

SWAMID Basic Identity Assurance Profile v1.0



Document	SWAMID Basic Identity Assurance Profile v1.0
Editor	Leif Johansson Torbjörn Wiberg Valter Nordh Mikael Berglund Pål Axelsson
Identifier	urn:mace:swami.se:swamid:assurance:basic
Version	1.0
Last Modified	2010-08-24
Status	FINAL
License	Creative Commons BY-SA 3.0

- [Terminology](#)
- [Purpose and Scope](#)
- [Compliance and Audit](#)
- [Requirements](#)
 - [Organisation](#)
 - [Identity proofing and registration](#)
 - [Credentials Issuance and Technology](#)
 - [Security and Management of Authentication Events](#)
 - [Identity Assertion Content](#)
 - [Technical Operational Environment](#)
- [Technical representation](#)

Terminology

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](#).

Purpose and Scope

This document defines the lowest common level of assurance required for all members of the Swedish Academic Identity (SWAMID) Federation. This identity assurance profile does not represent LoA 1 in the sense of NIST SP 800-63, but should rather be thought of as an 'unspecified' LoA.

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

- The subject is probably affiliated with the SWAMID member
- The subject is very likely a human and not a robot or piece of software
- The subject is most likely identified by a unique permanent user identifier

Relying parties in SWAMID may require elevated levels of assurance.

Compliance and Audit

Evidence of compliance with this profile MUST be part of the Identity Management Practice Statement, maintained as a part of the SWAMID membership process. No audits are required for this identity assurance profile.

Requirements

Organisation

- The organisation operating the identity provider **MUST** be a part of the SWAMID member organisation or under contract with the SWAMID member organisation.

Identity proofing and registration

- All subjects **MUST** at least with some degree of certainty represent a physical person affiliated with the SWAMID member organisation. Using CAPTCHAs or relying on an identity proofing process that uses CAPTCHAs (or a technical control of comparable reliability) is a minimally acceptable way of establishing 'humanness' with a sufficient degree of certainty for this assurance profile.

Credentials Issuance and Technology

- Each subject **MUST** be represented by an identifier ("username") which **MUST** be unique for the Identity Provider.
- Subject unique identifiers **SHOULD** not be re-assigned unless the unique identifier is known to be unused by all relying parties.
- If subjects are allowed access to self-service reset of credentials then either another trusted credential or a one-time password **MUST** be used.
- 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.
- Measures **MUST** be taken to reducing the vulnerability of credentials to password guessing attacks.
- 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 and **MUST** be changed at least every 3 years.

Security and Management of Authentication Events

- Secrets, credentials or long-term keys used in authentication (for instance when authenticating to an Identity Provider) **MUST** be encrypted if transmitted across open networks (eg. the Internet or Campus networks).
- 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 her/his password.
- Any session tokens **MUST** be cryptographically authenticated.
- Authentication mechanisms **MUST** be protected against common attacks such as man-in-the-middle attacks, eaves-dropper attacks and off-line password guessing.

Identity Assertion Content

- Each claim **MUST** contain a permanent identifier of the subject. This identifier **MAY** be specific to a singly relying party (a so called targeted identifier) or a shared common identifier.
- Each identity claim **MUST** include a unique representation of the administrative domain associated with the Identity Provider. This identifier **MUST NOT** be used unless it has been assigned to the Identity Provider by the SWAMID Operations Team.

Technical Operational Environment

- The servers and other infrastructure involved in the operation of identity providers or relying parties **MUST** be maintained according to best practice.

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 urn:mace:swami.se:swamid:assurance:basic	Representation of the administrative domain
eduroam	The existence of an IdP radius server validating authentication requests	Radius realmname
SAML WebSSO	The existence of a SAML IdP in published SAML metadata	Shibboleth scope