DIGITALISERINGSSTYRELSEN

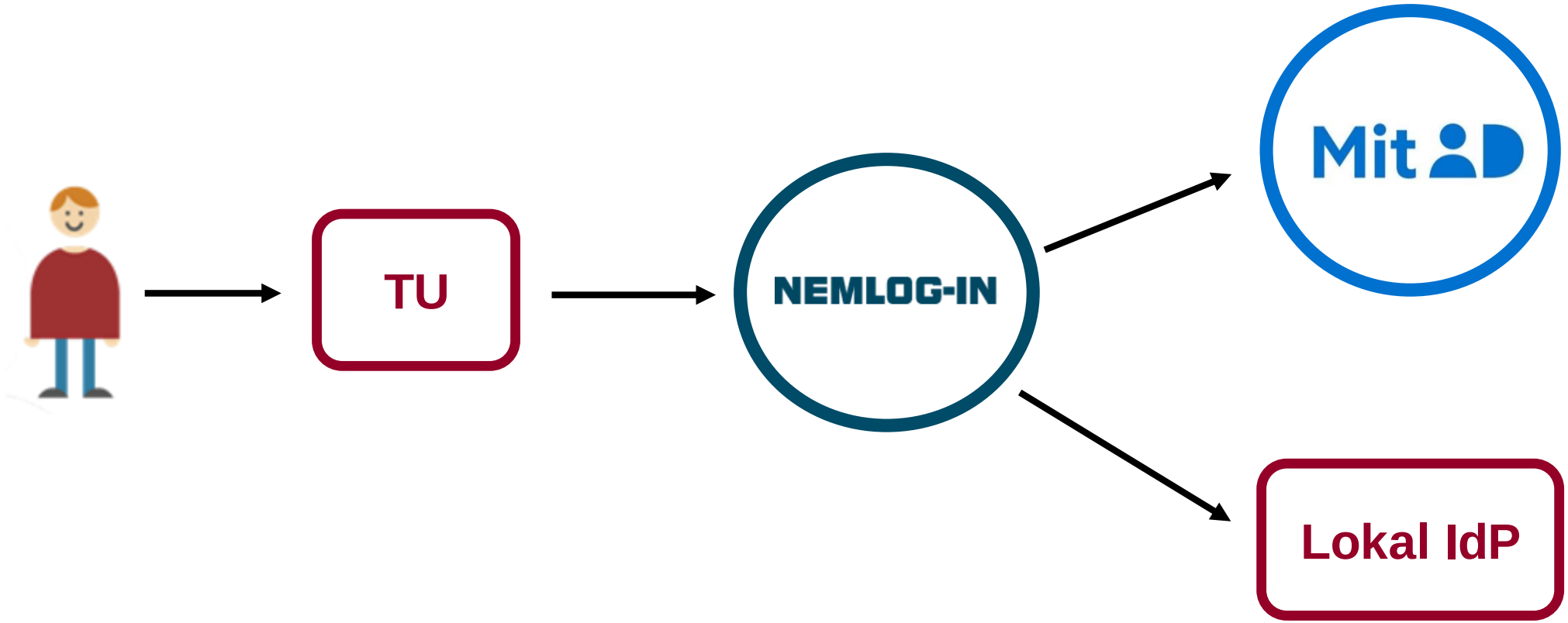
Lokal IdP

Februar 2020

Lokal IdP

- Lokal Signatur Server (LSS) udfases.
- Større brugerorganisationer kan vælge at etablere en Lokal IdP (identity provider) og administrere identifikationsmidler.
- For at kunne anvendes i den offentlige infrastruktur, skal en Lokal IdP anmeldes imod sit NSIS sikringsniveau og tilsluttes NemLog-in.
- Det kræver it-mæssig modenhed og kapacitet at implementere og vedligeholde en Lokal IdP.
- Med OIOSAML 3.0 er der også frigivet en Lokal IdP profil; se digitaliser.dk.

