



CONTEXT HANDLER - ARKITEKTURRÅD

NSIS og føderation

10 - 03 - 2022

Spørgsmål fra rådet

- Planerne for understøttelse af kommunernes implementering af NSIS via IST
- Planerne for kommunernes opkobling til den 'ny' Context Handler
- Hvilke dele af idp-opgaven løfter KOMBIT's løsning, og hvilke dele skal kommunerne selv løfte?



Intro til Context Handler

- Context Handler er et system der formidler kommunale brugeres log-in til de systemer de prøver at logge på.
- I mere tekniske termer fungere Context Handler som en SAML broker der formidler bruger log-ins i kommunale IdPer til Tjeneste udbydere der er registreret i den fælleskommunale infrastruktur
- Context Handler er funktionelt meget lig NemLog-In 3



Intro til Context Handler

Hvorfor har kommunerne Context handler når den ligner NemLog-In 3?

Context Handler har været i drift siden 2016 hvor den har givet kommunerne mulighed for:

- Lokal rettighedsadministration og ikke rettighedsadministration i systemerne
- Kommunal kontrol over videreudvikling af Context Handler.
- Understøttelse af hele den kommunale systemportefølge, både nyt og legacy

NSIS Context Handler - Baggrund og kommunale behov

NemLog-In 3, sætter krav om implementering af NSIS

- Det skal derfor understøttes at kommuner kan tilslutte en NSIS IdP
- Gamle IdPer (NIST sikringsniveauer) skal fortsat kunne fungere

Nogle IdPer understøtter ikke OIOBPP (rettighedsdelen i OIOSAML), så som Azure AD

- For at understøtte disse IdPer skal der laves en alternativ måde at overføre rettigheder på ved log-in

Behov for log-in til regionale og fællesoffentlige systemer



Ny funktionalitet

-Understøttelse af NSIS

- For tilslutning og understøttelse af både NSIS IdPer og gamle IdPer

-Implementering af Attributservice til overførsel af rettigheder

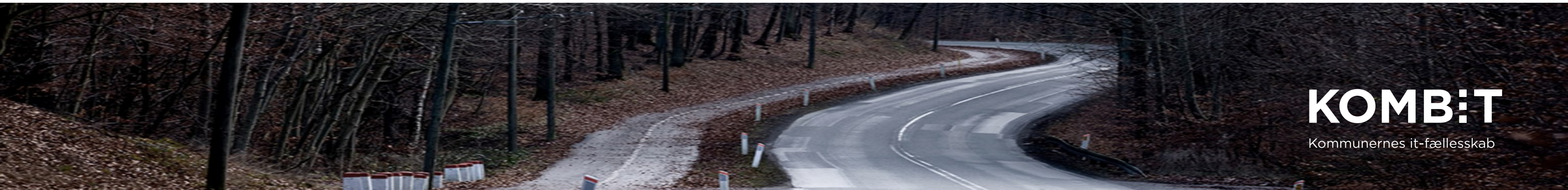
-Context Handler føderationer med:

- Sundhedsvæsenets elektroniske brugerstyring (SEB)

