SWAMID

SWAMID Identity Assurance Level 1 Profile

SWAMID Identity Assurance Level

- SWAMID Identity Assurance Level 1 Profile är SWAMIDs nya obligatoriska basprofil
  - SWAMID BoT har beslutat att SWAMID AL1 ersätter nuvarande basprofil från och med december 2014
- SWAMID Identity Assurance Level 2 Profile kommer att vara en frivillig utökad profil
  - SWAMID AL2 kommer att färdigställas under våren 2014
  - Vissa tjänster kommer att kräva SWAMID AL2
- AL-nivå signaleras vid attributöverföringen

Vad är då SWAMID AL1?

- SWAMIDs nya basprofil bygger på Kantara AL1 och är verifierad att den håller samma nivå av kantaraauktoriserad IT-revisor.
- SWAMID AL1 är uppdelad i olika delar:
  - Organisationella krav
  - Användarregler och strukturerad tjänstebeskrivning
  - Identitetshantering (motsv. obekräftad användare)
  - Lösenord
  - Tekniska krav
  - Revision

Organisationella krav

- **4.1 Enterprise and Service Maturity**
- **4.1.1** The member organisation MUST have a Swedish Company Registration Number (e g be a legal entity in Sweden, sv. Organisations-nummer 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.* *(ej klar!)*

Organisationella krav

- **4.1 Enterprise and Service Maturity**
- **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.*

Användarregler och strukturerad tjänstebeskrivning

- **4.2 Notices and User Information**
- **4.2.1** Each member organisation MUST publish the Acceptable Use Policy to all Subjects including any and all additional terms and conditions.
  - Exempel på användarregler finns i wikin (https://wiki.swamid.se/display/SWAMID/SWAMID+template+Acceptable+Use+Policy)
- **4.2.2** All Subjects MUST indicate acceptance of the Acceptable Use Policy before use of the Identity Provider.

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

Användarregler och strukturerad tjänstebeskrivning

- **4.2 Notices and User Information**
- **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 fulfill 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.

- I SWAMID AL2 kommer krav på att användarna periodiskt, t.ex. vartannat år, godkänner reglerna.

Användarregler och strukturerad tjänstebeskrivning

- **5.1 Credential Operating Environment**
- **5.1.4** 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.

Användarregler och strukturerad tjänstebeskrivning

- **4.2 Notices and User Information**
- **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.* *(ej klar!)*

Identitetshantering

- **5.2 Credential Issuing**
- **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.*

Identitetshantering

- **5.2 Credential Issuing**
- **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 have more than one set of unique identifiers 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.

Identitetshantering

- **5.2 Credential Issuing**
- 5.2.5 Subject enrolment MUST be done using one of the following methods:
  1. On-line using an e-mail with an one time password/pin code in combination with an on-line CAPTCHA or equal;
  2. On-line authenticating the Subject at Assurance Level 1 or higher level using an external Identity Provider;
  3. In-person visit at a service desk, or equivalent, or

     Guidance: *Note the following: for this Assurance Level no identity verification is formally required, however SWAMID strongly recommends that when in-person visit is used, a verification of valid and legal identity documents is performed and a record of this is maintained in the Identity Management System.*
  4. Off-line using a postal mail with an one time password/pin code in combination with an on-line CAPTCHA or equal.

Identitetshantering

- **5.2 Credential Issuing**
- **5.2.6** In case of failure of remote verification (i.e. using 1 or 2 above) or in-person verification (i.e. using 3 above) Subjects MUST be allowed an off-line verification (i.e. using 4 above) as a fallback option.
- **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).*

Lösenord

- **5.1 Credential Operating Environment**
- **5.1.1** Passwords MUST contain at least 10 bits of entropy as defined in NIST SP 800-63-2, Appendix A

  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 (https://wiki.swamid.se/display/SWAMID/SWAMID+ template+Password+Policy).*

Lösenord

- **5.2 Credential Issuing**
- **5.2.8** It MUST NOT be possible to assign a credential to an identity that has not passed a minimum of Assurance Level 1 verification.

  Guidance: *If the Credential Management component (e.g. password database) is separated from the identity verification component then careful use of service to service authentication and access control is required. For instance, consider an Active Directory back end with an web based enrolment. In order to fulfil this requirement it is sufficient that the web interface uses a service user in the Active Directory Account Operator group.*

Lösenord

- **5.3 Credential Renewal and Re-issuing**
- **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 fulfills 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 changing password application.

