FÆLLESKOMMUNAL ADGANGSSTYRING FOR BRUGERE – NY CONTEXT HANDLER

Kommunernes Data- og Infrastrukturdag 2022

KOMB:T

VELKOMMEN

Rasmus Halkjær Iversen

Chefkonsulent

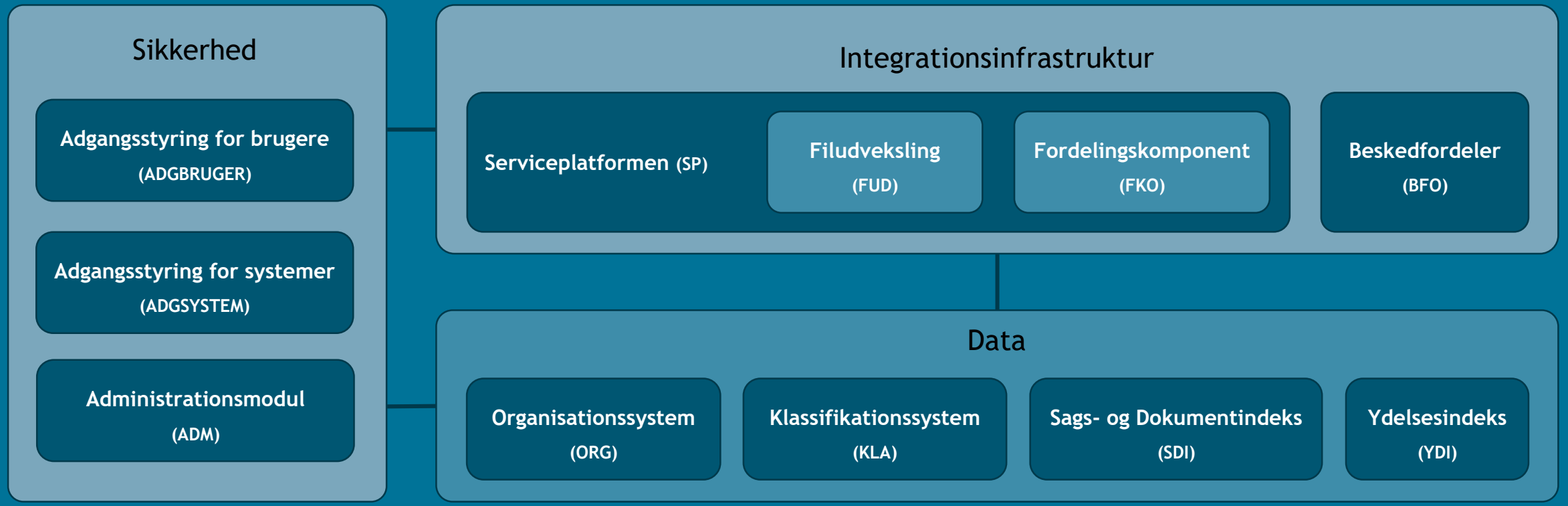
Christina Andersen

Seniorkonsulent

DAGSORDEN

- Funktionalitet i ny version af Context Handler
  - For IdP'er
  - For brugervendte systemer
- Sådan tager et brugervendt system den nye version i brug
  - Fire trin
  - Foreløbig tidsplan
- Demo – test af login-flow

