Sunet dagarna

Hur effektiviseras och förtydligas SWAMIDs tillitsprofiler?

SWAMID

SWAMID har tagit fram ett diskussionsunderlag för att uppdatera SWAMIDs tillitsprofiler. Avsikten med uppdateringarna är inte att höja nivån på SWAMIDs tillitsprofiler, utan att om möjligt förenkla och göra dem mer tydliga.

Uppdatering av SWAMIDs regelverk

- Vid uppdatering av SWAMIDs regelverk används alltid SWAMID Community Consultations Process
- SWAMID Operations har tagit fram ett förslag
- Aktuella förslag på uppdaterade tillitsprofiler finns publicerade på wikisidan Översyn av SWAMIDs tillitsprofiler 2024
    - Text som är överstruken gul är ändrad
    - Genomstruken text är borttagen och eventuellt ersatt med efterföljande text
    - Grön text är skillnad mot underliggande tillitsprofil
- Konsultationsprocessen pågår fram till 29 november
- Fråge- och diskussionsmöten 11, 21 och 27 november
- Kommentarer skickas till operations@swamid.se

SWAMID Identity Assurance Level 1 Profile

A claim at this Identity Assurance Profile implies the following:

- the subject is a natural person;
- the subject is affiliated with the Member Organisation;
- the subject can be contacted by the Member Organisation;
- the subject is identified by a unique permanent user identifier; and
- attributes/information released may be self-asserted.

SWAMID Identity Assurance Level 2 Profile

A claim at this Identity Assurance Profile implies the following:

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

SWAMID Identity Assurance Level 3 Profile

A claim at this Identity Assurance Profile implies the following:

- the subject is an identified and confirmed natural person;
- the subject is affiliated with the Member Organisation;
- the subject can be contacted by the Member Organisation;
- the subject is identified by a unique permanent user identifier;
- the Member Organisation is responsible for the attributes/information released; and
- the authentication of the subject ~~was~~ is a multi-factor authentication

4.2 Notices and User Information

- 4.2.1 ~~Each~~ The Member Organisation MUST maintain and publish the Acceptable Use Policy to all Subjects including any and all additional terms and conditions.
- ~~4.2.3 All Subjects MUST indicate renewed acceptance of the Acceptable Use Policy if the Acceptable Use Policy is modified.~~
- 4.2.3 All Subjects MUST either indicate renewed acceptance or be actively informed of any modifications to the Acceptable Use Policy.
- ~~4.2.5 Each Member Organisation MUST publish the identity provider Service Definition. The Service Definition MUST at least include:~~
- 4.2.5 The Member Organisation MUST maintain and publish the Identity Provider’s Service Definition. The Service Definition MUST be accessible online without requiring authentication. The Service Definition MUST at least include:

4.4 Security-relevant Event (Audit) Records

- Avsnittet var tomt under SWAMID AL1 men är nu samma som för SWAMID AL2 och SWAMID AL3, dvs. endast förändring i SWAMID AL1
- Denna förändring är nödvändig för att uppfylla kraven SWAMIDs incidenthanteringsprocess
- 4.4.1 The Member Organisation SHOULD 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 SHOULD be retained with appropriate protection and controls to ensure successful retrieval, accounting for service definition, risk management requirements, applicable legislation, and organisational policy.

4.5 Incident Management

- Ny punkt i samtliga tillitsprofiler men exakt samma krav finns redan i aktuell teknologiprofil för SAML WebSSO
- 4.5.1 The Member Organisation MUST follow the SWAMID Incident Management Procedure in case of a suspected security incident if
  - the Identity Provider is at risk; or
  - at least one user with federated logins is at risk or involved.

5.1 Credential Operating Environment

- Under 5.1.1 definieras när rullande engångskod med OTP inte längre får användas inom SWAMID som andra faktor.
- Förändringen finns inskriven i aktuella beslutade tillitsnivåer som vägledning
- a full Multi-Factor OTP Device as defined in NIST 800-63B;
  - Use of full Multi-Factor OTP Devices will no longer be compliant with this profile after 2027.
- a Single-Factor OTP Device as defined in NIST 800-63B;
  - Use of software-based Single-Factor OTP Devices will no longer be compliant with this profile after 2025.
  - Use of hardware Single-Factor OTP Devices will no longer be compliant with this profile after 2027.

5.1 Credential Operating Environment

- Under 5.1.1 har vi tydligt definierat vad multifaktorinloggning innebär
- Denna ändring är ingen höjning av nivån utan förklarande text
- Multi-Factor Authentication MUST ensure that the user authenticating is always the same Subject. This implies the following key aspects:
  - The login mechanism includes something you have combined with something you know or are;
  - The login mechanism is cryptographically secure;
  - The login mechanism cannot be transferred, duplicated, or synchronised across devices without the use of an additional knowledge-based or inherent authentication factor; and
  - The login mechanism has built-in protection against phishing and social engineering.

