



Document	SWAMID Identity Assurance Level 2 Profile
Identifier	http://www.swamid.se/policy/assurance/al2
Version	V1.0
Last modified	2015-12-02
Pages	11
Status	FINAL
License	Creative Commons BY-SA 3.0

SWAMID Identity Assurance Level 2 Profile

1. Terminology and Typographical Conventions	2
1.1. Definition of terminology	2
2. Purpose, Scope and Summary	3
3. Compliance and Audit	3
4. Organisational Requirement	4
4.1 Enterprise and Service Maturity	4
4.2 Notices and User Information	4
4.3 Secure Communications	5
4.4 Security-relevant Event (Audit) Records	6
5. Operational Requirements	6
5.1 Credential Operating Environment	6
5.2 Credential Issuing	7
5.3 Credential Renewal and Re-issuing	8
5.4 Credential Revocation	9
5.5 Credential Status Management	9
5.6 Credential Validation/Authentication	10
6. Technical representation	11

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 is 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 and SWAMID Identity Assurance Level 1.

SWAMID has multiple assurance levels. All assurance profiles share the same numbering scheme.

1.1. Definition of terminology

Home Organisation: The SWAMID Member Organisation with which an 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 affiliated with a Home 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 called a Service Provider (SP).

Shared secret: A piece of information that is shared exclusively between the parties involved in a secure communication. The shared secret can be a password, a passphrase, a big number or an array of randomly chosen bytes.

Credential: A piece of information which the Subject use to authenticate with (aka. login). The credential can be for example a password, a passphrase, a one time password device or a certificate.

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 Swedish Academic Identity Assurance Level 2 profile (SWAMID AL2). This profile is an extension of the SWAMID AL1 profile and is optional for all SWAMID federation members. A member can choose to enable this profile for some or all of its users. Please note that some Relying Parties may have this as a requirement for their services.

This identity assurance profile does not represent Assurance Level 2 (AL2) in the sense of Kantara Initiative Identity Assurance Framework: Service Assessment Criteria (Kantara IAF-1400-SAC).

This identity assurance profile does not represent Level of Assurance 2 (LoA2) in the sense of NIST Electronic Authentication Guideline (NIST SP 800-63).

A claim at this level of assurance implies roughly the following:

- The subject is affiliated with the SWAMID member.
- The subject is an identified and confirmed individual.
- The subject is identified by a unique permanent user identifier.
- The SWAMID member is responsible for the attributes/information released.

Some relying parties in SWAMID may require supplemental credentials such as multi factor authentication for access to (parts of) the service.

***Guidance:** This assurance profile is expected to be used when the information protected is related to individual information, such as student documentation in Ladok or similar.*

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 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.

***Guidance:** SWAMID operations supplies a template for the Identity Management Practice Statement. All parts of the template **MUST** be reflected in the member's submitted Identity Management Practice Statement.*

3.3 SWAMID Board of Trustees **MAY** impose an external audit performed by SWAMID Operations in special cases.

***Guidance:** This type of audit is normally conducted after a security incident.*

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** make 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 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 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 Swedish Personal Data Act (sv. Personuppgiftslagen, SFS 1998:204).

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.

Guidance: *A suggested way to fulfil this requirement is to display and require acceptance of the Acceptable Use Policy from the Subject after it has been 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: *There should be documented procedures for life cycle management of administrative accounts. Access should be limited to as few individuals as possible.*

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 5 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), and retain such records 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 unauthorized 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 Passwords **MUST** contain at least 24 bits of entropy as defined in NIST SP 800-63-2, Appendix A. If other authentication methods are used, they must be at least equivalent in strength.

Guidance: *SWAMIDs STRONG recommendation is to use complex passwords of at least 8 characters in length. This gives at least 24 bits of entropy. More details and a template password policy (including rate limiting) is available in the SWAMID Wiki. Other authentication mechanism could be smartcards, hardware tokens that replaces passwords.*

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.

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:*

1. *the introduction of malicious code;*
2. *compromised authentication arising from insider action;*
3. *out-of-band attacks by other users and system operators;*
4. *spoofing of system elements/applications;*
5. *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. All relying parties have a need to uniquely identify the Identity Provider and the Identities provided by that Identity Provider.

5.2.1 Each Subject assertion **MUST** include a unique representation of the administrative domain associated with the Identity Provider including a unique identifier of the member organisation.

Guidance: *Normally the administrative top level domain of member organisation is used.*

5.2.2 Each Identity Provider instance **MUST** have a globally unique identifier

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

5.2.3 Each Subject identity **MUST** be represented by an identifier ("username") which **MUST** be unique for the Identity Provider.

