

# Ladok3 och SWAMID

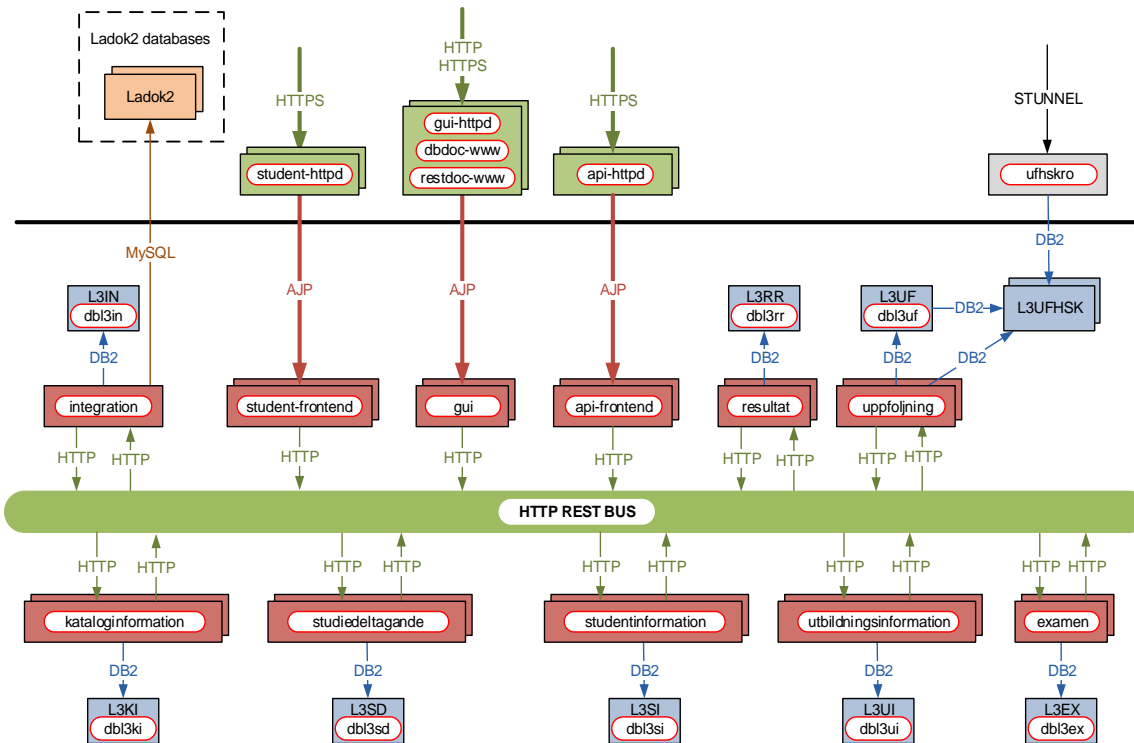
- » SWAMID Workshop 2, 2015-09-29
- » Fredrik Åslund <fredrik.aslund@umu.se>

# *Ladok3 och SWAMID*

- » Vad är Ladok3?
- » Leveranser
- » Tidsplan
- » Återautentisering
- » 2-faktor i Ladok3
- » SWAMID AL2 och Ladok3

# Ladok3

- » Sammanslagning av alla Ladok-instanser till ett system
- » 36 lärosäten
- » Fyra inlogningar
  - Inloggning via SWAMID
    - Studentgränssnitt
    - Admin-gränssnittet
  - SSL-cert
    - REST-API
  - SSL-cert + användare/lösenord
    - Uppföljningsdatabasen



