



DIGITALISERINGSSTYRELSEN

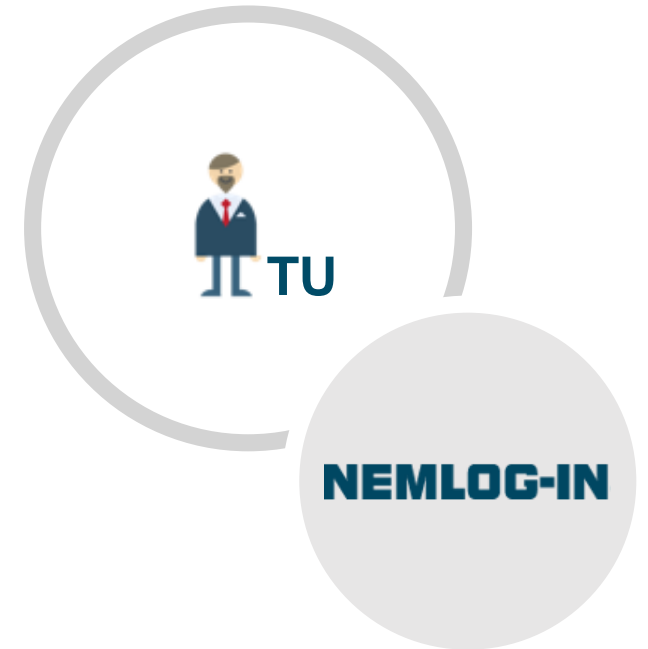
OIOSAML

Februar 2020



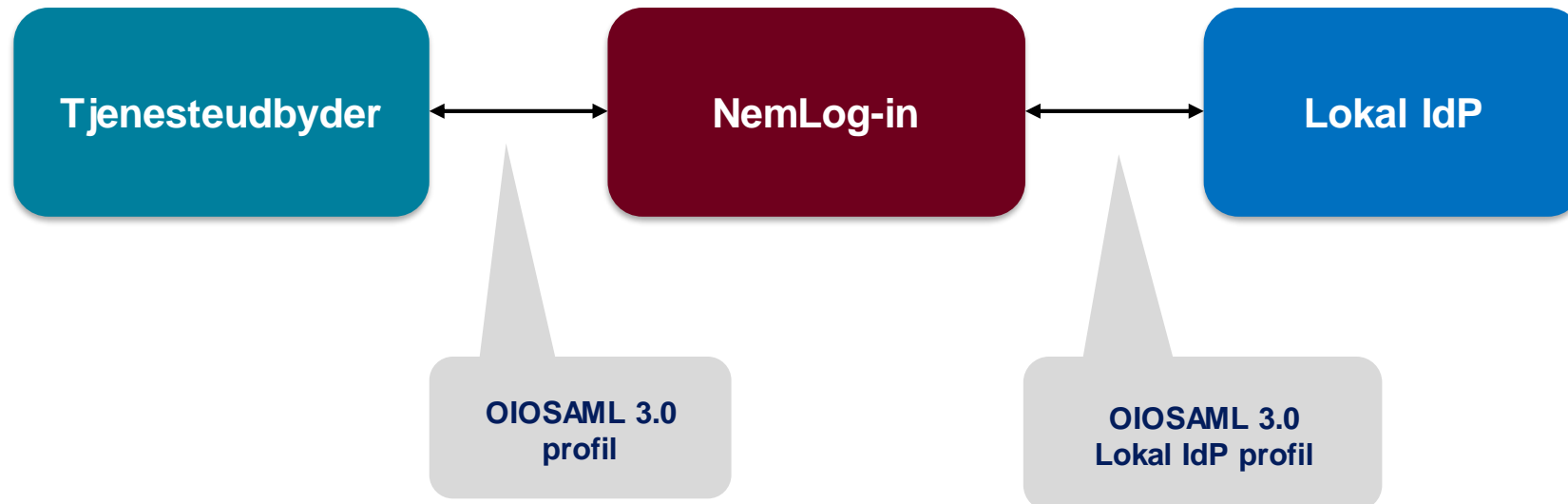
Ændringer i snitflade mellem TU og NemLog-in

- Ny snitflade for tjenesteudbyderes opkobling via NemLog-in: OIOSAML 3.0
 - OIOSAML 2.0.9 (nuværende) understøttet under migrering.
 - NemID og MitID understøttet via begge OIOSAML versioner.
- NemLog-in skjuler anvendt identifikationsmiddel over for TU
 - Dog ikke PKI i MitID: ingen OCES attributter i SAML token.
- Tjenesteudbyderspecifikt UUID i stedet for PID/RID
 - PID/RID understøttes i overgangsperiode.
- CPR kan leveres for borgere og erhvervsidentiteter m. CPR
 - Hvis tjenesten har hjemmel (primært offentlige tjenester).



