DIGITALISERINGSSTYRELSEN

Webinar om det nye NemLog-in:

referenceimplementeringer, opslagstjenester, den nye signeringkomponent og erstatningen til PID/RID

14. maj 2020

Christian Schmidt-Madsen

It-arkitekt,

Digitaliseringsstyrelsen

Thomas Gundel

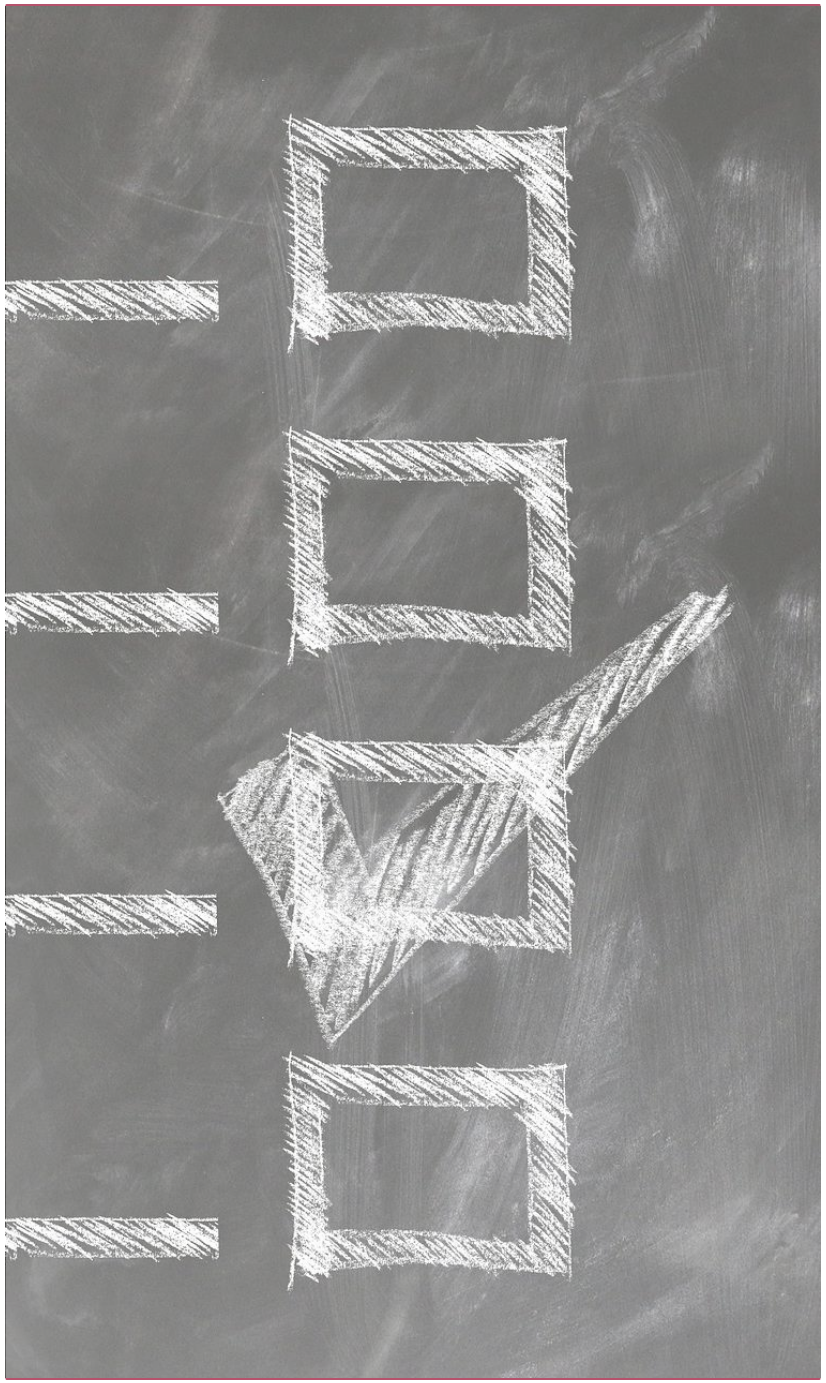
Ekstern konsulent,

Digitaliseringsstyrelsen

Thomas Mostrup Nymand

Løsningsarkitekt,

Nets



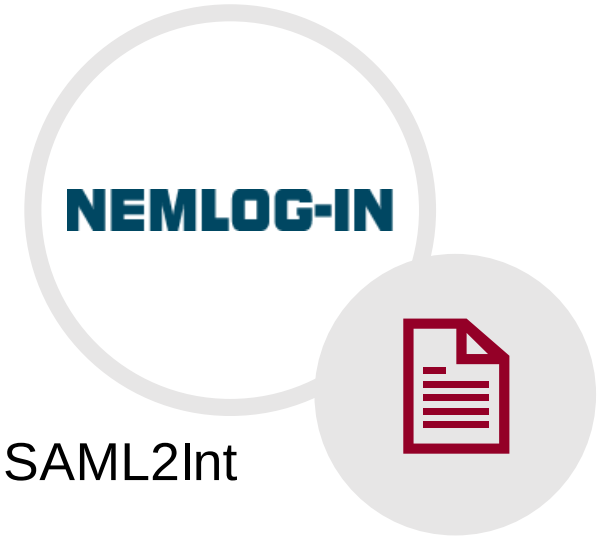
Dagsorden

- **OIOSAML referenceimplementeringer**
  - De vigtigste ændringer i version 3.0
  - Test-IdP
  - Testmiljø
- **Erstatningen til PID/RID: UUID**
  - Certifikater
  - UUID-typer
- **Opslagstjenester**
  - Eksisterende tjenester
  - Nye tjenester
- **Den nye signeringsløsning**
  - Sammenligning, ny og eksisterende løsning
  - Muligheder for tilpasning, migrering
- **Paralleldrift i migreringsperioden**
- **Det skal I gøre nu**
- **Spørgsmål**

DIGITALISERINGSSTYRELSEN

OIOSAML

Den nye OIOSAML 3.0 profil



- Snitfladen mod NemLog-in's IdP skifter fra OIOSAML 2.0.9 til 3.0.1.
- Begge end-points er aktive i en periode.
- OIOSAML 3.0.1 dokumentet følger en ny struktur med udgangspunkt i SAML2Int profilen fra Kantara Initiative:
  - Fokus på at adskille krav fra vejledning.
  - Profil afkobles fra identifikationsmidler (herunder PKI og OCES).
  - Mere privacy – UUID'er er de primære identifiers. Udgangspunktet er TU-specifikke identifiers.
  - Tidssvarende krav til algoritmer og nøglelængder.
  - Håndtering af 'levels of assurance' i henhold til NSIS.

DIGITALISERINGSSTYRELSEN

Vigtigste nyheder for tjenesteudbydere

1. Man kan efterspørge et bestemt NSIS sikringsniveau i SAML AuthnReq

- Low, Substantial, High

2. Man kan efterspørge en bestemt attributprofil

- Person
- Professionel

3. Man skal forholde sig til NSIS sikringsniveau i modtaget Assertion