- log-in til regionale systemer

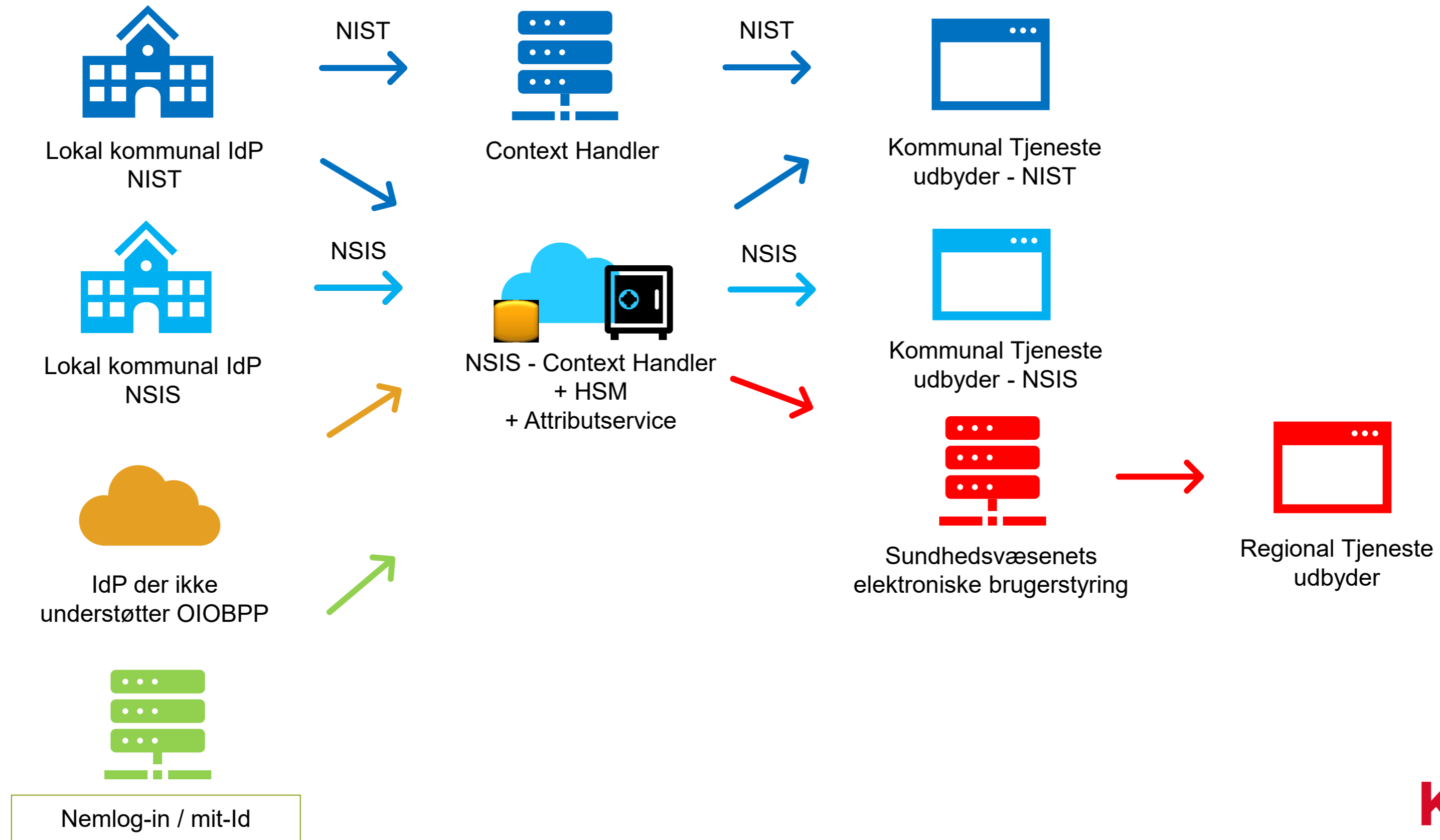
- NemLog-In 3

- Log-in/Step-up funktionalitet for kommunale IdPer der ikke har et givent NSIS sikringsniveau



OVERBLIK

Målbillede



Hvad betyder det for jer? - NSIS

Der vil være en periode hvor der vil være to Context Handlere.

-Indenfor den periode skal i jeres IdP stole på både Gamle- og NSIS Context Handler

Bemærk at jeres IdP skal ikke være NSIS compliant for at komme på NSIS Context Handleren, da den kan håndtere både gamle og NSIS IdPer

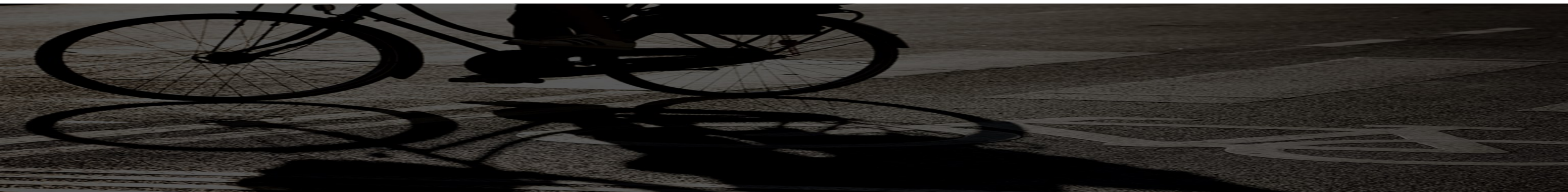
Obs: Når i så på et tidspunkt har en NSIS compliant IdP (enten opgraderet eller ny) og den er godkendt af DIGST, så kan I begynde at sende NSIS sikringsniveauer via NSIS Context Handleren

Hvad betyder det for jer? - Attributservice

Attributservicen kan anvendes hvis en kommune ikke kan sende brugeres rettigheder via deres IdP

Eksempelvis er nogle kommuner i gang med at ibrugtage Azure AD og den understøtter ikke rettighedsdelen out of the box.