Guidance: *Subject unique identifiers SHOULD not be re-assigned unless the unique identifier is known to be unused by all relying parties.*

5.2.4 If the Subject has more than one set of unique identifier within the Identity Provider (e g a student identifier and an employee identifier) the Subject **MUST** be able to choose what set shall be used at login.

5.2.5 Subject enrolment **MUST** be done using one of the following methods:

1. On-line authenticating the Subject at SWAMID Assurance Level 2 or higher level using an external Identity Provider compliant with SWAMID Assurance Level 2 or higher
2. 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
3. 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

4. Off-line using a registered address (sv. folkbokföringsadress) in combination with a time-limited one time password/pin code,
5. Off-line using a copy of the same identification token as described in 2 or 3 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
6. Other equivalent identity proofing method

Guidance item 2: *The Swedish Tax Agency has published a guideline “Godkända id-handlingar när du ansöker om id-kort” on identity proofing on new identity cards (<http://www.skatteverket.se/privat/folkbokforing/idkort/villkorforattfaansokaomidkort/godkandaidhandlingar.html>).*

Guidance item 3: *Driving licenses within EU/EES issued 2013 and later fulfil the directive.*

Guidance items 4 & 5: *Time-limited one time passwords/pins should be valid only as long as needed. By copy means either a scanned, photo of or hardcopy of the identity card/passport.*

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 Swedish Personal Data Act (sv. Personuppgiftslagen, SFS 1998:204).*

5.2.8 The Registration Authority performing the identity proofing needed to verify SWAMID Assurance Level 2 compliance MUST be authorized to perform identity proofing at SWAMID Assurance Level 2 or higher. To be authorized to perform identity proofing at SWAMID Assurance Level 2, the Registration Authority itself MUST be using credentials at SWAMID Assurance Level 2 or higher.

Guidance: *Both systems and system administrators, personal at helpdesks and other Registration Authorities must use at least AL2-credentials when working with other AL2-credentials. The recommendation is to use at least 2-factor.*

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.

5.3.1 All Subjects MUST be allowed to change their credentials while applying best practice with regards to credentials management (e.g. password reset and quality policies).

Guidance: *For example, use of Active Directory password policy fulfils this section.*

5.3.2 Subjects **MUST** demonstrate possession of current credentials before allowing the credential to be renewed.

*Guidance: Ask and verify the user's current password before allowing it to be changed. Remember to disable SSO for the **account management** application.*

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

1. Any of the methods in 5.2.5
2. Two separate channels in combination. The channels **MUST** be verified in advance using AL2 credentials by the Subject
3. A pre-linked account from another external Identity Provider compliant with SWAMID Assurance Level 2 or higher

***Guidance 2:** Two separate channels can for example be an activation link by email and a PIN code by SMS.*

***Guidance 3:** Account linking can be used during password reset of Subjects using a pre-linked account at an external Identity Provider compliant with SWAMID Assurance Level 2 or higher where no common unique identifier, such as a Swedish Personal Identity Number (sv. personnummer), is shared.*

5.3.4 The member organisation **MUST** be able to force a renewal of a Subject's Credential.

***Guidance:** An organisation must be able to force a user to change password.*

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.

5.4.2 For Credential Re-issuing after Revocation, the member organisation **MUST** use one of the methods in 5.2.5.

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 member organisation's Identity Management system **MUST** have a minimum of 95% availability.

Guidance: *This paragraph is to give Relying Parties a minimum level of expected uptime from the Identity Provider when the Relying Party can perform a authentication request. Numbers based on annual basis.*

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;
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 use an authentication protocol that requires the claimant to prove possession and control of the authentication token.

Guidance: *Any authentication protocols used when authenticating subjects MUST require a proof-of-possession step for subject credentials. For regular passwords this involves validating that the user knows his/her password.*

5.6.4 The Identity Provider MUST generate assertions so as to indicate and effect their expiration within:

1. 12 hours after their creation, where the service shares a common Internet domain with the Relying Party;
2. five minutes after their creation, where the service does not share a common Internet domain with the Relying Party.

Guidance: *This means that Single Sign-On sessions can only be valid for a maximum of 12 hours and an assertion request can only be valid for five minutes before usage.*

6. Technical representation

For all technology profiles compliance with this identity assurance profile is equivalent with the existence of a valid identity provider issuing valid identity claims, specifically:

Technology Profile	Representation of http://www.swamid.se/policy/assurance/al2	Representation of the administrative domain
SAML WebSSO	The existence of a SAML IdP in published SAML metadata	Shibboleth scope