Lokal IdP i infrastrukturen



DIGITALISERINGSSTYRELSEN

Overvejelser omkring Lokal IdP

Øget fleksibilitet med Lokal IdP

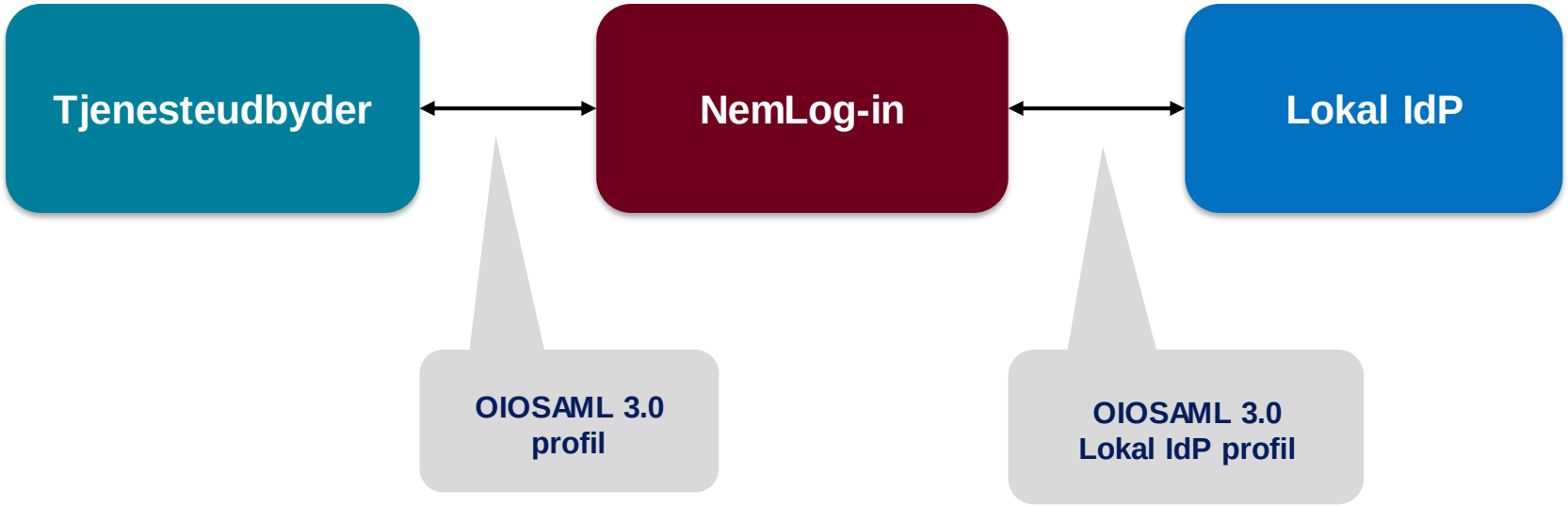
- Anvendelse af lokalt netværkspassword som den ene faktor.
- Lokal hjælp ved glemt password eller registrering af to-faktor enhed.
- Anvendelse af egne identifikationsmidler.
- Single sign on (SSO) oplevelse med egne it-miljøer.
- Mulighed for opkobling af lokal IdM løsning (brugeradministration) med NemLog-in

Ulemper ved Lokal IdP

- Høje sikkerhedskrav med revision og anmeldelse imod NSIS Betydelig.
- Øgede initiale investeringer og efterfølgende årlig revision.
- Organisationen skal selv vedligeholde egne identifikationsmidler.
- Dyrere og mere ressourcekrævende end anvendelse af MitID identifikationsmidler.

OIOSAML profil til lokal IdP

- NemLog-in er mellem en Lokal IdP og en tjenesteudbyder.
- Særlig profil af OIOSAML 3.0 målrettet lokale IdP'ers integration med en broker.
  - AuthnContextClassRef eller RelayState kan bruges til ekstra attributter



DIGITALISERINGSSTYRELSEN

Udvalgte krav til lokal IdP på niveau Betydelig

- Autentifikation - håndterer trusler mod kommunikationen (fx replay angreb)
- Organisation – erstatningsansvar og forsikring
- Drift – baggrundstjek af medarbejdere, adgangskontrol til driftslokaler, overvågning af betroede adgange i produktionssystemer.
- ISMS – ISMS skal **følge principperne** i ISO 27001
- Revisionserklæring fra statsautoriseret revisor + ledelseserklæring
- Sessionsstyring i IdP og best practice for token håndtering (kryptering), HSM ved national tjeneste

Udvalgte krav til lokal IdP på niveau Høj

Se forrige slide om niveau Betydelig, nedenstående angiver **skærpelser** hertil

- Drift – videoovervågning af driftslokaler, stærk perimeterbeskyttelse
- ISMS skal være **certificeret** efter ISO 27001 eller tilsvarende
- FIPS 140-2 level 3 certificeret HSM obligatorisk for IdP/broker, privat nøgle skal genereres i hardware

Anmeldelse af ID-tjenester og governance

- ID-tjenester skal anmeldes til DIGST, før de må benytte NSIS.
- Krav til dokumentation stiger med sikringsniveauet:
  - Lav: 'selvdeklarering'.
  - Betydelig og Høj: ISAE 3000 revisionserklæring fra uafhængig, statsautoriseret revisor.
  - Revision gentages årligt.
  - Derudover skal der afgives en ledelseserklæring.
- DIGST gennemgår anmeldelsen og publicerer denne inkl. sikringsniveau.
- DIGST kontrollerer formalia – revisor verificerer implementeringen.
- DIGST kan afmelde en ID-tjeneste, som ikke lever op til kravene.
- Til brug for anmeldelsen er der udarbejdet en række værktøjer bl.a.:
  - Revisionsvejledning med tilhørende Excel skema.
  - Revisor skal verificere samtlige krav i NSIS på det angivne sikringsniveau.
  - Anmeldelsesskabelon.

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

- **Lokal IdP:** Læs mere her

DIGITALISERINGSSTYRELSEN