Herefter kan i så uploade brugeres rettigheder til CH-attributservice



Hvad betyder det for jer? - Føderation til NemLog-In 3

Føderationen til NemLog-In 3 anvendes til kommunens IdP enten ikke understøtter et krævet NSIS sikringsniveau eller de ikke har fået etableret en NSIS IdP

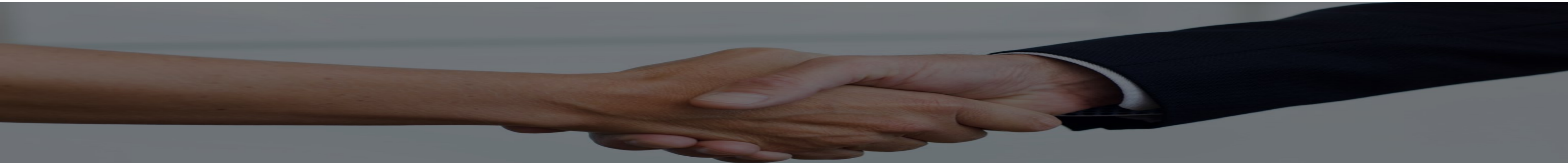
Med denne føderation kan i stadig administrere jeres brugeres rettigheder i jeres lokale brugerrettighedsstyring. Selve i identifikationen af brugeren forgår i NL3 eksempelvis via MitID

De af jeres brugere der har behov for at kunne lave et Log-in eller step-up mod NL3 har behov for et MitID erhverv og jeres IdP skal kunne sende brugerens MitID referenceID.

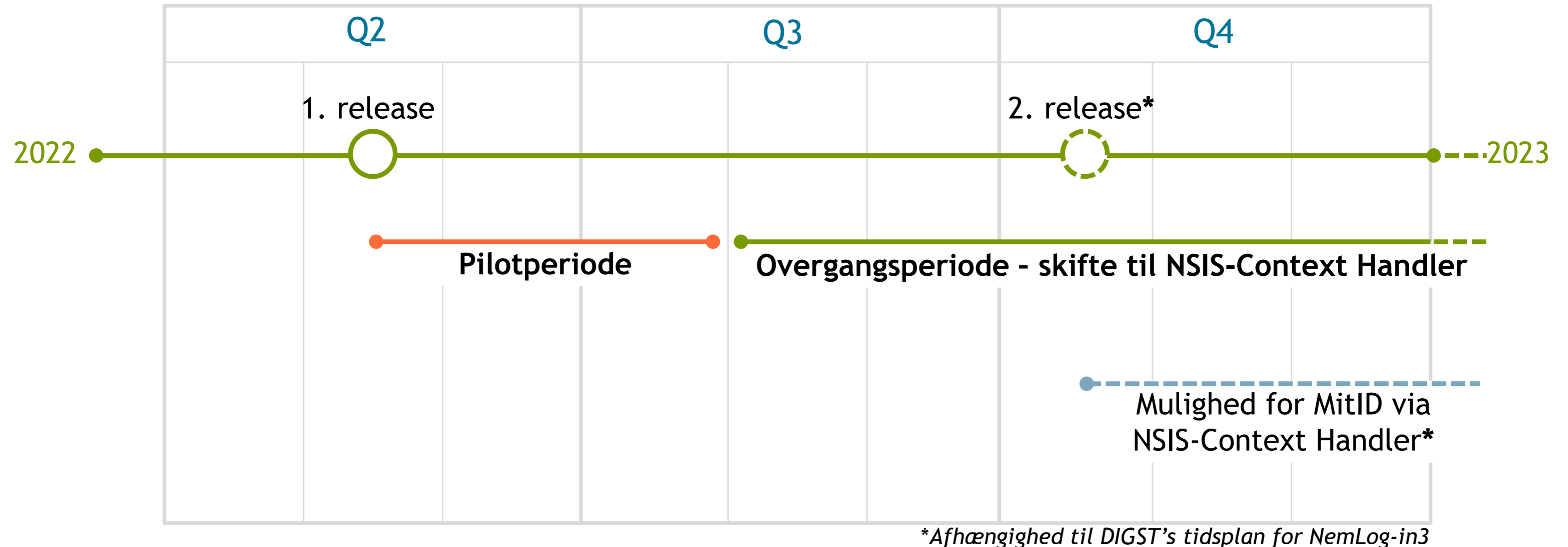
Hvad betyder det for jer? - Føderation til SEB