- OBS: Ingen garanti for, at brugerne er logget ind på det niveau, som man efterspørger!
- OBS: Husk at frasortere NSIS Low, hvis man ikke er interesseret i dette!

4. Reviderede attributsæt for brugerne

- To attributprofiler defineret: én for personer og én for professionelle (en del fælles attributter).
- Sikringsniveau følger nu NSIS, mulighed for IAL og AAL.
- PID og RID videreføres i en overgangsperiode, men erstattes med UUID.
- UUID er generelt tjenesteudbyder-specifikke af privacy-hensyn.
- OCES-specifikke attributter udgår.

Fælles attributter (person og professionel)

- https://data.gov.dk/model/core/specVersion
- https://data.gov.dk/model/core/eid/bootstrapToken
- https://data.gov.dk/model/core/eid/privilegesIntermediate
- https://data.gov.dk/concept/core/nsis/loa
- https://data.gov.dk/concept/core/nsis/ial
- https://data.gov.dk/concept/core/nsis/aal
- https://data.gov.dk/model/core/eid/fullName
- https://data.gov.dk/model/core/eid/firstName
- https://data.gov.dk/model/core/eid/lastName
- https://data.gov.dk/model/core/eid/alias
- https://data.gov.dk/model/core/eid/email
- https://data.gov.dk/model/core/eid/cprNumber
- https://data.gov.dk/model/core/eid/age
- https://data.gov.dk/model/core/eid/cprUuid

Attributter kun for personer

- https://data.gov.dk/model/core/eid/person/pid

DIGITALISERINGSSTYRELSEN

Attributter kun for professionelle

- https://data.gov.dk/model/core/eid/professional/uuid/persistent
- https://data.gov.dk/model/core/eid/professional/rid
- https://data.gov.dk/model/core/eid/professional/cvr
- https://data.gov.dk/model/core/eid/professional/orgName
- https://data.gov.dk/model/core/eid/professional/productionUnit
- https://data.gov.dk/model/core/eid/professional/seNumber
- https://data.gov.dk/model/core/eid/professional/authorizedToRepresent

