Document	SWAMID Granskningsmöte SWAMID AL3
Version	1.2
Last modified	2022-03-22
Pages	2
Status	Final
License	Creative Commons BY-SA 3.0

SWAMID Granskningsmöte SWAMID AL3

Organisation:	Högskolan i Borås
Deltagare från granskad organisation:	Helena Corbé, Per-Olof Axelsson, Henrik Bengtsson, Henrik Kronander
Deltagare SWAMID Operations:	Fredrik Domeij, Björn Mattsson, Pål Axelsson
Datum:	2024-12-03

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?

Använder mjukvarubaserad TOTP (Google Authenticator eller Microsoft Authenticator) och Yubikeys. De är medvetna om att de behöver byta ut TOTP mot något annat under 2025.

Ingen lösenordsåterställning via andra faktorn, och ingen möjlighet för användare att själva återställa sin andra faktor.

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?

Uppdaterat användarreglerna för att hantera både lösenord och den andra faktorn.

5.2.5 Utdelning av multifaktor

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

Legitimationskontroll. Ska ha genomgångar med personalen om hur man kontrollera en legitimation. Rutiner innefattar PRADO och polisen. Allt finns nedskrivet i rutinen.

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.

Uppfyller kraven.

5.3.2 Fristående faktorer vid faktorbyte

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

Andra faktorn kan endast bytas vid personligt besök.

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?

Studenter
Personnummer från Ladok som jämförs med identitetshandling. För studenter utan svenskt personnummer används interimspersonnummer från Ladok vid aktivering via Antagning.se, annars riskbaserad bedömning baserat på namn och födelsedata.

Anställda
Personnummer från Primula som jämförs med identitetshandling. Använder ett eget ”interimspersonnummer” för personal utan svenskt personnummer.

Ska komplettera sina lösenordsåterställningsrutiner för AL3 över disk så att det bättre beskriver hur man säkerställer att personer utan svenskt personnummer, eller som saknar svensk identitetshandling, fortfarande är samma individ. Pratar om att personens chef ska närvara som stöd i riskbaserad bedömning men det verkar inte helt definierat.

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?

Uppfyller kraven.