NSIS CH kan bruges til at logge in på regionale systemer via SEB føderationen. Det kræver selvfølgelig at Sundhedsdatastyrelsen har tilsluttet systemerne til SEB brokeren

Hvis jeres IdP ikke kan sende de nødvendige attributter til SAML token til CH, kan i så i stedet uploade brugerens rettigheder til CH-attributservice



Plan for NSIS Context Handler



- Vi sender yderligere information ud op til henholdsvis 1. og 2. release
- Kommunerne vil modtage KLIK-opgave vedr. overgang til NSIS-Context Handler
- I overgangsperioden vil der være to kørende versioner af Context Handler; den nuværende og NSIS-Context Handler

Opsummering

Planerne for understøttelse af kommunernes implementering af NSIS via IST

- Context Handler går i luften slut Q2 (pt 28 maj)

Planerne for kommunernes opkobling til den 'ny' Context Handler

- Det planlægges at have miljøer klar så kommunerne kan etablere trust til NSIS Context Handler i start maj

Hvilke dele af idp-opgaven løfter KOMBIT's løsning, og hvilke dele skal kommunerne selv løfte?

- Lige gyldig om en kommune tilslutter sig til NL3 eller CH, så skal i stadig overholde samtlige DIGST krav til NSIS sikringsniveauer. CH kan hjælpe med de nye tiltag der er beskrevet i disse slides

Her kan du læse mere

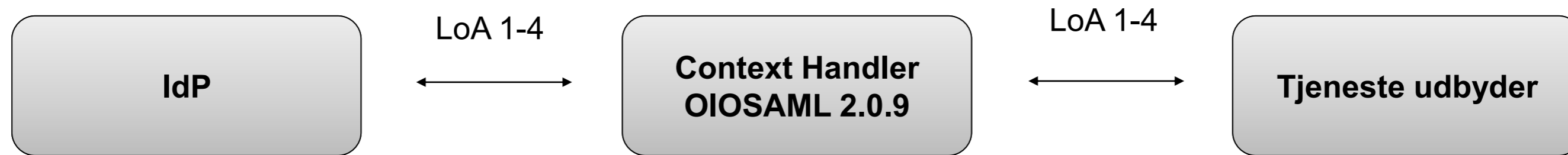
- [Om Fælleskommunal Adgangsstyring for brugere i Digitaliseringskataloget](#)
- [Om NSIS-standarden hos Digitaliseringsstyrelsen](#)
- [Om KL's projekt til støtte og sikring af koordinering af implementering af NSIS i kommunerne hos KL/KOMBIT Videncenter](#)