OIOSAML profiler

- To varianter
 1. OIOSAML ml. Tjenesteudbyder og NemLog-in
 2. OIOSAML Lokal IdP ml. Lokal IdP og NemLog-in



OIOSAML 2.0.9 til 3.0

- Ny struktur med udgangspunkt i SAML2Int profilen fra Kantara Initiative.
- To nye attributprofiler for hhv. (privat)personer og professionelle
 - OCES-specifikke attributter udgår
 - RID og PID fortsættes, men deprecated.
- Identifiers baseret på UUID'er og Subject er tjenesteudbyderspecifikke – styrket privacy.
- Krav til kryptografiske algoritmer og nøglelængder er skærpet.
- 'Levels of assurance' i henhold til NSIS og angivelse af ønsket sikringsniveau (herunder muligheden for step-up autentifikation).
- Support for multiple certifikater i metadatafiler.
- Tilladt at anvende kvalificeret certifikat for en juridisk person i metadata.



Sikringsniveau iht. risikovurdering



- Den enkelte tjenesteudbyder er dataansvarlig for egne data.
- Fastsættelse af krævet sikringsniveau for tjenesteudbyder ud fra risikovurdering.

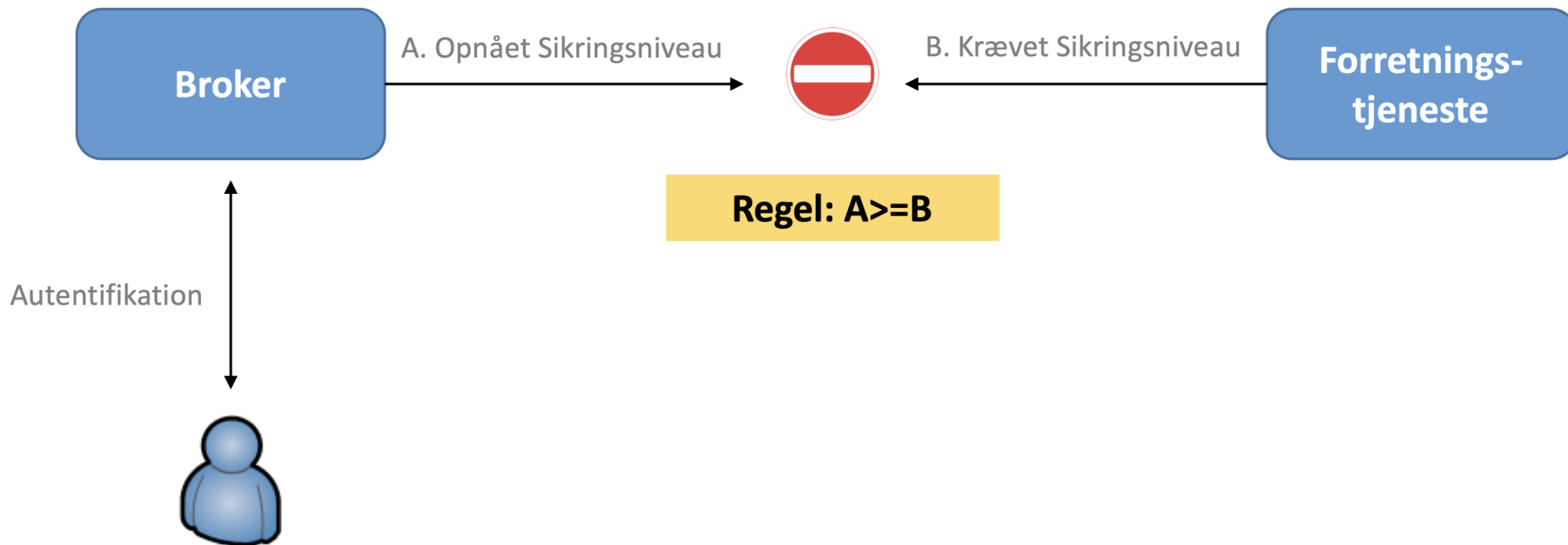


- NSIS stiller ikke specifikke krav til sikringsniveau.
- Opmærksomhed på krav til brugergruppes sikringsniveau.

