eduID 2FA API

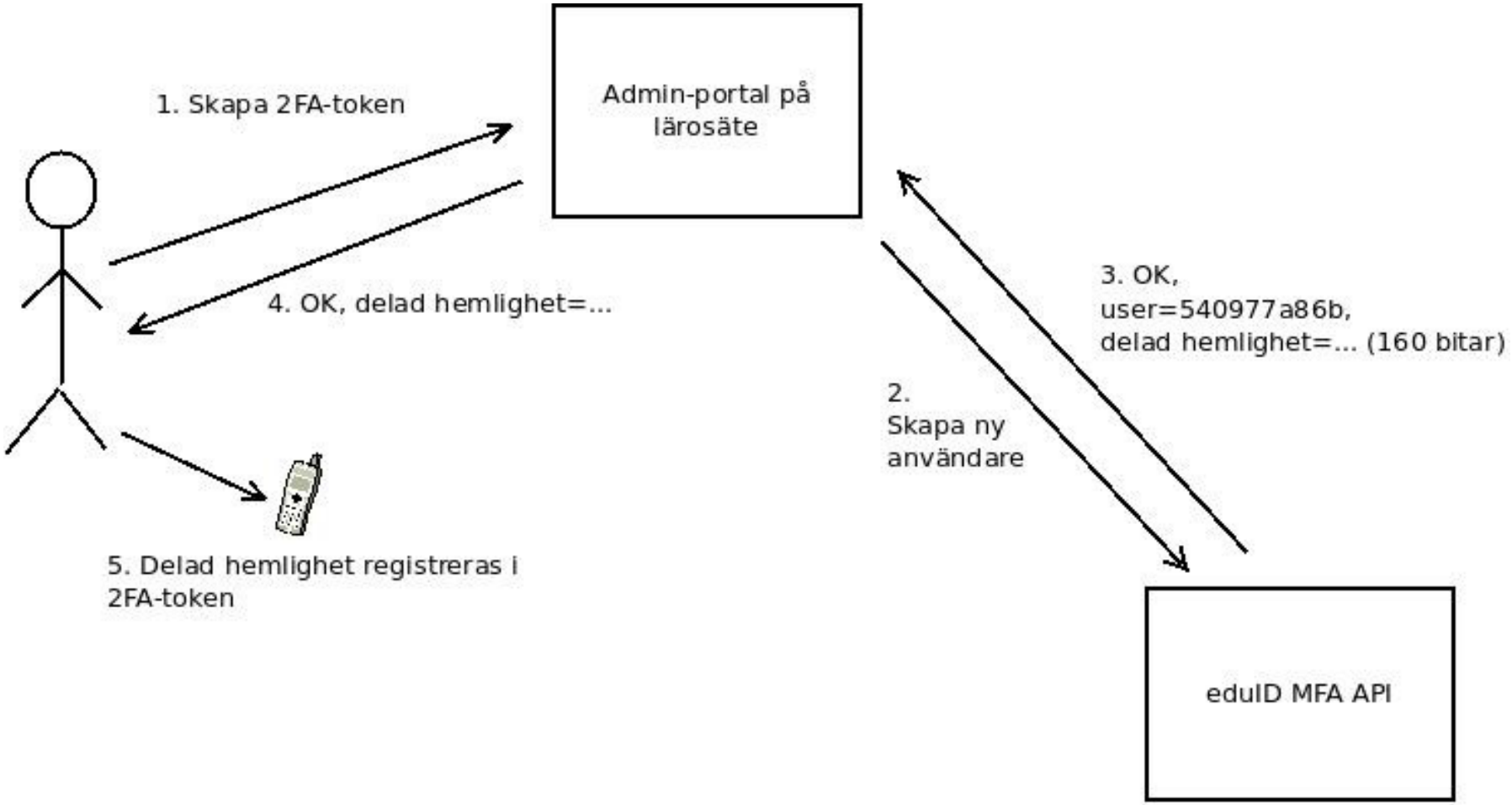
Hans Nordlöf

hanor@sunet.se

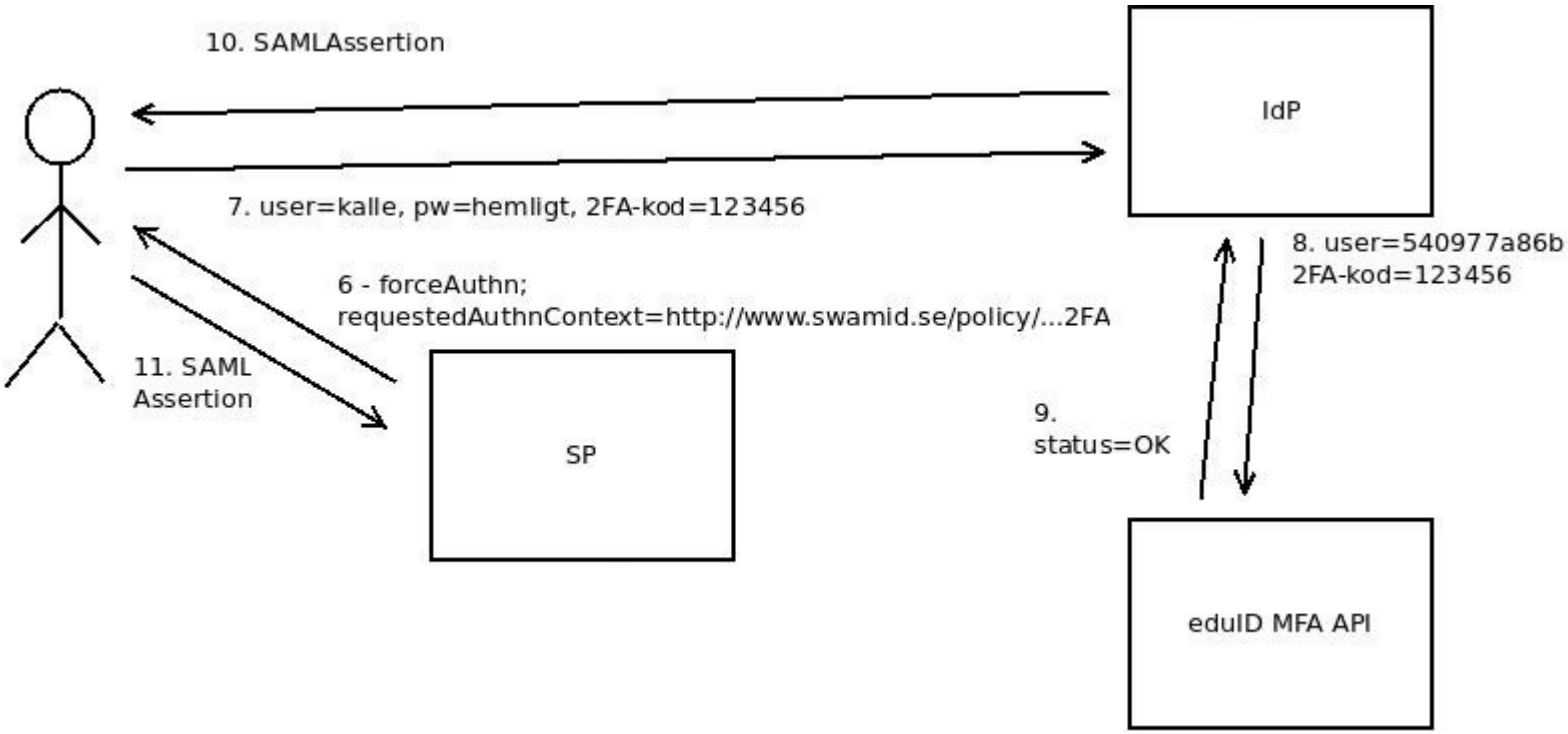
eduID 2FA API

- Ger ett lättanvänt interface för tvåfaktorsautenticering (JOSE)
- OATH TOTP HMAC-SHA-1 (sex eller åtta siffrors koder)
- Tidsbaserat, koder giltiga 30+30 sekunder
- Anonyma ”användare” skapas hos eduID
- eduID svarar JA eller NEJ baserat på uppgiven kod