KOMPONENTOVERBLIK I INFRASTRUKTUREN



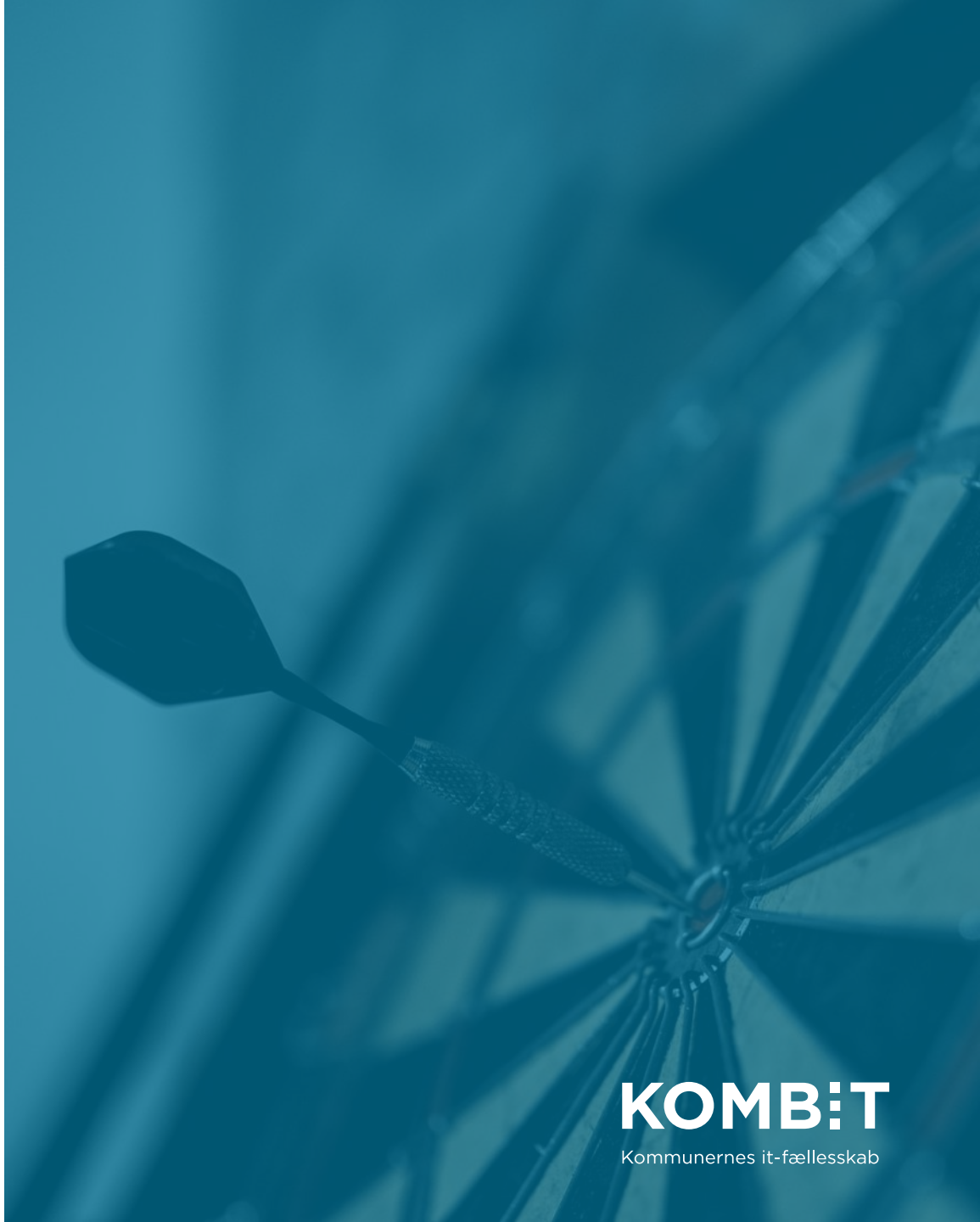
KOMBIT

FORMÅL

Når oplægget er slut, ved I hvilken ny funktionalitet, den nye version af Context Handler indeholder, og hvordan tidsplanen ser ud for ibrugtagning.

Det sker helt konkret, ved at;

- I har fået viden om hvordan den nye version af Context Handler kan bruges og
- I har fået viden om, hvordan og hvornår I kan tage den nye version i brug



KOMB:T
Kommunernes it-fællesskab

FUNKTIONALITET I NY VERSION AF CONTEXT HANDLER

KOMB:T

BAGGRUND: KOMMUNALE BEHOV

Krav fra NemLog-in3 om implementering af National Standard for Identiteters Sikringsniveauer (NSIS)

- Den nye version skal derfor understøtte både:
  - Kommuners NSIS-IdP'er
  - Kommuners "gamle" IdP'er (NIST)

Nogle IdP'er understøtter ikke OIOBPP-format (rettighedsdel i OIOSAML)

- Den nye version skal derfor understøtte en alternativ måde at overføre rettigheder på ved log-in

Kommunale brugere skal kunne logge på regionale og fællesoffentlige systemer

NY FUNKTIONALITET SKAL UNDERSTØTTE BEHOV

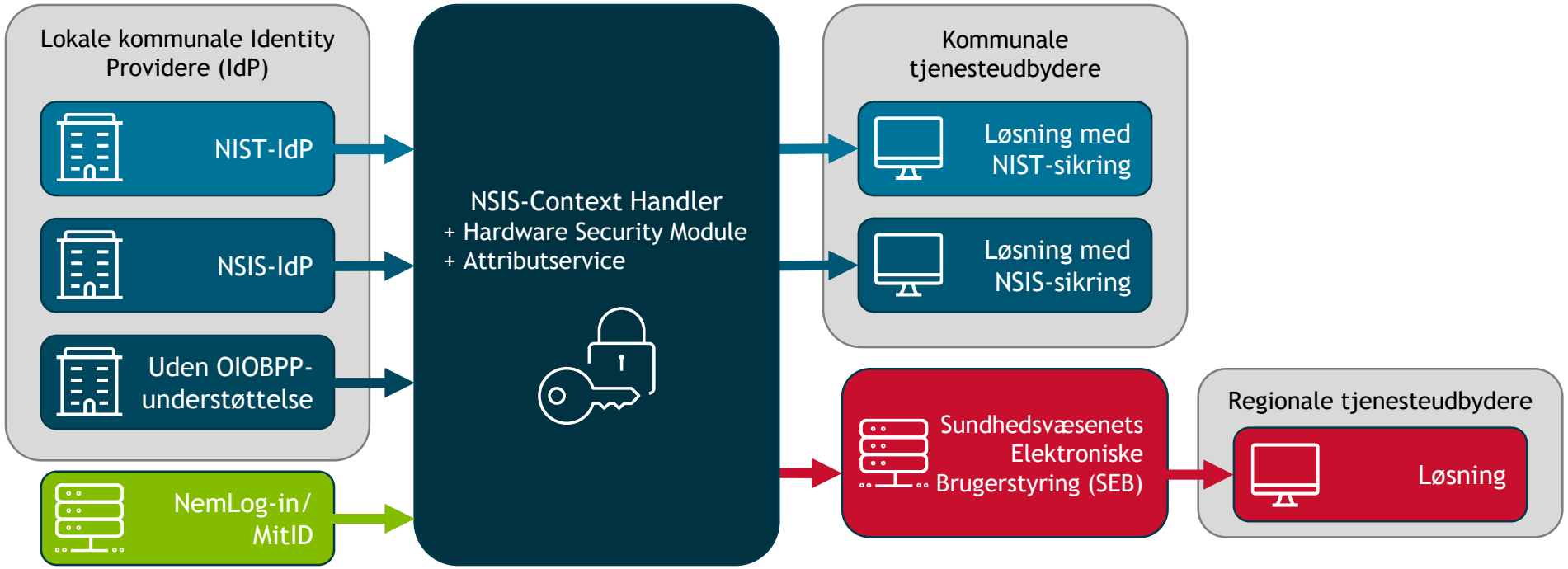
Understøttelse af NSIS
- Tilslutning og understøttelse af både NSIS-IdP'er og "gamle" IdP'er