Referenceimplementeringer

Digitaliseringsstyrelsen har fået udarbejdet open source referenceimplementeringer i Java og .NET

- Java: https://www.digitaliser.dk/resource/5189721
- .NET: https://www.digitaliser.dk/resource/5246799

- Begge er udarbejdet som beta-versioner ud fra OIOSAML 3.0 specifikationen og er endnu ikke testet mod den nye NemLog-in løsning (IdP).
- Begge har en indbygget IdP til testformål, så man kan afvikle et flow på en udviklermaskine.
- Hensigten er at gøre det muligt for tjenesteudbydere at komme i gang med omstilling til OIOSAML 3.0 snitfladen tidligt.

Ofte stillede spørgsmål (Java)

Kan man bruge det gamle OIOSAML.java framework mod det nye NemLog-in?

- I princippet omend det ikke anbefales.
- Ingen validering af NSIS sikringsniveauer indbygget i det gamle framework, så man skal selv håndtere den del, hvis man ikke opdaterer til OIOSAML.java 2.2.0 eller nyere.
- Ingen understøttelse for de nye attributter, der udstedes af det nye NemLog-in, så dem skal man ligeledes selv håndtere, og det er ikke muligt at efterspørge en specifik profil og/eller andre af de funktioner, som det nye NemLog-in understøtter.

Kan man anvende det nye OIOSAML.java framework med nuværende NemLog-in?

- Ja - man kan roligt opdatere allerede nu, da OIOSAML.java 2.2.0 og nyere også fungerer fint med det eksisterende/gamle NemLog-in.

Ofte stillede spørgsmål (.NET)

Er .NET Core understøttet?

- Ikke endnu – men ønsket er noteret!

Hvad sker der, hvis en bruger logger ind på OIOSAML 3.0 endpoint med et NemID?

- Hvis brugerens NemID er på NSIS Betydelig, sendes dette tilbage i Assertion.
- Hvis brugerens NemID ikke er på NSIS Betydelig, sendes den gamle LoA attribut fra OIOSAML 2.0.9.

Hvilke af de tre modeller i OIO Basic Privilege Profile er understøttet af NemLog-in?

- Ved go-live er det kun model 2, som er understøttet. Constraints (dataafgrænsninger) er i pipeline, men der er ingen officiel dato endnu.

Testmiljøer

- NemLog-in's eksisterende integrationstestmiljø og IdP på https://test-nemlog-in.dk bliver først opdateret tæt på go-live af det nye NemLog-in.
- Forinden bliver der etableret et nyt testmiljø:
  - https://devtest4-nemlog-in.dk
- Her kan tjenesteudbydere teste:
  - Integration til NemLog-in med OIOSAML 3, herunder step-up.
  - Dog uden MitID og Lokal IdP-integration.
  - Den nye NemLog-in signeringsløsning (mere herom senere).
  - Den opdaterede STS.
- Forventet tilgængeligt september/oktober 2020.

Erstatningen til PID/RID

Erstatning af PID/RID

- De velkendte PID/RID numre er snævert knyttet til de gamle OCES certifikater - disse udfases.
- Ved at tilbyde ikke-globale UUID'er gøres det muligt at designe mere privatlivsvenlige løsninger.
- PID og RID erstattes af UUID'er:
  - i SAML-billetter
  - i certifikater (OCES og kvalificerede*).
- UUID**-syntax: 32 hexadecimale cifre i 5 grupper adskilt af '-', fx:

```
e914151e-1334-4ff5-93d2-424763f82e25
```

* Til dannelse af kvalificerede signaturer og segl, mere herom senere.
** UUID: Universally Unique Identifier

Nye certifikater

Den nye løsning understøtter OCES og kvalificerede certifikater, som erstatter NemID OCES2 certifikaterne:

Certifikatholder	OCES	Kvalificerede langtidscertifikater	Kvalificerede korttidscertifikater
Person	-	-	X
Medarbejder	X	X	X
Organisation	X	X	X

- Korttidscertifikater udstedes kun ved anvendelse af den nye signeringskomponent.
- OCES og kvalificerede certifikater bestilles og udstedes i NemLog-ins nye erhvervsløsning.
- Der kræves særskilt godkendelse, før en organisation kan benytte kvalificerede certifikater i den nye erhvervsløsning.
- Brugercertifikater kan *ikke* anvendes direkte til log-in i NemLog-in, kun indirekte via lokal IdP.

