



SWAMID

Swedish Academic Identity Federation

AL2 för personer utan svenskt personnummer

SWAMID Webinar 2023-11-16

Utmaningen

Att automatiserat digitalt identifiera en person som antingen inte har svenskt personnummer eller inte är folkförd i Sverige

Utmaningen finns inte bara för studenter utan även för andra personer men här använder vi studenter som exempel

SWAMIDs regelverk runt identifisering av personer i tillitsprofilen SWAMID AL2

Regler i SWAMID AL2 för användarvalidering (5.2.5 Online)

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;

Regler i SWAMID AL2 för användarvalidering (5.2.5 In-person)

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;

Regler i SWAMID AL2 för användarvalidering (5.2.5 Off-line)

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 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
6. Other equivalent identity proofing method.

Regler i SWAMID AL2 för att veta att det är samma person (5.2.5, 5.3.3 och 5.4.2)

- **5.2.5**

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.

- **5.3.3 och 5.4.2**

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;

eduID och identifiering av användare på nivån SWAMID AL2

eduID och SWAMID AL2

- Personer med svenskt personnummer folkbokförda i Sverige
 - Freja eID Plus, mobilabonnemang eller folkbokföringsadress
 - BankID kommer att ersätta mobilabonnemang
- Personer från EU/EES med e-legitimation inom eIDAS
 - Använd nationell e-legitimation (eID) annonserad i eIDAS på minst tillitsnivå Substantial
 - Kan vara en annan e-legitimation än den som de normalt använder
- Övriga personer
 - Använd pass med ePassport (biometriskt pass) via SvipecID
 - Nationella identitetskort inom EU/EES har oftast ePassport
 - Identitetskort från andra länder kan ha ePassport



Länder med eID inom eIDAS nov 2023

- Belgien
- Danmark
- Estland
- Italien
- Kroatien
- Lettland
- Liechtenstein
- Litauen
- Luxemburg
- Malta
- Nederländerna
- Portugal
- Slovakien
- Slovenien
- Spanien
- Sverige
- Tjeckien
- Tyskland



Länder utan ePassport nov 2023



Afrika

- Kap Verde
- Egypten
- Eritrea
- Eswatini
- Etiopien
- Mauritius
- Sydafrika
- Tunisien
- Zambia

Karibien

- Kuba
- Dominikanska republiken
- Grenada
- Haiti
- Trinidad och Tobago

Mellanamerika

- El Salvador
- Guatemala
- Honduras
- Nicaragua

Mellanöstern

- Irak
- Jemen
- Jordanien
- Palestina
- Syrien

Ostasien

- Bhutan
- Myanmar
- Nordkorea

Oceanien

- Kiribati
- Marshallöarna
- Mikronesien
- Nauru
- Palau
- Papua New Guinea
- Samoa
- Salomonöarna
- Tonga
- Tuvalu
- Vanuatu

Äldre pass från andra länder kan också sakna ePassport!

Uppgifter tillgängliga från eduID för personer bekräftade SWAMID AL2

- Användaridentitet i eduID
- Användarens tillitsnivå
- För- och efternamn från folkbokföring, eIDAS-inloggning alternativt resehandling (ePassport) via SvipecID
- Födelsedata från folkbokföring, eIDAS-inloggning alternativt ePassport via SvipecID
- Personnummer för personer med svenskt personnummer
- Registrerade och validerade e-postadresser

Hur kan man hantera utmaningen?

Förslag på lösning i korta punkter

- Utöka lärosätets kontoaktiveringsportal med stöd för personer utan svenskt personnummer
- Gör en automatiserad riskbaserad bedömning om inloggad person går att unikt koppla samman med en person i det lokala källsystemet för personer, t.ex. Ladok för studenter
- Om den automatiserade riskbedömningen misslyckades
 - Om uppgifterna från edulD nästan stämmer överens med uppgifterna från källsystemet för studenter gör en manuell riskbedömning
 - Aktiveras via kontoaktiveringsportalen, inte via direkt kontakt med supporten
 - Användaren behöver bara veta att verifiering pågår
 - Om uppgifterna inte stämmer överens, neka aktiveringen

Vad behövs för en riskbaserad bedömning?

- Jämför personuppgifterna från eduID och källsystemet för studenter
 - Födelsedata måste vara samma
 - För- och efternamn måste vara tillräckligt lika (inte fullständigt förnamn och annorlunda stavning är vanligt)
- Användaren måste vara bekräftad SWAMID AL2 i eduID
- Utökad riskbedömning: E-postadress i eduID ska vara samma som registrerad adress i källsystemet för studenter
 - Endast för att förenkla matchning av personuppgifter mellan eduID och lokalt register

Vilka uppgifter behöver lärosätet få från eduID?

Begär följande attribut från eduID med hjälp av entitetskategorin REFEDS Data Protection Code of Conduct v2:

- Subject-id och/eller eduPersonPrincipalName (*för loggning och säkerställande att det är samma individ vid återställning och återaktivering, bägge attributen har samma värde*)
- eduPersonAssurance (*för kontroll av tillitsnivå*)
- norEduPersonNin (*för matchning via personnummer*)
- schacDateOfBirth (*för riskbaserad matchning*)
- givenName (*för riskbaserad matchning*)
- sn (*för riskbaserad matchning*)
- mail och mailLocalAddress (*lista på validerade e-postadresser*)

Och till sist...

Glöm inte att uppdatera och få er Identity Management Practice Statement (IMPS) godkänd innan ni driftsätter lösningen!

Demo eduID

Frågor och funderingar?

Tack för att ni kom!

Pål Axelsson, pax@sunset.se
Zacharias Törnblom, zacharias@sunset.se



SWAMID

Swedish Academic Identity Federation