Implementering af Attributservice
- Til overførsel af rettigheder (attributter)

Føderationer
- Sundhedsvæsenets Elektroniske Brugerstyring (SEB): Log-in til regionale systemer
- NemLog-in3: Log-in/step-up-funktionalitet for IdP'er, der ikke har et givent NSIS-sikringsniveau

FUNKTIONALITET I NUVÆRENDE CONTEXT HANDLER

FUNKTIONALITET I NY VERSION AF CONTEXT HANDLER



KOMBIT

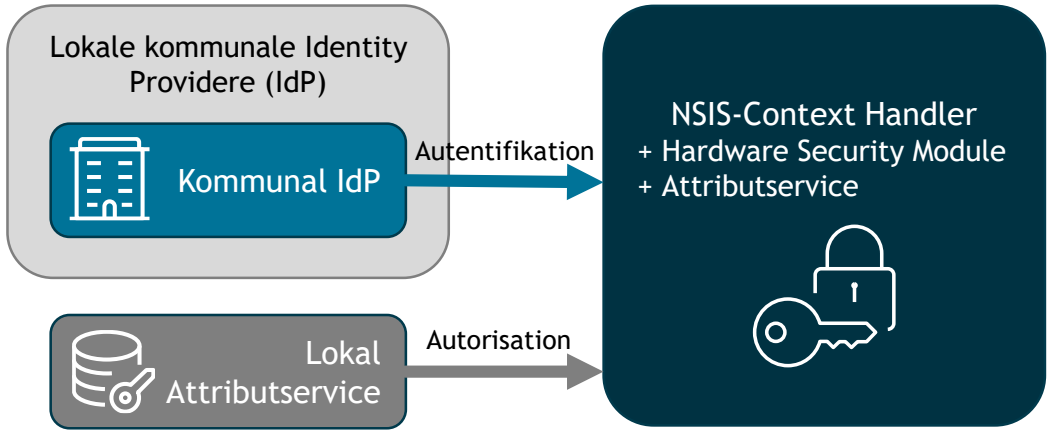
LOG-IN FOR BÅDE NIST- OG NSIS-IDP'ER

Det vil være muligt at logge på en løsning med NIST-sikring med en NSIS-IdP – men det vil omvendt ikke være muligt at bruge en NIST-IdP til en løsning med NSIS-sikring, uden at bruge step-up-funktionaliteten.

KOMBIT

ATTRIBUTSERVICE

Attributservicen kan anvendes, hvis en kommune ikke kan sende brugeres rettigheder via deres IdP - fx er nogle kommuner i gang med at ibrugtage Azure AD, der ikke understøtter rettighedsdelen ”out of the box”.