Navne i de nye certifikater

De nye certifikaters navnestruktur (SubjectDN) er ændret:

Brugercertifikat (tidligere MOCES)	Anonym brugers certifikat	OCES organisationscertifikat (tidligere VOCES)
cn=Peter Flemming Hansen, gn=Peter Flemming, sn=Hansen, serialNumber=UI:DK-5d7d6819-…, o=Digitaliseringsstyrelsen, organizationIdentifier=VATDK-34051178, c=DK	cn=Pseudonym, pseudonym=Pseudonym, serialNumber=UI:DK-5d7d6819-…, o=Digitaliseringsstyrelsen, organizationIdentifier=VATDK-34051178, c=DK	cn=Fællespostkasse, serialNumber=UI:DK-5d7d6819-…, o=Digitaliseringsstyrelsen, organizationIdentifier=VATDK-29915938, c=DK

- Tidligere indeholdt subjectSerialNumber PID, CVR+RID, CVR+UID, CVR+FID
- Disse erstattes med et UUID
- Bemærk, at UUID og dermed SubjectDN *kan* ændres ved fornyelse, men sammenhæng imellem certifikat-UUID og medarbejderidentitetens UUID kan kontrolleres med UUID-match.

UUID-typer og deres anvendelse

UUID'er klassificeres ift. graden af privatlivsvenlighed

Type	Egenskaber	SAML-anvendelse	Certifikatanvendelse
Global	Persistent og global. Som RID/PID.	Medarbejder: Persistent Identifier attribut Person: CPR-UUID attribut	Alle
Tjenesteudbyder-specifik	Hver tjenesteudbyder oplever egen identifikator	Persistent Subject NameID	Kvalificerede korttidscertifikater (signering)
Certifikat-specifik	Hvert udstedt certifikat udstyres med nyt UUID. Også ved fornyelse.	-	Kvalificerede langtidscertifikater og OCES til medarbejdere og organisationer.
Sessions-specifik	Hver session tildeles nyt UUID. Hvert korttidscertifikat tildeles nyt UUID.	Transient Subject NameID	Kvalificerede korttidscertifikater (signering)

Opslagstjenester

Eksisterende opslagstjenester

NemID PID-CPR og NemID RID-CPR
- Begge videreføres i NemLog-in (ny snitflade).

NemLog-in AttributeQuery
- Videreføres og udbygges med understøttelse for nye OIOSAML 3.0 attributter.

NemID PID-CPR-match
- Udfases med NemID (*).
- Erstattes af adgang til CPR eller CPR-UUID i SAML-billet med brugersamtykke.

WhoIsLRA og IsLRA
- Udfases med NemID (*).

(*) Der er ikke truffet beslutning om hvornår NemID tages ud af drift. Det sker dog tidligst ved udgangen af 2021.

Nye opslagstjenester

Generelt ønskes privatlivsvenlige løsninger, hvor bruger kontrollerer afgivelse af personoplysninger. Derfor udbydes ikke stærke/generelle opslagstjenester, hvor en brugercentrisk, privatlivsvenlig løsningsmodel er mulig.

Løsningen tilbyder tre nye opslagstjenester:

1. UUID->RID
- UUID fra langtidsbrugercertifikat (MOCES eller kvalificeret).
- Ingen tilsvarende tjeneste for PID, men PID kan udleveres i SAML billet ved behov.

2. UUID->CPR-UUID
- UUID fra langtidsbrugercertifikat (MOCES eller kvalificeret).
- Svarer til RID->CPR.

3. UUID-match
- ”Givet to forskellige UUID, udpeger disse samme identitet?”
- Fx UUID fra SAML-billet og UUID fra signeringscertifikat.
- Borger eller medarbejder.

Brugsscenarier

Opslagstjenesterne understøtter migrering og brugsscenarier for dokumentsignering.

Eksempler:

TU har registreret brugerkonti til PID eller CVR+RID

- Tjeneste modtager RID i SAML-billet (ellers er der tale om en ny bruger).
- Herefter omregistreres brugerkonto til TU-specifikt UUID (persistent SAML-subjekt).
- Hvis tjeneste har brugerkonti registreret til PID, forespørges PID i SAML-billet og foretager tilsvarende omregistrering.

Tjeneste, der bruger lokal certifikatautentifikation eller lokal signering

- Tjeneste modtager signerede data, signeret med nyt brugercertifikat (tidl. MOCES).
- Tjeneste forespørger herefter **UUID->RID.**
- Hvis RID findes, omregistreres konto til brugercertifikat-UUID. Findes RID ikke ved opslag, er der tale om en ny bruger.