Lösenord

- **5.3 Credential Renewal and Re-issuing**
- **5.3.3** For Credential Re-issuing the same methods apply as in 5.2.5.
  - 5.2.5 Subject enrolment MUST be done using one of the following methods:
    1. On-line using an e-mail with an one time password/pin code in combination with an on-line CAPTCHA or equal;
    2. On-line authenticating the Subject at Assurance Level 1 or higher level using an external Identity Provider;
    3. In-person visit at a service desk, or equivalent, or
    4. Off-line using a postal mail with an one time password/pin code in combination with an on-line CAPTCHA or equal.
- Uppdatering av SWAMID AL1 kommer troligtvis framöver tillåta lösenordsåterställning med SMS till förregistrerad mobil och förregistrerad e-postadress i samverkan.

Lösenord

- **5.5 Credential Status Management**
- **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.*

Tekniska krav

- **4.3 Secure Communications**
- **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.*

Tekniska krav

- **4.3 Secure Communications**
- **4.3.3** All network communication between systems related to Identity or Credential management MUST be encrypted.

  Guidance: *For example the communication between the Identity Provider and a LDAP server must be encrypted via ldaps.*

- **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*

Tekniska krav

- **5.1 Credential Operating Environment**
- **5.1.2** All protocols used MUST be protected against message replay

  Guidance: *ALL SWAMID technology profiles fulfil this requirement.*
- **5.1.3** All network communication between systems related to Identity or Credential management MUST be secured and encrypted.

  Guidance: *Always use TLS/SSL or similar for establishing encrypted communications between endpoints. Clients and servers needs to be mutually authenticated. An example of clients can be the webpage for changing passwords and the server can be the Identity management back-end (e.g. AD).*

Tekniska krav

- **5.1 Credential Operating Environment**
- **5.1.5** 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.*

Tekniska krav

- **5.4 Credential Revocation**
- **5.4.1** All network communication between systems related to Identity or Credential management MUST be secured and encrypted.

  Guidance: *Always use TLS/SSL or similar for establishing encrypted communications between endpoints. Clients and servers need to be mutually authenticated. An example of clients can be the webpage for account locking for service desks, or equivalent, and the server can be the Identity management back-end (e.g. Active Directory).*

Tekniska krav

- **5.5 Credential Status Management**
- **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**
- **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.*

Tekniska krav

- **5.6 Credential Validation/Authentication**
- **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;

  …

Tekniska krav

- **5.6 Credential Validation/Authentication**
- **5.6.1** The Identity Provider MUST provide validation of credentials to a Relying Party using a protocol that:

  ...

  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 fulfill this requirement when implemented as recommended by SWAMID Operations.*

Tekniska krav

- **5.6 Credential Validation/Authentication**
- **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.*

Tekniska krav

- **5.6 Credential Validation/Authentication**
- **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.*

Revision

- **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.

Revision

- **3. Compliance and Audit**
- **3.2** The member organisation MUST audit the effective provision of the Identity Provider and the underlying systems at least once every 12 months by internal audit or by information security functions of the member organisation. Special considerations to the evidence of compliance with this profile MUST be done by the member organisation. The part of the audit that describes the evidence of compliance with this profile MUST be submitted to SWAMID Operations. …

Revision

- **3. Compliance and Audit**
- **3.2** …SWAMID operations conduct an audit of the submitted Identity Management Practice Statement based on the member organisation self-audit.

  Guidance: *If the information security functions is used for the audit it has to be independent from the internal organisation that develops and operates the Identity Provider and the underlying systems. The self-audit document must be sent to SWAMID Operations via the operations mail address directly after the annual self-audit.*

Revision

- **3. Compliance and Audit**
- **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.*
- **3.4** The member organisation MUST retain records (sv. diarieföras) of all audits, both internal and independent, for a period which, as a minimum, fulfils its legal obligations and otherwise for greater periods required by any obligations it has with/to Subjects, and which in any event is not less than 36 months. Such records MUST be held securely and be protected against unauthorized access, loss, alteration, public disclosure, or unapproved destruction.

Slutord

- SWAMID Identity Assurance Level 1 Profile är SWAMIDs obligatoriska basprofil från och med ***december 2014***
- Införandet kommer att kräva förändringar i de flesta lärosätenas identitetshanteringsprocesser
- Införandet kan komma kräva förändringar i de flesta lärosätenas konfiguration av identitetshanteringssystem, t.ex. Active Directory
- ***BÖRJA I GOD TID!!!***