FØDERATION: NEMLOG-IN

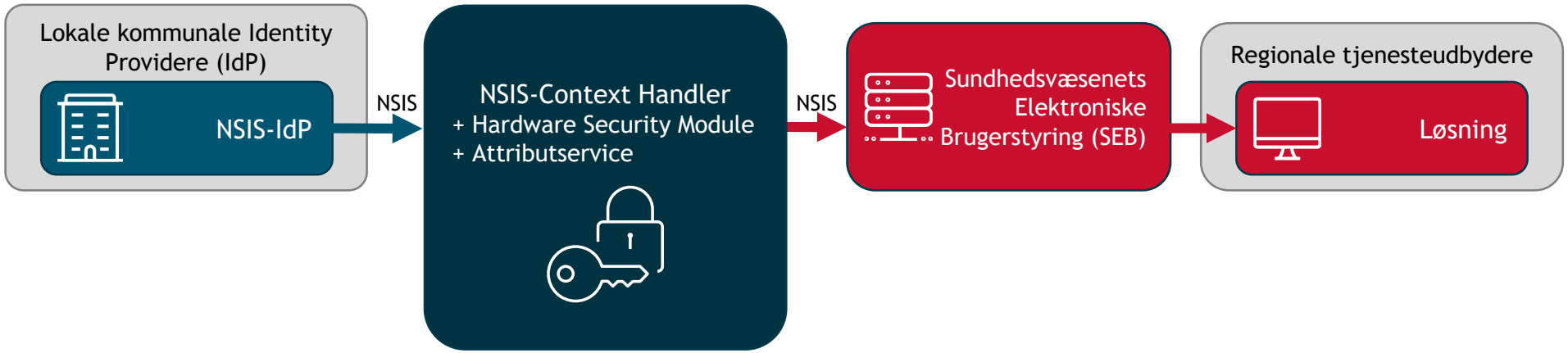
Føderation med NemLog-in kan anvendes, hvis kommunens NSIS-IdP ikke understøtter et tilstrækkeligt NSIS-sikringsniveau.

Brugeres rettigheder administreres i lokal brugerrettighedsstyring. Identifikation af bruger foregår i NL3, fx via MitID. Brugere, der skal kunne lave log-in/step-up med NL3, skal have et MitID Erhverv, og IdP skal kunne sende brugerens MitID-referenceID.

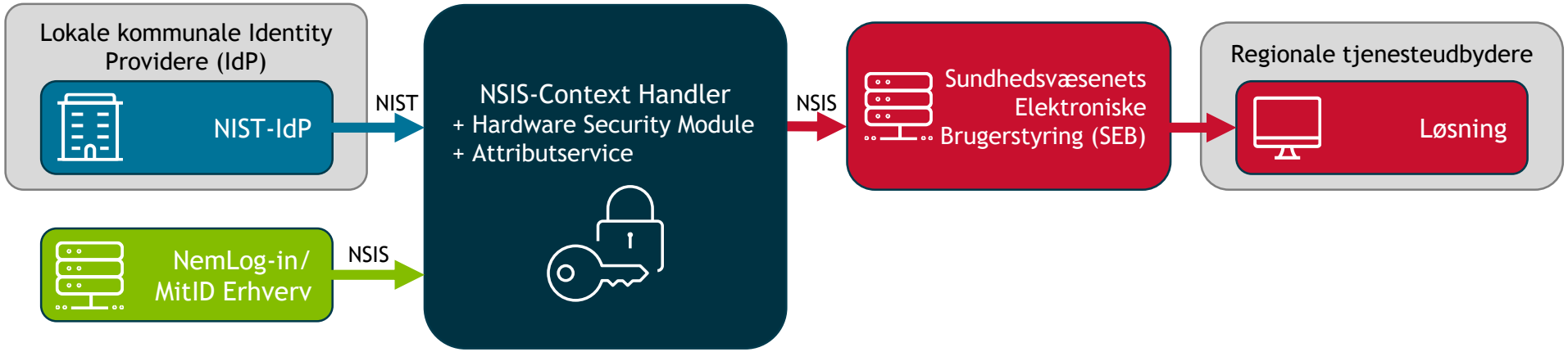
KOMBIT

FØDERATION: SUNDHEDSVÆSENETS ELEKTRONISKE BRUGERSTYRING

For NSIS-IdP



For NIST-IdP (step-up via NemLog-in)



SÅDAN TAGER ET BRUGERVENDT SYSTEM DEN NYE VERSION I BRUG

KOMB:T

HVORDAN GØR MAN DET?

Jeres brugervendte system skifter til ny version af Context Handler ved at gå igennem disse fire trin:

1. Hent SAML-metadata for ny version
2. Opdatér det brugervendte system med SAML-metadata for ny version
3. Dan nye SAML-metadata for jeres brugervendte system
   - Alternativ: Dan et link, som den nye version af Context Handler kan hente systemets nye SAML-metadata fra
4. Opdatér information for det brugervendte system i Fælleskommunalt Administrationsmodul

Trinnene udføres for hhv. Eksternt testmiljø og Produktionsmiljø.

