# EDUP – teknik og arkitektur

Tom Bisgård Sørensen
02.05.2018



Experience the commitment®

# Agenda

- STILs integrationsarkitektur
  - IP-Ung – Fælles integrationsplatform for ungdomsuddannelsesområdet
- EDUP
  - XML/SOAP-baserede service udstillet gennem IP-Ung
  - Principper for beskedudveksling
  - Certifikatbaseret autentificering af den kaldende part
    - Primær og sekundær identitet
  - Autorisation i samarbejde med UNI-Login
- Praksis – og hvordan man integrerer til EDUP
  - Certifikater til hhv. test- og produktionsmiljøer
  - Tilmelding og konfiguration

# STILs integrationsarkitektur

To integrationsplatforme hos STIL

- IP-Grund – dedikeret til grundskoleområdet
- IP-Ung – dedikeret til ungdomsuddannelsesområdet

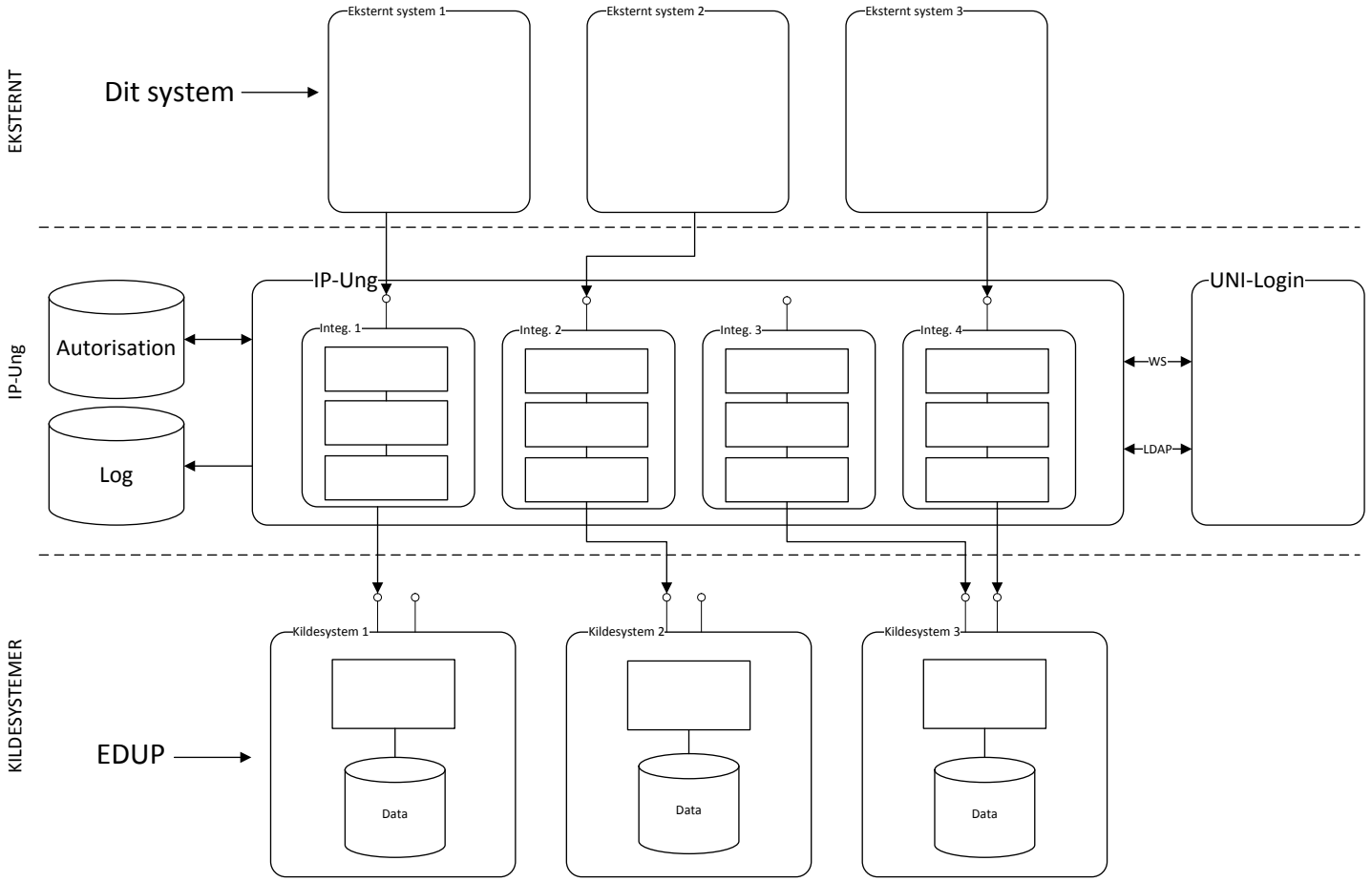
- Teknisk ens – begge er baseret på JBoss FUSE