5.1 Credential Operating Environment

- Under 5.1.1 har vi tydliggjort vad fristående faktorer innebär
- All factors used to perform a combined Multi-Factor authentication MUST be independent; this includes processes to renew, re-issue, or add authentication factors. Initial issuance of one or more additional factors MAY take place subject to authentication by only a single factor.
- Under 5.1.1 har vi möjliggjort användning av annan identitetsutfärdare eller e-legtimation för att genomföra själva inloggningen
- To fulfil the authentication requirements outlined above, the Member Organisation MAY utilise an external authentication source. In such cases, the external authentication source MUST satisfy at least one of the methods 1-3 in section 5.2.5. Additionally, the Member Organisation's Identity Provider and the external authentication source MUST share a pre-registered identifier.

5.2 Credential Issuing

- 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. The Member Organisation's administrative domain(s) MUST be described.
- 5.2.3 Each Subject MUST be represented by one or more globally unique identifiers.

  Subject identifiers MUST NOT be re-assigned.

  The Member Organisation MUST have documented procedures and controls to ensure that Subject identifiers are not re-assigned.

5.2 Credential Issuing

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

  2. Online authenticating the Subject at Swedish E-identification ~~Level of Assurance 3~~ Level of Assurance 2, 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 amended by 2024/1183 assurance level substantial, or higher, using an Identity Provider or a European Digital Identity Wallet 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 or authenticating the Subject using method 2 above;

5.2 Credential Issuing

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

  5. In-person visit at a service desk in combination with identity proofing with ~~an international~~ a non-Swedish passport fulfilling ICAO Doc 9303 or an a non-Swedish EU/EES national identity card fulfilling the European Commission Regulation No 562/2006 or authenticating the Subject using method 3 above;

  6. Off-line using a Swedish 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 non-Swedish postal address on the utility bill;

5.2 Credential Issuing

- 5.2.6 In the process of transitioning Assurance Level of Subjects, renewed identity proofing MUST be done using one of the methods in 5.2.5 with pre-registered identifiers to ensure that it is the same Subject.

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

5.2 Credential Issuing

SWAMID AL1

- 5.2.7 Any personal identifiable information and contact details MUST be self-asserted by the Subject or managed by the Member Organisation. The Subject MUST be able to update stored self-asserted personal information.

SWAMID AL2

- 5.2.7 Personal identifiable information MUST be obtained from authoritative sources. The Member Organisation MUST be able to update personal identifiable information either by request by the Subject or by decision from the Member Organisation. Contact details MUST be self-asserted by the Subject or managed by the Member Organisation. The Subject MUST be able to update stored self-asserted personal information.

5.2 Credential Issuing

- 5.2.7 ...
  The Member Organisation MUST have means to contact all Subjects using either self-asserted contact details, contact details managed by the Member Organisation or contact details registered in the Swedish population registry (sv. folkbokföringsregistret).

  Self-asserted contact details SHOULD be verified using a time-limited one-time password/pin code and the Subject's credentials.
- 5.2.8 To be authorised to perform ~~identity proofing~~ credential issuing at this Identity Assurance Profile, the Registration Authority itself MUST be using credentials at this Identity Assurance Profile or higher.

5.3 Credential Renewal and Re-issuing

SWAMID AL1

- 5.3.3 Credential Re-issuing MUST be done using one of the following methods:
   1. ~~One of the methods 1-3 in 5.2.5 with pre-registered identifiers;~~
   2. ~~One of the methods 4 and 6 in 5.2.5 with pre-registered address information;~~
   3. ~~Method 5 in 5.2.5 with high probability that it is the same Subject; or~~
   4. ~~Other equivalent identity proofing method with high probability that it is the same Subject~~

   1. One of the methods in 5.2.5 with pre-registered identifiers to ensure that it is the same Subject;
   2. Other equivalent identity proofing method with high probability that it is the same Subject

5.3 Credential Renewal and Re-issuing

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

~~1. One of the methods 1-3 in 5.2.5 with pre-registered identifiers;~~
~~2. One of the methods 4 and 6 in 5.2.5 with pre-registered address information;~~
~~3. Method 5 in 5.2.5 with high probability that it is the same Subject; or~~
~~4. Other equivalent identity proofing method with high probability that it is the same Subject~~

1. One of the methods in 5.2.5 with pre-registered identifiers to ensure that it is the same Subject;
2. A combination of two time-limited one-time passwords/pin codes sent using two pre-registered, verified and independent channels; or *(endast I SWAMID AL2)*
3. Other equivalent identity proofing method with high probability that it is the same Subject *(finns ej i SWAMID AL3)*

SWAMID

5.4 Credential Revocation

- 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.

  The Member Organisation MUST be able to block a Subject from Credential Issuing after Credential Revocation.

  The Member Organisation MUST have documented processes to revoke Subjects’ credentials that no longer should be valid.
- 5.4.2 Credential Issuing after Credential Revocation MUST be done using one of the following methods:
  - Samma förändringar som i 5.3.3
  - Går att hänvisa till 5.3.3 när man skriver IMPS

5.5 Credential Status Management

- 5.5.1 The Member Organisation MUST maintain a record of all credentials issued. This record MUST be retained with appropriate protection and controls to ensure successful retrieval, accounting for service definition, risk management requirements, applicable legislation, and organisational policy.

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; and
  - 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.~~

Nästa steg...

Kom på SWAMIDs fråge- och diskussionsmöten 11, 21 och 27 november

Kommentera på den öppna konsultationen senast 30 november

För mer information se Översyn av SWAMIDs tillitsprofiler 2024

SWAMID

SWAMID

Swedish Academic Identity Federation