1. HENT SAML-METADATA FOR DEN NYE VERSION

- SAML-metadata for Context Handler hentes fra Digitaliseringskataloget.
- Vælg metadata for brugervendt system for det miljø, du vil opdatere (*NB: metadata for brugervendt system gøres tilgængelig, når alle kommuner har etableret trust til ny version af Context Handler*):

Metadata til ny version - NSIS-Context Handler

Metadata Ekstern Test (ny version):

- For brugervendt system: (*ikke tilgængelig endnu*)
- For IdP (kommunal eller leverandørmyndighed): https://n2adgangsstyring.eksterntest-stoettesystemerne.dk/runtime/saml2auth/metadata.idp

Metadata Produktion (ny version):

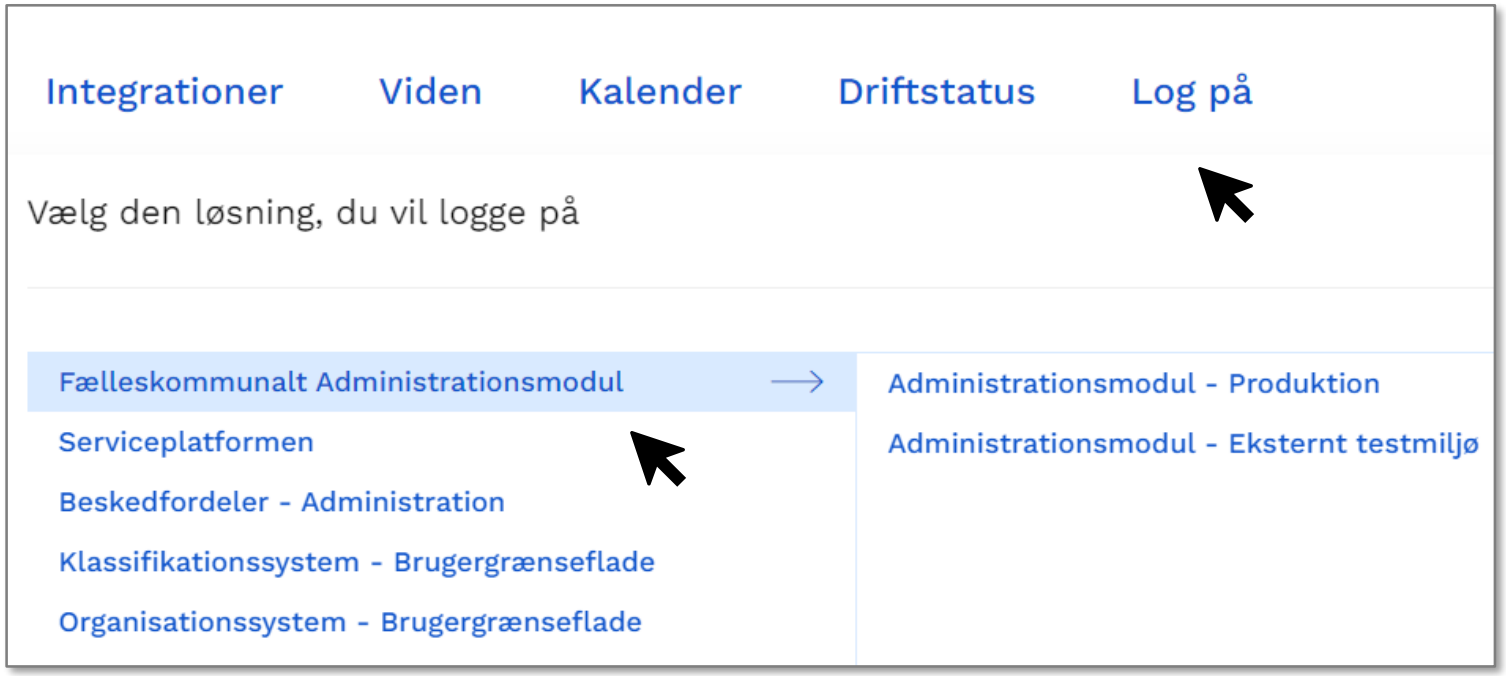
- For brugervendt system: (*ikke tilgængelig endnu*)
- For kommunal IdP: https://n2adgangsstyring.stoettesystemerne.dk/runtime/saml2auth/metadata.idp

KOMBIT

4. OPDATÉR INFORMATION I ADMINISTRATIONSMODUL (I)

Log på Fælleskommunalt Administrationsmodul*:

- Eksternt testmiljø
- Produktion

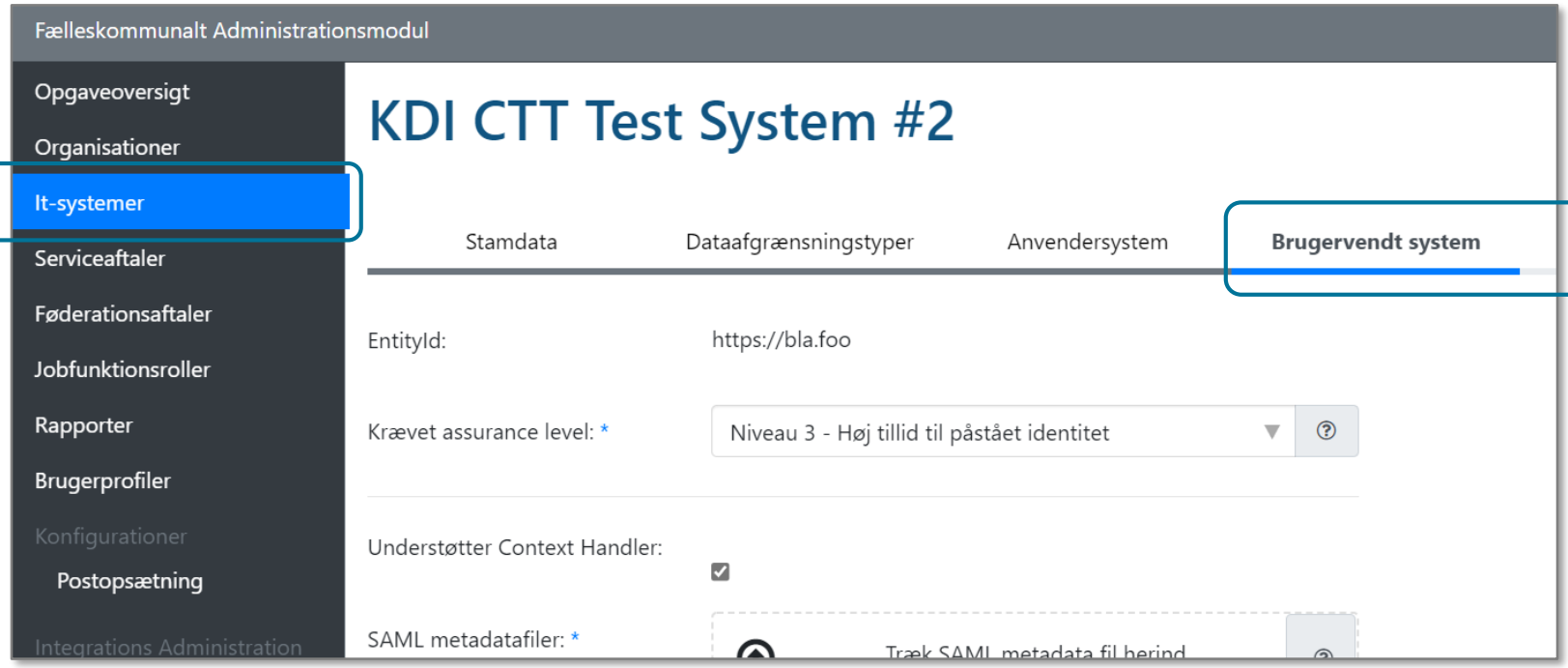


**For at kunne opdatere/redigere et it-system i Administrationsmodulet skal du have de rigtige rettigheder*

KOMBIT

4. OPDATÉR INFORMATION I ADMINISTRATIONSMODUL (II)

1. Find jeres system



2. Vælg fanen *Brugervendt system*

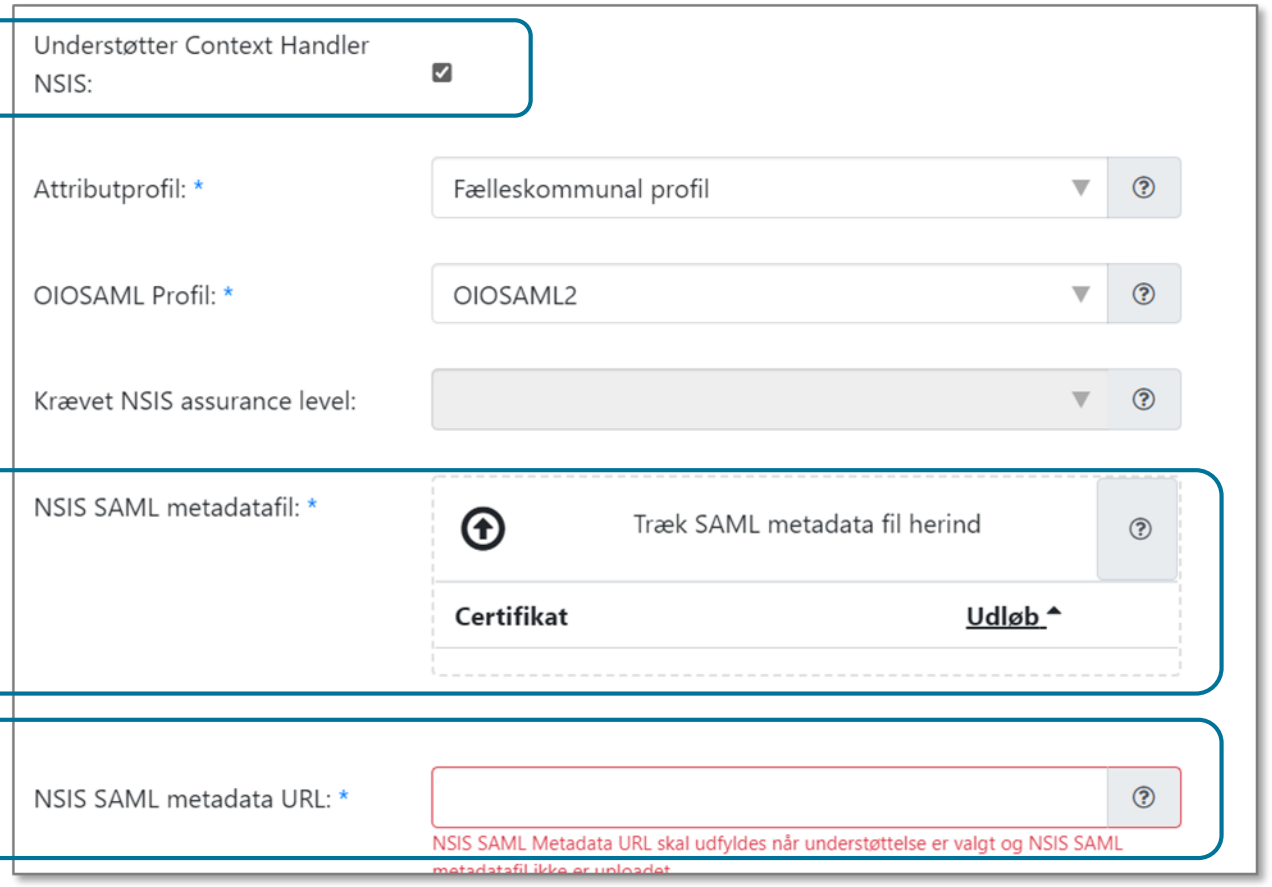
KOMBIT

4. OPDATÉR INFORMATION I ADMINISTRATIONSMODUL (III)