- Formål
  - Afkobling mellem STILs egne systemer og eksterne systemer
  - Standardisering af snitflade og processer for tilkobling og adm.
  - Standardisering af autentificering
  - Standardisering af autorisation
  - Standardisering af logning



CGI

# STILs integrationsarkitektur - fortsat



# Services

EDUP udstiller en XML/SOAP-baseret service gennem IP-Ung – med følgende metoder:

- SendBesked – besked til institution vedr. elevflytning, -udlån, -deling og skolehjemsbooking
- HentStatus – har modtager hentet en afsendt besked
- HentListe – liste af endnu ikke-afventede beskeder sendt til institution
- AfhentBesked – hent besked og markér denne som afhentet

# Principper

- A til B kommunikation – der er altid en eksplicit afsender og modtager, udpeget ved deres respektive institutionsnumre

- Alle beskeder indeholder en fælles BeskedKuvert og variable BeskedData – afhængigt af beskedtypen – og besked-subtypen. BeskedKuverten indeholder oplysninger om:
  - Afsender og modtager
  - Elevens identitet (CPR-nr.)
  - Elevens uddannelse (CØSA-formål)

- EDUP validerer syntaks, men ikke semantik

- EDUP håndhæver ikke beskedmønstre

# Autentificering

Fastlæggelse af den kaldende parts primære og sekundære identitet

- Primær identitet = det kaldende system
  - DanID funktionscertifikat (FOCES) indeholdende CVR-nr. og FID
  - Hvordan?
    - Afsender signerer request iht. WS Security Signature
      - <SignedInfo> beskrivende hvilke dele af requestet som er anvendt til at beregne message digest (Body og Timestamp)
      - <SignatureValue> indeholdende message digest krypteret med afsender private nøgle
      - <KeyInfo> indeholder den offentlige del af certifikatet som BST – Binary Security Token
    - Modtager (IP-Ung) dekrypterer SignatureValue med medsendt offentlig nøgle og genberegner message digest

- Sekundær identitet = institutionen
  - Angivelse af institutionsnummer via WS Security UsernameToken

- ….og WS Security Timestamp – aht. replay attacks

# Autorisation

Fastlæggelse af om den kaldende part må tilgå den aktuelle service

- Efter succesfuld autentificering anvendes CVR, FID og servicenavn til opslag i IP-Ungs autorisationstabeller. Resultatet er navnet på en WS-bruger i UNI-Login
- IP-Ung spørger UNI-Login om den kaldende part har adgang til den kaldte service
- Efter succesfuld autorisation viderestilles til EDUP

# Praksis

Hvis du tidligere har integreret til service på IP-Ung – så er det ”business as usual” at integrere til EDUPs services ☺

- Udgangspunktet er den generelle integrationsvejledning: ”Integration-til-STILs-services-via-IP-Ung-og-IP-Grund.docx”
  - Detaljeret beskrivelse af autentificering via WS Security standard
  - Anskaffelse og anvendelse af certifikater i hhv. test. og produktionsmiljøer
    - Kun testcertifikater i test og kun produktionscertifikater i produktion!
  - Eksempler på Java og .Net WS-klienter og eksempel på kald fra SoapUI

1. Anskaf testcertifkat via DanID og produktionscertifikat via din LRA
2. Byg WS-klient i din egen teknologi pba. udstillet snitflade (WSDL)
3. Anmod og tilslutning til STILs testmiljø (CVR, FID, IP-adresse)
4. Efter succesfuld test, anmod om tilslutning til STILs produktionsmiljø (CVR, FID, IP-adresse)

# Our commitment to you

We approach every engagement with one objective in mind: to help clients succeed