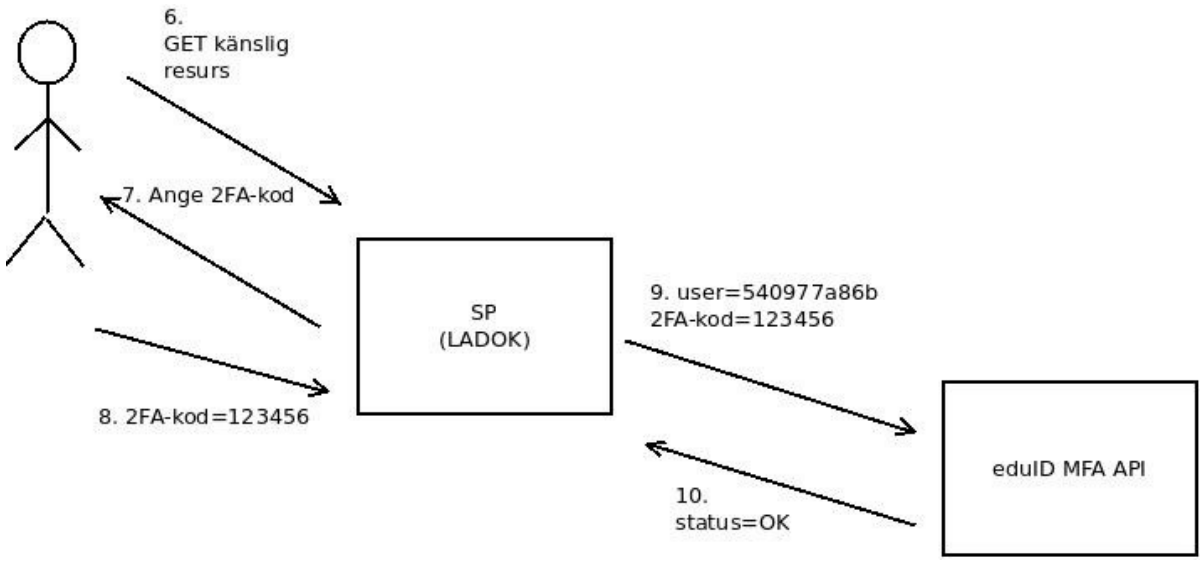
Registrera 2FA för ny användare



SP vill ha starkare autenticering via en IdP i federationen



SP vill ha starkare autenticering, använder eduID direkt



OBS: I detta fall har 2FA-användaren skapats via SP (LADOK), inte via det egna lärosätet.
För att förhindra phishing och andra säkerhetsproblem kan inte organisation A autentisiera med tokens från organisation B.

Användningsområden

	Låga krav på information om individen	Höga krav på information om individen
Normala krav på säker användning av kontot	SWAMID AL1 + lösenord	SWAMID AL2 + lösenord
Höga krav på säker på säker användning av kontot		SWAMID AL2 + MFA

Varför eduID OATH API

- Eftersom
  - Kryptering är svårt/läskigt
  - Behov på serversidan att kunna förvara hemligheter säkert
  - Kommande/befintliga system kommer att vilja ha MFA (nya LADOK ex.vis)
  - eduID kommer att själv kunna generera OTP tokens för att kunna genomföra 2FA om SP begär det (och för eduID:s supportfunktion)

U2F – liten ordlista

- **FIDO Alliance** (Fast Identity Online) bildades av bl.a. PayPal, Nok Nok Labs, Validity Sensors. Samtidigt arbetade Google, Yubico och NXP fram en andrafaktorsdongel. Resulterade i FIDOs 2 protokoll:
- Ett protokoll kallas **UAF** (Universal Authentication Framework) och handlar om singelfaktor utan lösenord (exempelvis fingeravtryck)
- **U2F** (Universal 2nd Faktor) är ett öppet protokoll för skapande av en andra faktor, som komplement till användarnamn/lösenord

U2F – generering om eduIDs API används

- SP genererar en “challenge” (utmaning) och skickar till användaren (lägger till AppID)
- Javascript för över utmaningen till U2F “token”
- “Token” skapar en ny privat nyckel, skickar klientdata och registreringsdata
- SP skickar klientdata, registreringsdata, utmaning och appID till eduID
- eduID API lägger till bl.a. eduID user, nyckelID
- eduID sparar den publika nyckeln
- SP sparar eduID user och nyckelID

U2F autentisering

- SP autentiserar användare med användarnamn och lösenord och får tillbaka U2F nyckelID och eduID username
- SP skapar en utmaning
- SP skickar utmaningen och nyckelID till U2F-klienten
- SP skickar svar plus eduID username till eduID API
- eduID API kollar signaturen med hjälp av publika nyckeln, använder eduID username, kollar räknaren och svarar med sant eller falskt

För och emot att eduID skulle ha ett API för U2F

- **För:**
  – Vi kan ge support
  – Extern verifiering – ökar säkerheten
- **Emot**:
  – SP måste göra javaskripten ändå
  – SP måste hålla register ändå
- **Säkerhet**:
  - Varken SP eller eduID behöver lagra några hemligheter!

Diskussion

- Skall eduID API stödja U2F?
- Skall eduID använda U2F för ombud (RA) som skall genomföra ”vetting” till AL2 av personer som saknar svenskt personnummer/samordningsnummer?