- Hvis I vil bruge OIOSAML 2

Sæt hak ved *Understøtter Context Handler NSIS*

Enten indlæs NSIS SAML-metadatafil for det brugervendte system

Eller indsæt URL, hvorfra Context Handler kan hente NSIS SAML-metadata for det brugervendte system



4. OPDATÉR INFORMATION I ADMINISTRATIONSMODUL (III)
- Hvis I vil bruge OIOSAML 3, skal I desuden

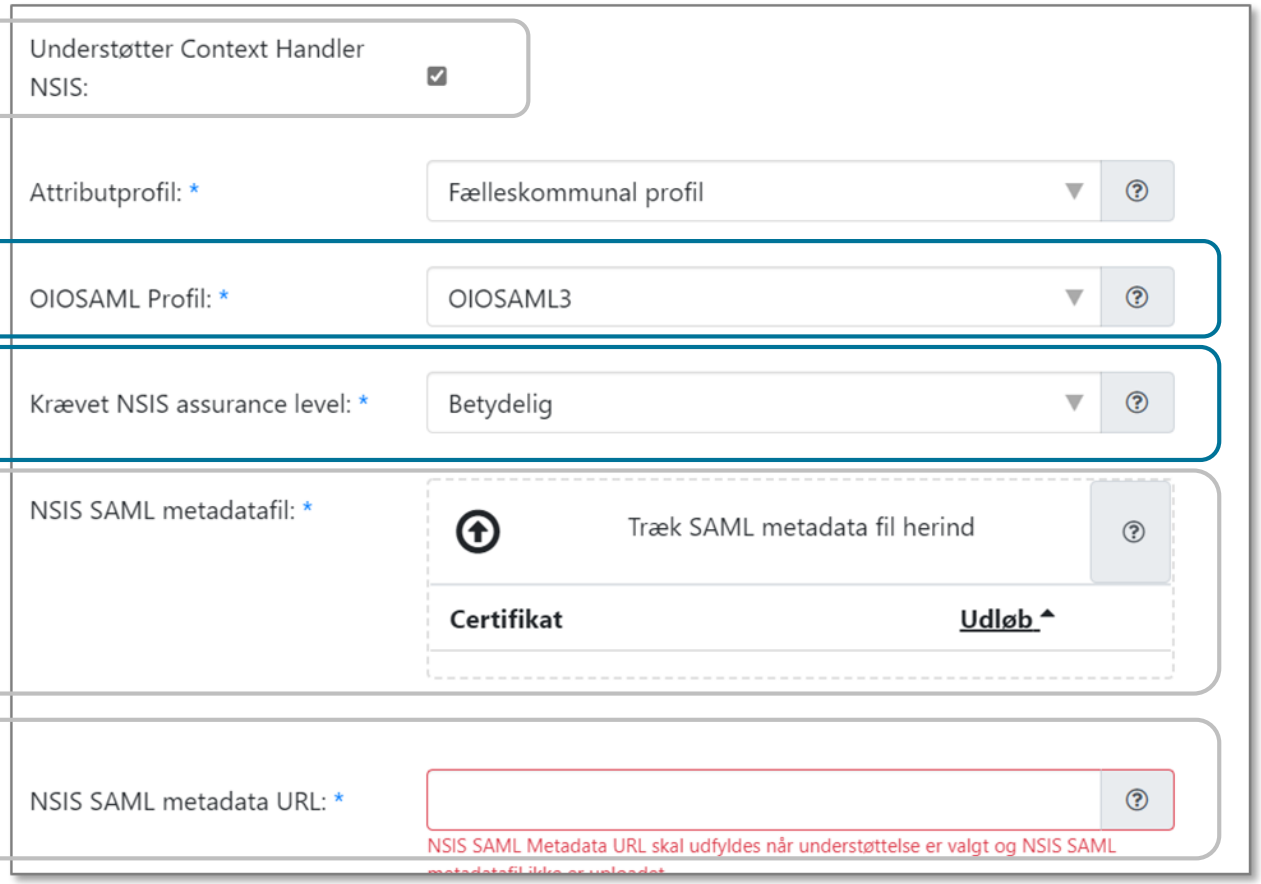
Sæt hak ved *Understøtter Context Handler NSIS*