# Leveranser

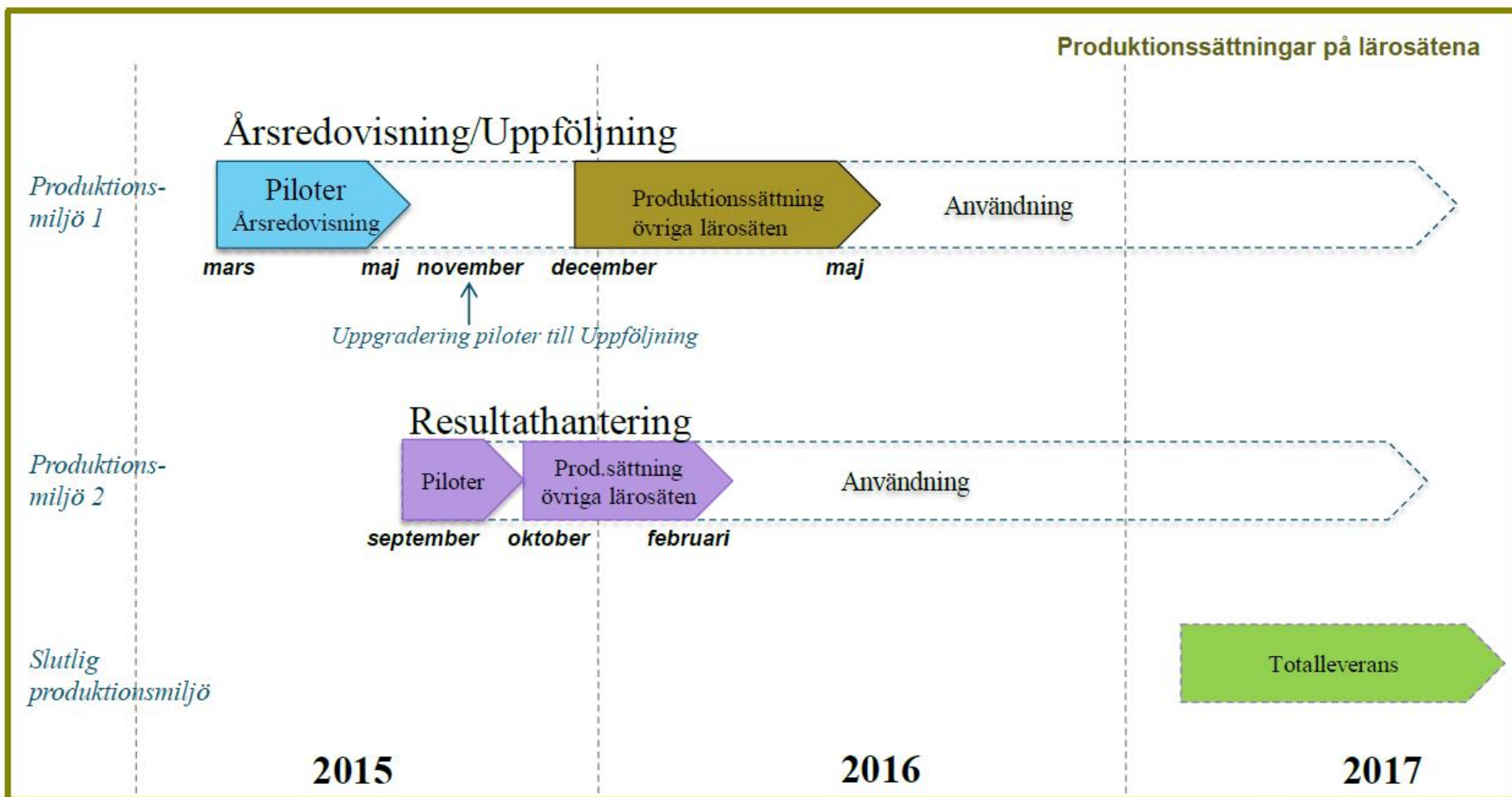
- » Ladok Årsredovisning
  - Basal rapportfunktionalitet
  - 4 piloter (HV, KMH, LIU, LNU)
  - Feb 2015
- » Ladok Uppföljning
  - Mer avancerade uppföljningsrapporter
  - REST-tjänster
  - Uppföljningsdatabaser
  - Okt 2015
- » Ladok Totalleveransen
  - Funktionalitet för att helt ersätta Ladok2
  - SWAMID AL2 för inloggning av studenter och anställda
  - MFA för bland annat alias-hantering
  - Produktionssättning under 2017

## *Ladok 3 Resultathantering*

### » Resultathantering

- Kör Ladok3:s resultattjänst, men mot Ladok2:s databas
- Funktionalitet för att rapportera och attestera betyg
- Återautentisering vid attestering
- Driftsättning under hösten

# Produktionssättningsplan





# Återautentisering i Resultathanteringsleveransen

## » Återautentisering

1. Spara eppn och timestamp

2. Utloggning från SP:n (behåll webbsessionen)

3. Inloggning via samma IdP

- ForceAuthN: true

- Authentication Context Class: PasswordProtectedTransport

4. Kontrollera återautentiseringen

- Jämför eppn med tidigare eppn

- Jämför AuthenticationInstant med tidigare timestamp

- Jämför AuthnContextClass med begärd Authentication Context Class

# Återautentisering i Resultathanteringsleveransen...

## » Status IdP:er

- 28 med reauth-stöd (inkl eduID)
- 7 utan reauth-stöd
  - 5 Shibboleth IdP med CAS
  - 1 gammal Shibboleth IdP
  - 1 SimpleSAMLphp med CAS
- 1 icke verifierad som inte ska köra Ladok3 Resultathantering



## 2-faktor i Ladok3

- » Behövs där kravet på autentisering är extra hög, exvis:
  - Hantering av skyddade personer
  - Utfärdande av examen
- » Fyra lösningar
  1. Lärosätet har en egen implementation av MFA i sin IdP
  2. Lärosätet låter de användare som behöver MFA använda sin eduID-inloggning med av lärosätet verifierad MFA
  3. Lärosätet använder eduID:s API för att implementera MFA i sin IdP
  4. Ladok3 använder eduID:s API för att koppla MFA till användare och sköter allt internt

# SWAMID AL2

## » SWAMID Bas

- Lite odefinierat, skicka personnummer i norEduPersonNIN om det är en “bekräftad” identitet (så fungerar Antagning.se/NyA-IdP:n idag)

## » SWAMID AL1

- Vi vet att det är en person, men inte vem

## » SWAMID AL2

- Vi vet vilken person det är, ID-kontroll har genomförts

## SWAMID AL2 i Ladok3

### » Studentgränssnittet

- Hantering av personuppgifter och studieresultat för sig själv
- Ladok3 måste veta vem studenten är

### » Administratörsgränssnittet

- Hantering av personuppgifter och studieresultat
- Hantering av behörigheter
- Ladok3 måste veta att lärosätet vet vem administratören är