



SWAMID

Swedish Academic Identity Federation



SWAMID

Multifaktorinloggning i SWAMID

Eskil Swahn, Pål Axelsson
SWAMID Operations



SWAMID

Vägen mot säkrare inloggning

- Lösenordsinloggning är alltmer utsatt för flera olika nätbaserade hot, t.ex. lösenordsfiske och lösenordstestning
- Att ersätta lösenordet med en hårdvarunyckel, t.ex. en säkerhetsnyckel baserad på U2F eller FIDO2, ökar kraftigt skyddet mot nätbaserade hot men är sårbart för stöld
- Lösenordsinloggning tillsammans med hårdvarunyckel ökar skyddet mot både stöld och nätbaserade hot men ökar kraftigt komplexiteten för användarna



SWAMID

Vägen mot säkrare personidentifiering

- Vissa tjänster vill bara veta att det är samma person loggar in varje gång, inte vem personen är (*SWAMID AL1*)
 - Här krävs det minst att det går att kontakta användaren vid behov genom att verifiera e-post
- Vissa tjänster behöver med god sannolikhet veta att det är rätt person som loggar in (*SWAMID AL2*)
 - Här krävs det minst utskick till folkbokföringsadress för att binda kontot till användaren
- Vissa tjänster kräver med hög säkerhet att det är rätt person som loggar in (*SWAMID AL2 + utökad personidentifiering*)
 - Här krävs att kontot binds till användaren med hjälp av identitetskontroll

Tjänsten väljer nivå, inte identitetsutgivaren

	Låga krav på att det är rätt person	Normala krav på att det är rätt person	Höga krav på att det är rätt person
Normala krav på inloggning	SWAMID AL1 + en faktor*	SWAMID AL2 + en faktor**	<i>Ej lämpligt!</i>
Höga krav på inloggning	SWAMID AL1 + flera faktorer	SWAMID AL2 + flera faktorer	SWAMID AL2 + utökad person-identifiering + flera faktorer

* Lösenord eller självregistrerad hårdvarunyckel

** Lösenord eller personverifierad hårdvarunyckel



SWAMID



SWAMID

Swedish Academic Identity Federation



SWAMID

Frågor och andra funderingar

- Hur presenterar vi detta för slutanvändarna?
- Hur stor andel av användarna kommer att påverkas av detta införande?
- Är det skillnad mellan hur vi hanterar nationella IT-tjänster och lokala lärosätes-IT-tjänster?
- Vilken information är det vi på lärosätena vill skydda mest? Är det bara externa krav som styr ställningstagandet?
- Hur många tekniker behöver vi som lärosäten kunna stödja?
- Vad kännetecknar en bra teknik?



SWAMID

”Framtida” potentiella krav

- Registrering av tentamina i Ladok
- E-signering
- Känsliga personuppgifter
- Lagring av forskningsdata
- Forskningstjänster/forskningssamarbete
- Digitala Nationella Prov