OIOSAML Profil ændres til *OIOSAML3*

Krævet NSIS Assurance level sættes til det sikrings-niveau, brugere skal have, for at kunne logge ind

Enten indlæs NSIS SAML-metadatafil for det brugervendte system

Eller indsæt URL, hvorfra Context Handler kan hente NSIS SAML-metadata for det brugervendte system



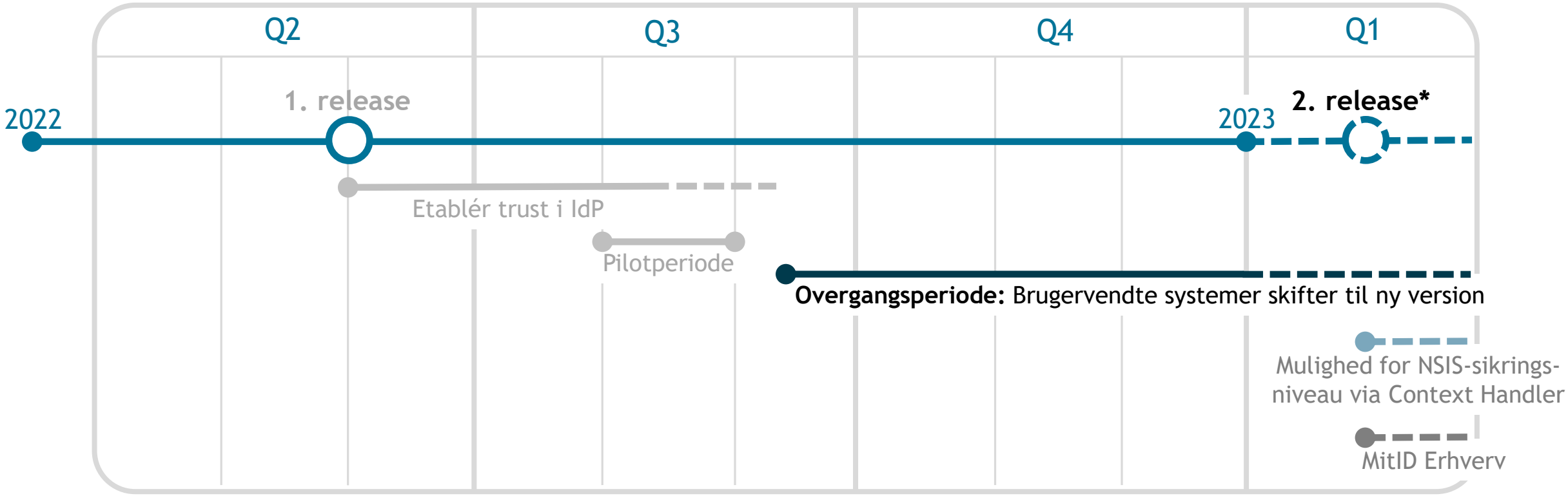
- Den nye version af Context Handler anvender kun OIOSAML 3-protokol, men med krypto-algoritmer, der virker i både OIOSAML 3- og OIOSAML 2-profil.
- Det brugervendte system skal i log-in request angive, om der anvendes NIST eller NSIS, samt niveau.

KOMBIT

HVORNÅR KAN ET BRUGERVENDT SYSTEM SKIFTE TIL NY CONTEXT HANDLER?

KOMB:T

FORELØBIG TIDSPLAN FOR IBRUGTAGNING AF NY VERSION



**NSIS-revidering af ny version af Context Handler*

- I overgangsperioden vil der være to kørende versioner af Context Handler; den nuværende og den nye version. Det er i denne periode, at brugervendte systemer skal skifte til den nye version. Overgangsperioden kan starte, når alle kommuner har etableret trust. Vi melder ud, når overgangsperioden går i gang.
- Efter 2. release, kan en kommunes IdP sende NSIS-sikringsniveauer, hvis den er NSIS-godkendt. Der kan stadig sendes NIST-sikringsniveauer via den nye version af Context Handler.

KOMBIT

DEMO
- TEST AF LOGIN-FLOW

KOMB:T

VÆRKTØJER TIL TEST AF LOGIN-FLOW

KOMBIT stiller testværktøjer til rådighed for myndigheder til test af deres IdP'er.

Testværktøjerne giver mulighed for at inspicere login-flowet i en browser i forbindelse med test af Fælleskommunal Adgangsstyring for brugere i det eksterne testmiljø.

Du finder links til testværktøjerne i Digitaliseringskataloget.