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:	VR-Sunet
Deltagare från granskad organisation:	Zacharias Törnblom, Pål Axelsson, Björn Mattsson
Deltagare SWAMID Operations:	Fredrik Domeij, Eskil Swahn
Datum:	2023-05-30

Kontrollfrågor vi möte med organisation

5.1.1 Inloggningsfaktorer

Motivera valet av att använda eduID för autentisering av era användare och varför detta passar bra för er organisation.

Det lät rimligt så de slipper hantera MFA själva.

5.2.5 Utdelning av multifaktor

Kommentar på IMPS: Bra med en gemensam identifierare mellan eduID och inbjudningstjänsten för Sunet IdP som anges i förväg av kontoadministratören. Dock behöver ni definiera vilken den gemensamma identifieraren är och hur ni säkerställer att den hör till avsedd individ för att vi ska bedöma om det uppfyller kraven i profilen. Den kan t ex hämtas ur ett HR-system om vi pratar anställda med svenskt personnummer alternativt fastställas genom en identitetskontroll vid ett fysiskt besök av individen i fråga.

Hur säkerställs att det är avsedd individ som aktiverar användarkonto vid Sunet?

Identifierare: Personnummer (men det kanske vi vill undvika för att kunna få in alla anställda), sannolikt verifierad e-postadress för utlämning, tidsbegränsad till en vecka.

Efter diskussioner ska det ändras till personnummer och övriga hanteras via manuell verifiering efter ansökan.

Hut sker riskbedömning när annan identifierare än personnummer används vid kontokoppling?

Manuell riskbedömning och jämförelse av födelsedata och namnuppgifter.

5.2.8 SWAMID AL3 för kontoadministratörer

Hur kontrolleras att system- och kontoadministratörer i Sunets inloggningstjänst autentiserar sig enligt SWAMID AL3.

Kontroll vid inloggning.

5.3.3 Förregistrerade identifierare i samband med återställning av faktorer

Hur hanteras förregistrerade identifierare mellan eduID och Sunets inloggningstjänst? eppn vs personnummer vs födelsedata/förnamn/efternamn

Personnummer och födelsedata/namn uppdateras med automatik vid inloggning

Hur hanteras fallet att en användare helt tappar tillgång till sitt eduID-konto? (med lite vilja går det att gissa sig till att en användare kan logga in med ett annat eduID-konto men med samma personnummer eller födelsedata/förnamn/efternamn och få sitt eppn uppdaterat).

Eppn plockas bort och en ny etablering görs då personnummer eller födelsedata/namn måste matcha.

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?

Personlig kännedom via chef osv. Eftersom organisationen är så liten så vet man vilken användaren är.