Udskiftning af VOCES/FOCES med nye organisations- og systemcertifikater

- Behov for genregistrering af autorisation, idet UID/FID ikke migreres til NemLog-in.

Den nye signeringsløsning

NemLog-in signeringsløsning

- NemLog-ins nye signeringsløsning tilbyder dannelse af kvalificerede signaturer.
- Kvalificerede signaturer har samme retsvirkning som en håndskrevet underskrift i hele EU (jf. eIDAS Artikel 25).
- Signering foregår centralt i NemLog-in, uafhængigt af om der anvendes identifikationsmidler fra MitID, Lokal IdP eller (overgangsperiode) NemID (ikke nøglefil).
- Signeringskomponenten er privatlivsvenlig, idet kun signeringsklienten (JavaScript) har adgang til dokumentet.
- Signaturerne indeholder kryptografisk tidsstempel og certifikatstatus (OCSP), dvs. integreret signaturbevis.
- Som noget nyt tilbydes mulighed for segldannelse, dvs. signering med organisationscertifikater.
- Nye EU-standardiserede output-formater: **XAdES** – XML eller **PAdES** – PDF.
- Løsning er bagudkompatibel mht. input-formater, så man kan fortsat signere samme formater.

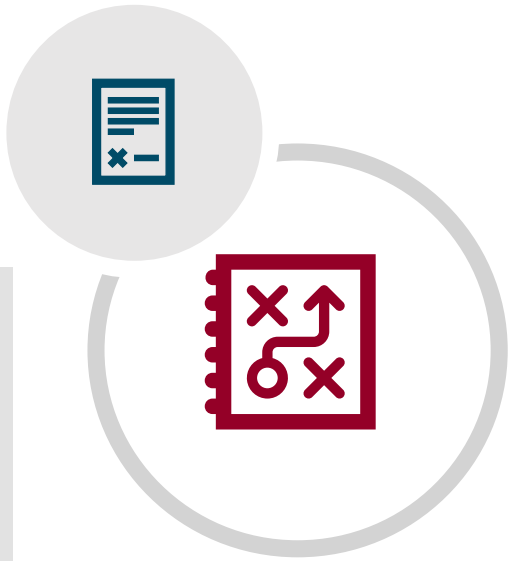
NemLog-in og NemID signering, tekniske egenskaber

Egenskab	NemID-signering	NemLog-in signering
Identifikationsmidler	NemID	Alle accepterede identifikationsmidler i NemLog-in (NSIS Betydelig)
Brugeroplevelse	iframe	iframe og godkendelse
Input	Tekst, HTML, PDF eller XML	Tekst, HTML, PDF eller XML
Outputformat	OpenSign (XML-Dsig)	XAdES eller PAdES (vælges uafhængigt af input). Kryptografisk tidsstempel indeholdt.
Signeringscertifikater	POCES2 eller MOCES2	Automatisk udstedte kvalificerede korttidscertifikater til person, medarbejder eller organisation, alene anvendt ved signering.
Validering	Lokalt hos TU (TU-pakken eller tilsvarende)	Valideringswebservice (API) eller lokalt (DSS-biblioteket)
Værktøjer	TU-pakken (Java og C#)	SignSDK (Java og C#)

DSS: EUs referenceimplementering. https://github.com/esig/dss

Tilpasning af signeringsflow

Tjenesteudbyder kan tilpasse det enkelte signeringsflow bl.a. ift. følgende:



Underskriver

- Person/medarbejder/organisation.
- Angivelse af specifik underskriver – fx den bruger, der er logget ind.
- Alderskrav – fx for at sikre, at underskriver er fyldt 18 år.

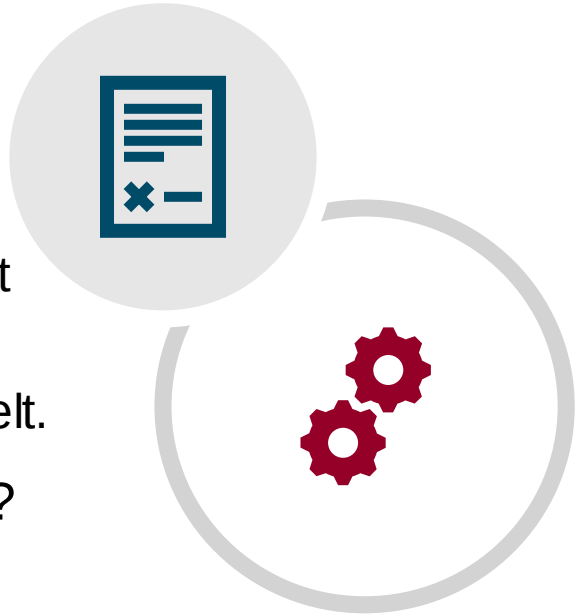
Privatlivsbeskyttelse

- Skal underskrivers navn angives i certifikat?
- Ønsket UUID-type i signeringscertifikat
  - Dvs. global, tjenesteudbyder-specifik eller sessionsspecifik
  - Efterfølgende identitetskontrol vha. UUID-match.

