| | |
|---|---|
| **Document** | SWAMID Granskningsmöte SWAMID AL3 |
| **Version** | 1.2 |
| **Last modified** | 2022-03-22 |
| **Pages** | 3 |
| **Status** | Final |
| **License** | Creative Commons BY-SA 3.0 |

# SWAMID Granskningsmöte SWAMID AL3

| | |
|---|---|
| **Organisation:** | Örebro universitet |
| **Deltagare från granskad organisation:** | Anders Strand, Tomas Liljebergh, Tomas Larsson, Conrad Granath |
| **Deltagare SWAMID Operations:** | Fredrik Domeij, Pål Axelsson, Björn Mattsson |
| **Datum:** | 2023-11-24 |

## Kontrollfrågor vi möte med organisation

### 5.1.1 Inloggningsfaktorer

Motivera valet av multifaktorteknologi och varför denna/dessa passar bra för er organisation.

Hur byggs multifaktorn?

- Full multifaktor
- Kombinerad multifaktor
  - Lösenord + något man har
  - Något man är + något man har

Hur säkerställs att inblandade faktorer är oberoende av varandra?

**Tillsfreställande beskrivning**

***Operations guidance:*** *Det är exempelvis inte godkänt med SMS då SMS:et kan gå att avlyssna och även i vissa fall går att nå med endast användarens användarnamn och lösenord via till exempel en teleadministrationsportal.*

### 5.1.3 Skydd av inloggningsfaktorer

Vilka interna riktlinjer har ni om utdelade autentiseringsenheter?

Hur säkerställer ni att användare betraktar dessa som värdehandlingar (i likhet med lösenord) och t.ex. ej förvarar dessa åtkomliga på skrivbordet?

***Operations Guidance:*** *Frågan endast relevant för fristående andra faktorer, t.ex. USB-nycklar och OTP-enheter.*

**Tillsfreställande beskrivning**

### 5.2.5 Utdelning av multifaktor

Motivera valet av identifieringsrutiner och varför dessa passar bra för er organisation.

Frågor runt resp. utdelningsmetod:

- (1) Kontrolleras både att IdP (metadata) och användare (eduPersonAssurance) uppfyller SWAMID AL3?

- (2) Svenskt e-leg: Hur säkerställs att e-legitimationen är på LoA3-nivå, eller högre?

- (2) eIDAS: Hur kontrolleras att tillitsnivån är substantial eller högre?

  ***Operations guidance:*** *Hur sker riskbedömning vid befintligt konto att identifierad individ är samma som kontoinnehavare?*

- (4, 5) Beskriv era riktlinjer för hur er personal ska genomföra en identitetskontroll och hur ni säkerställer att identitetskontroller utförs enligt dessa riktlinjer.

  ***Operations guidance (5):*** *Hur sker riskbedömning vid befintligt konto att identifierad individ är samma som kontoinnehavare?*

  ***Operations guidance:*** *Om medlemmen inte har någon metod för AL3-identifiering med uppvisande av legitimation så behövs ingen dokumenterad rutin för hur legitimationskontroll skulle ske.*

- (6) Om ni använder folkbokföringsadress i samband med identifiering, hur säkerställer ni folkbokföringsadressen för kontoinnehavaren?

  ***Operations guidance:*** *Skillnaden mellan Skatteverkets register och söktjänster på nätet.*

**Tillsfreställande beskrivning**

### 5.2.8 SWAMID AL3 för kontoadministratörer

Beskriv hur ni säkerställer att alla administratörer som utför identifiering enligt SWAMID AL3 själv autentiserar sig enligt SWAMID AL3.

**Tillsfreställande beskrivning**

### 5.3.2 Fristående faktorer vid faktorbyte

Hur säkerställer ni fristående faktorer i samband med lösenordsbyte eller byte av andra faktor?

***Operations guidance:*** *Denna är inte aktuell om full multifaktor används.*

***Operations guidance:*** *Rimligtvis får man ersätta en faktor med en annan faktor av samma typ, men inte byta exempelvis sin Yubikey genom att bara ha sitt lösenord och tvärtom*

**Tillsfreställande beskrivning**

### 5.3.3 Förregistrerade identifierare i samband med återställning av faktorer

Vilka i förväg registrerade identifierare används för att säkerställa att det endast är korrekt individ som kan få tillgång till ett användarkonto?

**Tillsfreställande beskrivning**

### 5.4.2 Information till användaren vid spärrat konto

Vilken rutin finns för att informera användaren i samband med att ett konto spärras och hur säkerställer ni att det är rätt individ som informeras?

**Tillsfreställande beskrivning**