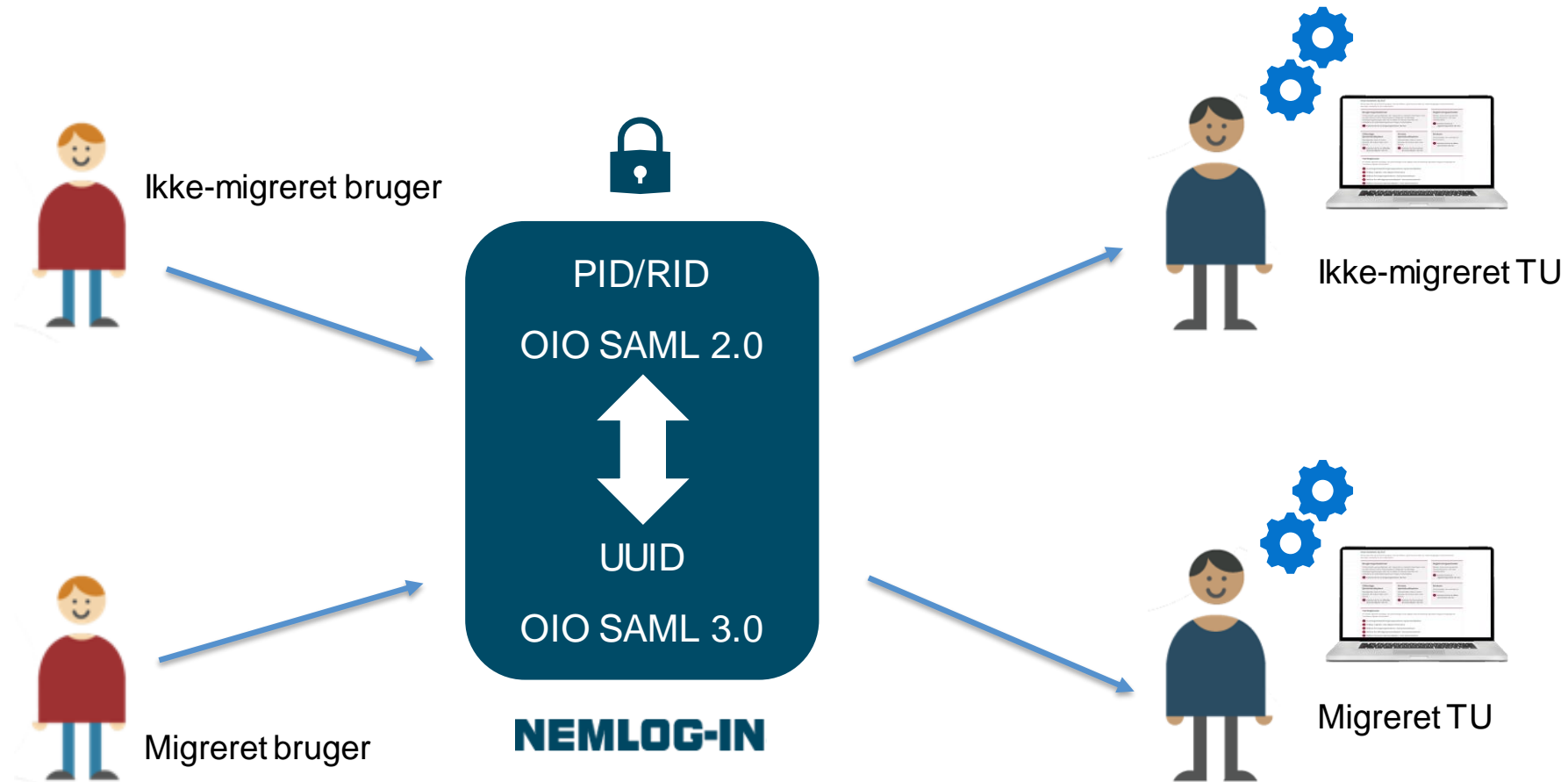


- Inspiration i “Vejledning til valg af NSIS Sikringsniveau for tjenesteudbydere”.
- Digitaliseringsstyrelsen arbejder på et støtteværktøj til fastsættelse af sikringsniveau.

NSIS ved login til tjeneste



NemLog-in bro i migreringsperioden



Attributoversigt – uddrag

- UUID – *TU-specifik persistent identifier eller transient*
- Persistent Identifier – *global (på tværs af TU) identifier for erhvervsidentitet*

- LOA – *level of assurance*
- IAL – *identity assurance level*
- AAL – *authentication assurance level*

- CPR UUID – *nyt UUID fra CPR registeret*
- PID – *deprecated*
- RID – *deprecated*

Implementerings- og kommunikationsaktiviteter

- **NemLog-in portalen:** www.nemlog-in.dk
 - Målgruppeopdelt information for brugerorganisationer, offentlige og private tjenesteudbydere.
 - Vejledninger, teknisk dokumentation, testmiljø mv.
- **Digitaliseringsstyrelsens [implementeringssite](#)**
 - Relevant information om overgangen til MitID og NemLog-in.
 - Implementeringsværktøjer: Screeningsværktøj, ordbog, mv.
- **Nyhedsbreve**
 - Nyt om NemLog-in: [Tilmeld dig her](#)
 - Nyt om overgangen til NemLog-in3 og MitID: [Tilmeld dig her](#)
- **OIOSAML:** [Læs mere her](#)