Værktøjer

- SignSDK til hjælp for TU – tilbyder i Java og C#.
- Indeholder referenceimplementering/demo-applikation.

Input til migrering fra NemID signering



- Valg af outputformat:
  - XAdES er også signeret XML (XML-Dsig), migrering vil formentlig være enklest ved valg af dette format.
  - PAdES-dokumenter kan åbnes i PDF-læser, og signatur kan identificeres visuelt.
- Hvordan identificeres underskriver, når der ikke er PID/RID i dokumentet?

  Eksempel:
  - Bruger logger ind, tjeneste A modtager TU-specifikt UUID i SAML-billet.
  - Bruger signerer dokument i NemLog-in signeringsløsning.
  - Tjeneste A bekræfter, at UUID fra signeringscertifikat og UUID fra SAML-billet udpeger bruger ved opslag i UUID-match-tjenesten.
  - Bruger logger på tjeneste B, tjeneste modtager TU-specifikt UUID i SAML-billet.
  - Bruger uploader dokument signeret hos tjeneste A.
  - Tjeneste B bekræfter, at UUID fra signeringscertifikat og tjeneste-B specifikt UUID fra SAML-billet udpeger bruger - også ved opslag i UUID-match.

Paralleldrift i migreringsperioden

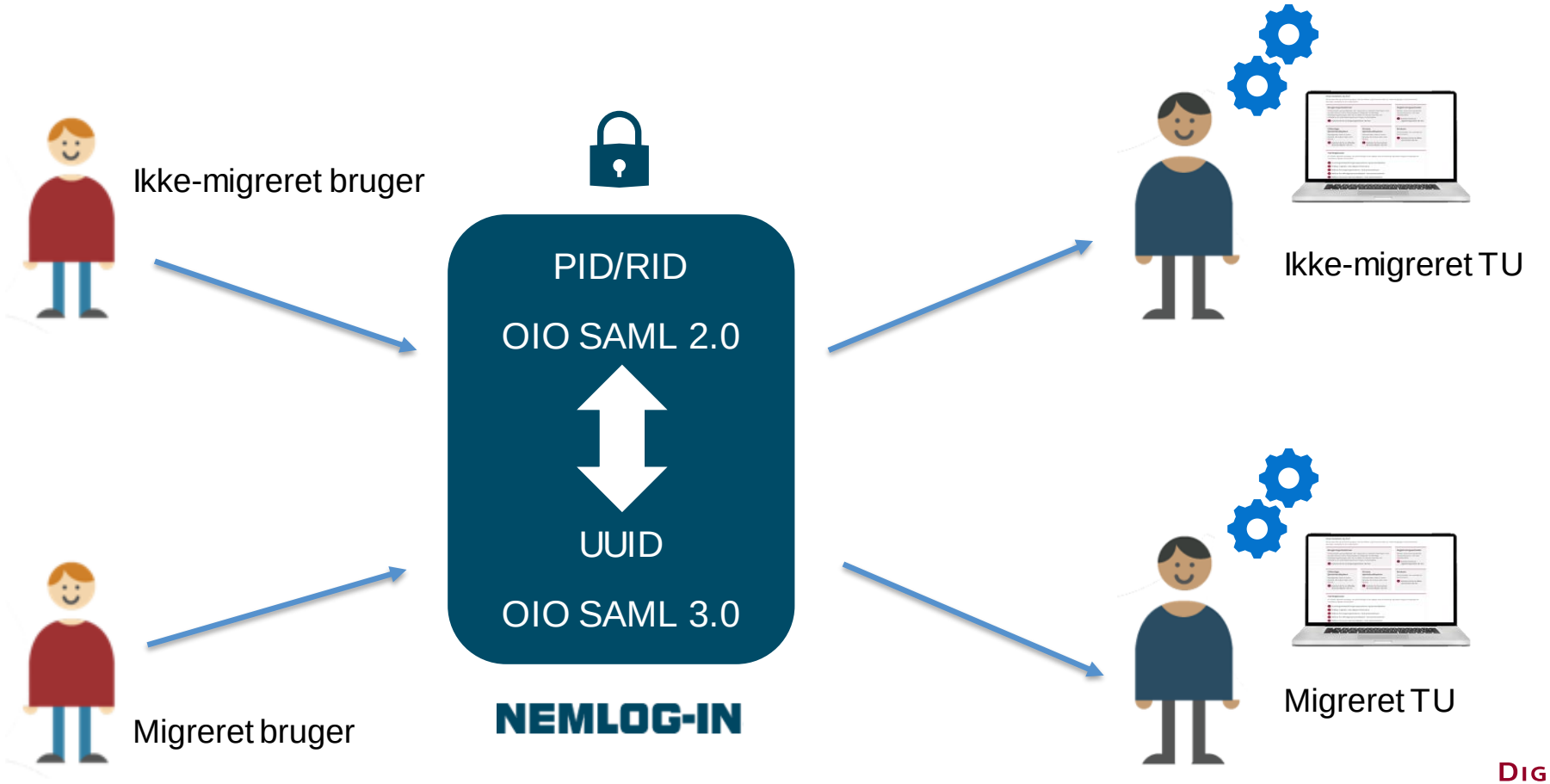
Paralleldrift i migreringsperioden

- NemID og MitID kører i paralleldrift.
- Tjenesteudbydere bør understøtte både NemID, MitID og de nye NemLog-in erhvervsidentiteter fra begyndelsen af migreringsperioden, da der hurtigt kan komme brugere, som ikke har NemID.

- Gamle tjenester, der ikke er klar til nye identiteter.
- Nye tjenester, der ikke understøtter gamle identiteter.

NemLog-in bro i migreringsperioden

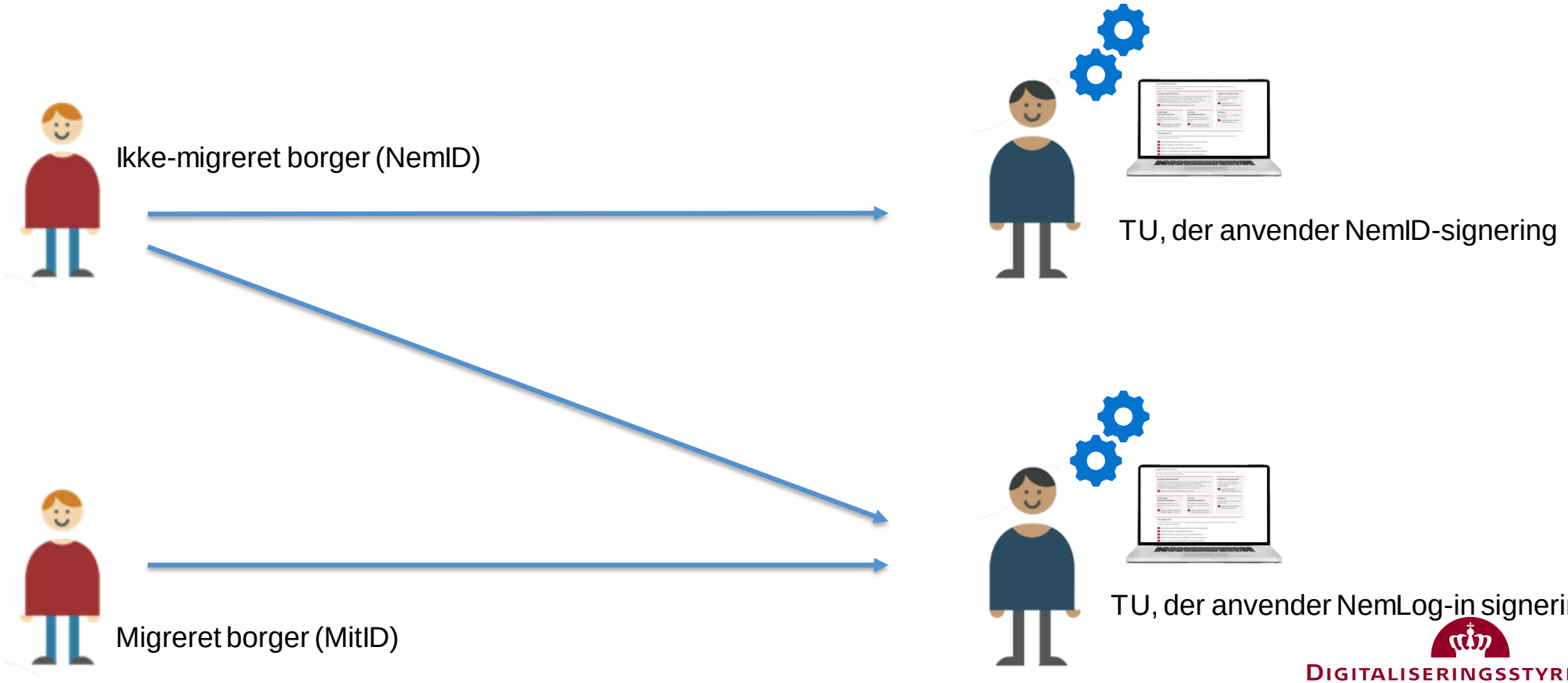
Vi skal sikre, at alle brugere kan anvende alle tjenester – hele tiden!