**TAK FOR
OPMÆRKSOMHEDEN**

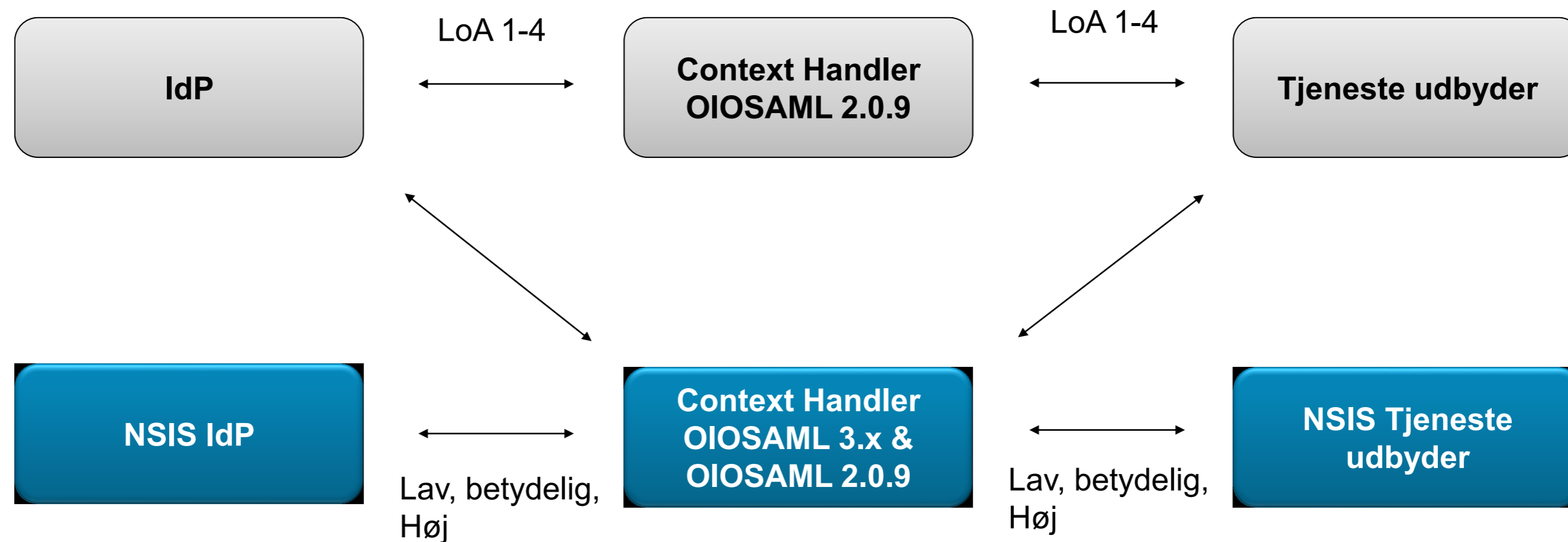
EKSTRA SLIDES

GLIDENDE OVERGANG

Glidende overgang - Nu

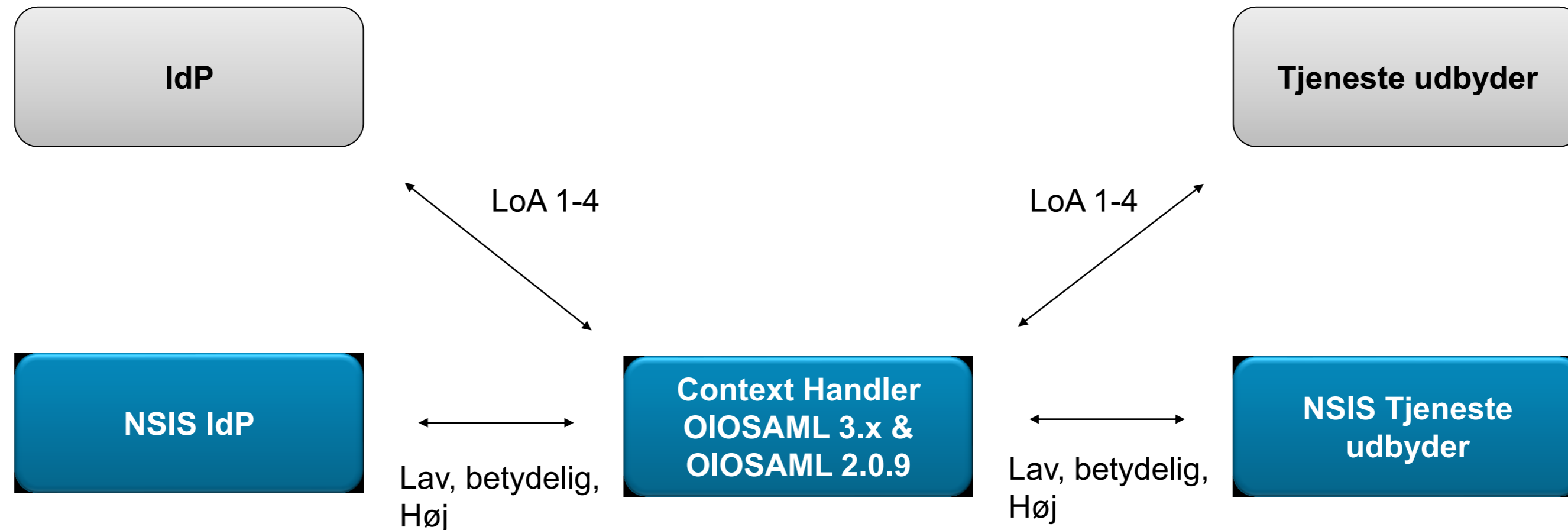


Glidende overgang - To CH



- CH skal overholde NSIS niveau Høj
- Ny og gammel LoA angivelse eksisterer parallelt.
- CH kan veksle nyt 'LoA Betydeligt' til gammelt 'LoA 3', men ikke omvendt.
- Et NSIS niveau kan kun opnås hvis kommunens IdP er godkendt hos DIGST

