subjects MUST actively demonstrate possession of current credentials in the process of credential renewal.

Guidance: *Single sign-on authentication should be disabled during the credential renewal process.*

5.3.3 Credential Re-issuing MUST be done using one of the following methods:

1. One of the methods 1-4 or 6 in 5.2.5 with pre-registered identifiers;
2. One of the methods 5 or 7 in 5.2.5 with assurance that it is the same Subject;
3. A combination of two time-limited one-time passwords/pin codes sent using two pre-registered, verified and independent channels; or
4. Other equivalent identity proofing method with assurance that it is the same Subject.

Guidance item 2: *To minimise the risk of identity fraud for Subjects with no Swedish Personal Identity Number it is necessary that the identity proofing can be linked to the previous identity proofing. This can be accomplished using for example a passport with the same passport number and issuing country or a passport with the same name, date of birth and issuing country with risk assessment that it is the same Subject.*

Guidance item 3: *Can for example be an activation link by email and a PIN code sent by SMS, where the email address and mobile phone number have been verified in advance using SWAMID AL2, or higher, credentials by the Subject.*

5.4 Credential Revocation

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

5.4.1 The Member Organisation MUST be able to revoke a Subject's credentials either by request by the Subject or by decision from the Member Organisation.

Guidance: *Possible reasons for revocation can be, for example, by request of the Subject, Subject leaving the Member Organisation or security related incidents.*

5.4.2 Credential Issuing after Credential Revocation MUST be done using one of the following methods:

1. One of the methods 1-4 or 6 in 5.2.5 with pre-registered identifiers;
2. One of the methods 5 or 7 in 5.2.5 with assurance that it is the same Subject; or

3. Other equivalent identity proofing method with assurance that it is the same Subject.

Prior to Credential Issuing after Credential Revocation caused by a security related incident, the Member Organisation MUST inform the Subject of the reason behind the revocation.

Guidance item 2: *To minimise the risk of identity fraud for Subjects with no Swedish Personal Identity Number it is necessary that the identity proofing can be linked to the previous identity proofing. This can be accomplished using for example a passport with the same passport number and issuing country or a passport with the same name, date of birth and issuing country with risk assessment that it is the same Subject.*

5.4.3 In the event of a Credential Revocation caused by a security related incident the Member Organisation MUST take precautions to prevent the incident from reoccurring.

5.5 Credential Status Management

The purpose of this subsection is to ensure that credentials are stored accordingly and that Identity Management systems have a high degree of availability.

5.5.1 The Member Organisation MUST maintain a record of all credentials issued.

Guidance: *All changes, such as password changes and/or new/closed credentials shall be stored in accordance with Swedish legislation.*

5.5.2 The Identity Provider MUST have an availability that allows the Member Organisation to use it for internal systems.

5.6 Credential Validation/Authentication

The purpose of this subsection is to ensure that the implemented Validation/Authentication processes meet proper technical standards.

5.6.1 The Identity Provider MUST provide validation of credentials to a Relying Party using a protocol that:

1. requires authentication of the specified service or of the validation source;
2. ensures the integrity of the authentication assertion;
3. protects assertions against manufacture, modification and substitution, and secondary authenticators from manufacture;
   and which, specifically:
4. creates assertions which are specific to a single transaction;
5. where assertion references are used, generates a new reference whenever a new assertion is created;
6. when an assertion is provided indirectly, either signs the assertion or sends it via a protected channel, using a strong binding mechanism between the secondary authenticator and the referenced assertion; and

7. requires the secondary authenticator to:
    1. be signed when provided directly to Relying Party, or;
    2. have a minimum of 64 bits of entropy when provision is indirect (i.e. through the credential user).

***Guidance**: ALL SWAMID technology profiles fulfil this requirement when implemented as recommended by SWAMID Operations.*

5.6.2 The Identity Provider MUST not authenticate credentials that have been revoked.

***Guidance**: Only active accounts shall be authenticated, i.e. don't authenticate revoked or closed accounts.*

5.6.3 The Identity Provider MUST force the Subject to demonstrate possession of current credentials in the process of authentication.

5.6.4 The Identity Provider MUST force the Subject to authenticate at least once every 12 hours in order to maintain an active session.

***Guidance**: This means that Single Sign-On sessions must not be valid for more than 12 hours. This balances user experience against security risks.*

6. Conformity, Syntax and Technical representation

Authentication at this Identity Assurance Profile MUST NOT be asserted unless the following criteria are met:

- the Member Organisation is approved at this Identity Assurance Profile, or higher, by the SWAMID Board of Trustees;
- the Subject has been identity proofed at this Identity Assurance Profile, or higher; and
- all Credentials used during the authentication are issued at this Identity Assurance Profile, or higher.

A Subject fulfilling this Identity Assurance Profile also fulfils SWAMID Identity Assurance Level 1 Profile. The Identity Provider SHOULD assert SWAMID Identity Assurance Level 1 Profile compliance when asserting SWAMID Identity Assurance Level 2 Profile compliance for Subjects.

Syntax and Technical representation of conformity with this Identity Assurance Profile are defined in the SWAMID Technology Profiles.