DIGITALISERINGSSTYRELSEN

Signering i migreringsperioden - borgere

NemID-signeringsløsninger kan kun anvende NemID (nøglekort/nøglefil).



DIGITALISERINGSSTYRELSEN

Signering i migreringsperioden - medarbejdere

NemLog-in-signering understøtter ikke NemID erhverv.

Ikke-migreret medarbejder (NemID erhverv)

TU, der anvender NemID-signering

Migreret medarbejder (privat NemID/MitID/lokal IdP)

TU, der anvender NemLog-in signering

DIGITALISERINGSSTYRELSEN

Det skal I gøre nu

Migreringsforløb for tjenesteudbyder

Vil jeg gøre brug af nye NSIS niveauer, eller er Betydelig fint for mig?

Bruger jeg lokal(e) signering/certifikater og har brug for UUID->RID-opslag?

Vælg evt. input- og outputformater i min signeringsløsning.

Design af OIOSAML 3.0 understøttelse – herunder evt. brugerkonti-migrering.

Udvikling af OIOSAML 3.0-understøttelse.

Tilslut tjeneste til NemLog-in testmiljø.

Gennemfør test og kvalitetssikring.

Flyt tjeneste til produktion.

DIGITALISERINGSSTYRELSEN

Det skal I gøre nu:

Planlæg migrering til den nye Signeringskomponent, og hold jer orienteret om information om denne

- Valg af input og outputformat.
- Tag stilling til nye muligheder med segldannelse.

Forbered ibrugtagning af NSIS-standarden

- Hvilket sikringsniveau skal mine tjenester kræve?
- Kan min tjeneste/mine brugere få gavn af Lav/Høj sikringsniveauerne?

Hold jer orienterede ift. OIOSAML referenceimplementeringer og testmiljø

- Referenceimplementeringer er tilgængelige nu.
- Testmiljø forventes tilgængeligt september/oktober.

Tag stilling til omfanget af betydning af, at PID/RID på sigt udfases

- Har jeg lokale løsninger, der anvender certifikat-autentifikation eller lokal signering? Kan brugerkonti ”standardmigreres”? (slide 15).

Hold jer orienterede om UUID API’er, og orienter jer omkring ændret brug af certifikater

- Dokumentation for UUID->RID og UUID-match tilgængelig ultimo maj.

Links til hjemmesider, vejledninger og dokumentation

- Se og læs mere på den nye NemLog-in portal: www.nemlog-in.dk
- Tilmeld dig NemLog-in nyhedsbrev og få nyheder samt løbende information om det nye NemLog-in, der er relevant for dig og din virksomhed/myndighed. Tilmelding via NemLog-in portalen.
- Se og læs mere på vores NemLog-in og MitID implementeringssite: www.digst.dk/it-loesninger/implementeringssite
- Læs mere om det nye NemLog-in: https://migrering.nemlog-in.dk/om-nemlog-in/
- Læs mere om NSIS: https://migrering.nemlog-in.dk/nemlog-in-broker/offentlig-tjenesteudbyder/nsis/
- Læs mere om OIO SAML standarden: https://migrering.nemlog-in.dk/nemlog-in-broker/offentlig-tjenesteudbyder/oiosaml-3-0-1/
- Læs mere om de nye certifikatpolitikker: https://migrering.nemlog-in.dk/nemlog-in-broker/offentlig-tjenesteudbyder/certifikater/
- Se tidligere afholdte webinarer og infovideoer om NSIS, Lokal IdP og OIOSAML: https://migrering.nemlog-in.dk/kontakt-og-support/infovideoer-og-webinarer/

Spørgsmål

DIGITALISERINGSSTYRELSEN

Tak for i dag

Christian Schmidt-Madsen

It-arkitekt,

Digitaliseringsstyrelsen

Thomas Gundel

Ekstern konsulent,

Digitaliseringsstyrelsen

Thomas Mostrup Nymand

Løsningsarkitekt,

Nets