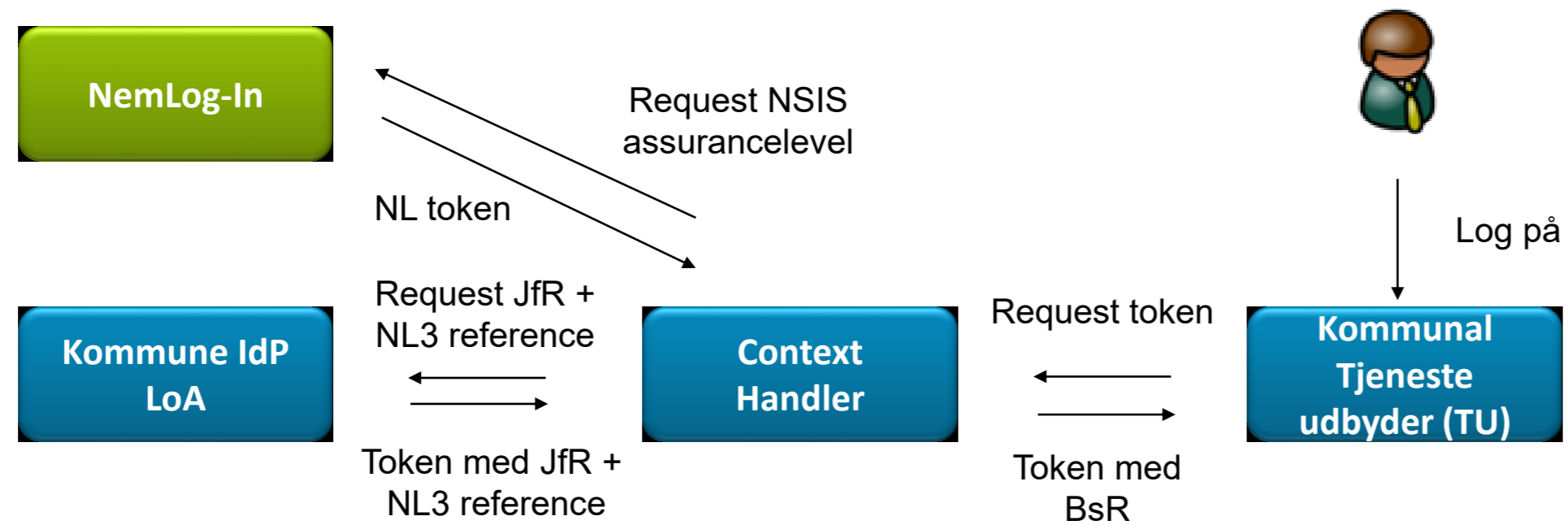
Glidende overgang - Gammel CH udfases (Når alle systemer har rettet pegepinde mod ny CH)



- CH skal overholde NSIS niveau Høj
- Ny og gammel LoA angivelse eksisterer parallelt.
- CH kan veksle nyt 'LoA Betydeligt' til gammelt 'LoA 3', men ikke omvendt.
- Et NSIS niveau kan kun opnås hvis kommunens IdP er godkendt hos DIGST

**STEP-UP VIA NEMLOG-IN
MED MITID**

Step-up via Nemlog-in



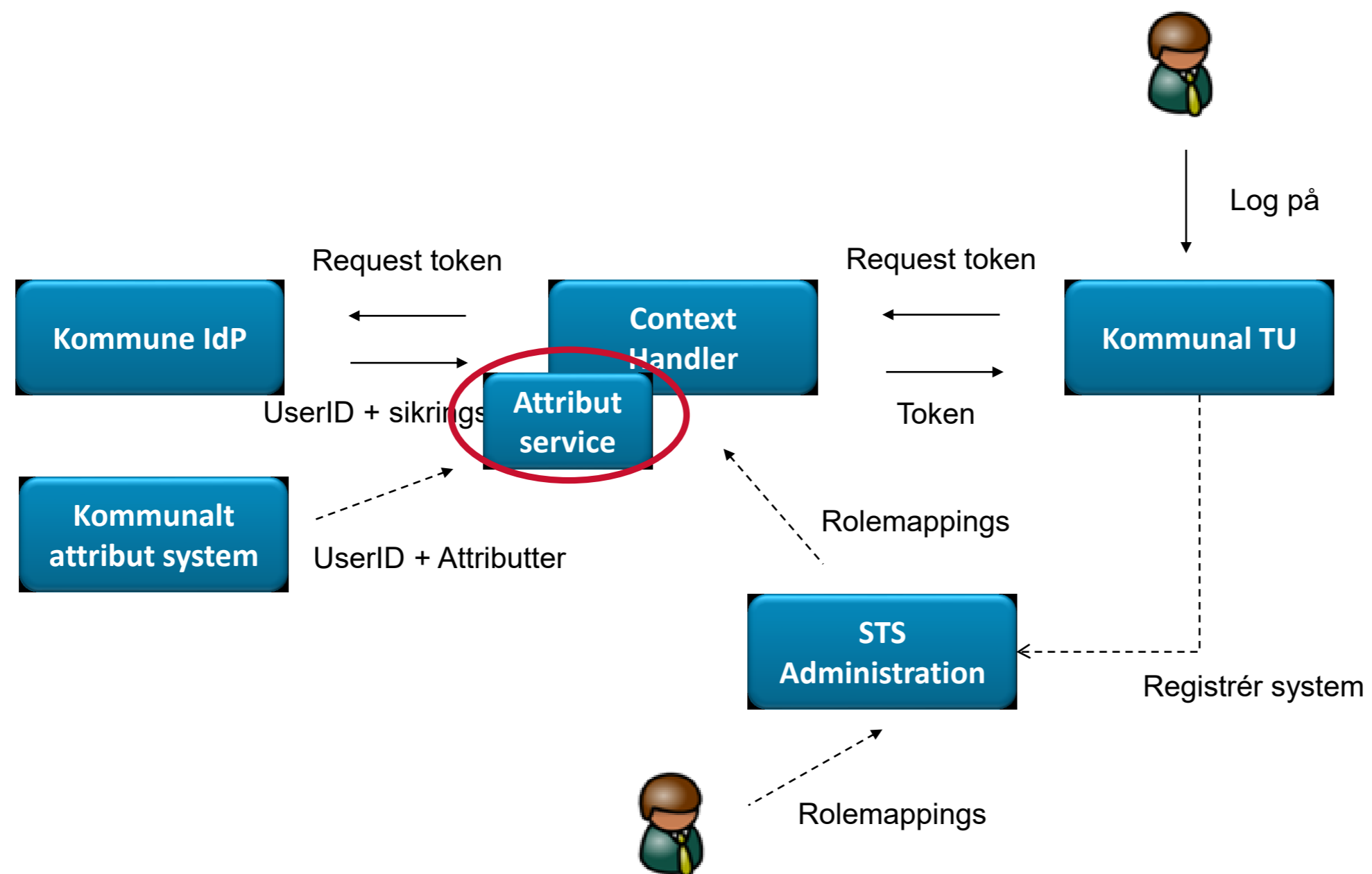
KOMBIT
Attributprofil

NemLog-In
Attributprofil

CLOUD IDP

-MANGLENDE UDNERSTØTTELSE AF OIOBPP

IdPer der ikke kan sende attributter som OIOBPP



KOMBIT
Attributprofil

FØDERATIONER

SEB føderation

