DIGITALISERINGSSTYRELSEN

# Fremtidens infrastruktur for digitale identiteter i Danmark

I løbet af den kommende årrække bliver Danmarks digitale infrastruktur bygget op på ny.

Ultimo 2017 offentliggøres parallelle udbud for næste generation af NemID (MitID) og NemLog-in (NemLog-in3). Noget videreføres, mens andet laves helt om. Visionen på tværs af udbuddene er at skabe langsigtede løsninger med høj grad af fleksibilitet og gode brugeroplevelser. Læs her om de store linjer for de løsninger, der vil komme til at forme landets fremtidige infrastruktur for digitale identiteter, signering og brugerrettighedsstyring.

**Indhold**



## MitID-udbuddet

*Baggrund*
Digitaliseringsstyrelsen og Finans Danmark har via datterselskabet "FR1 AF 16. SEPTEMBER 2015 A/S" (herefter kaldt FR1) indgået et partnerskab om fælles udvikling og drift af MitID, som er en ny, central identitetsgarant for digitale personidentiteter. Løsningen bliver sendt i EU-udbud i slutningen af 2017 og skal erstatte NemID.

MitID vil bygge på én fælles identitetskerne. Denne kerne vil kunne benyttes af både offentlige aktører, banker og andre private tjenesteudbydere med behov for sikre, digitale personidentiteter. Et af hovedmålene er, at alle personidentiteter i kernen som udgangspunkt kan benyttes på tværs af sektorer og tjenesteudbydere, uanset hvilken aktør der har registreret og indrulleret den pågældende person.

*Scope*
Den finansielle og den offentlige sektor har forskellige ønsker til, hvad løsningen skal kunne håndtere, fx inden for autorisation, fuldmagt, dokumentsignering og transaktionsgodkendelse. MitID-udbuddet vil derfor fokusere på de dele af den fremtidige identitetsløsning, hvor de to sektorer har fælles behov. De øvrige elementer vil blive udviklet separat af de enkelte parter.

Forgængeren NemID, der er drevet af Nets DanID A/S, består af to selvstændige dele: "bank-løsningen" og den offentlige, PKI-baserede "OCES-løsning". Den opdeling vil partnerskabet gøre op med. MitID-udbuddet vil fokusere på udvikling af en fælles identitets- og autentifikationsløsning med en identitetskerne, der understøtter autentifikation og livscyklushåndtering af digitale personidentiteter. Livscyklushåndtering indbefatter proces- og systemunderstøttelse for fx registrering, indrullering, opdatering og spærring af personidentiteter og akkreditiver (login-midler).

Til brugerne skal der udvikles et sæt standardakkreditiver, som skal kunne udvides løbende i takt med den generelle teknologiske og forretningsmæssige udvikling. Som minimum kommer der en

DIGITALISERINGSSTYRELSEN

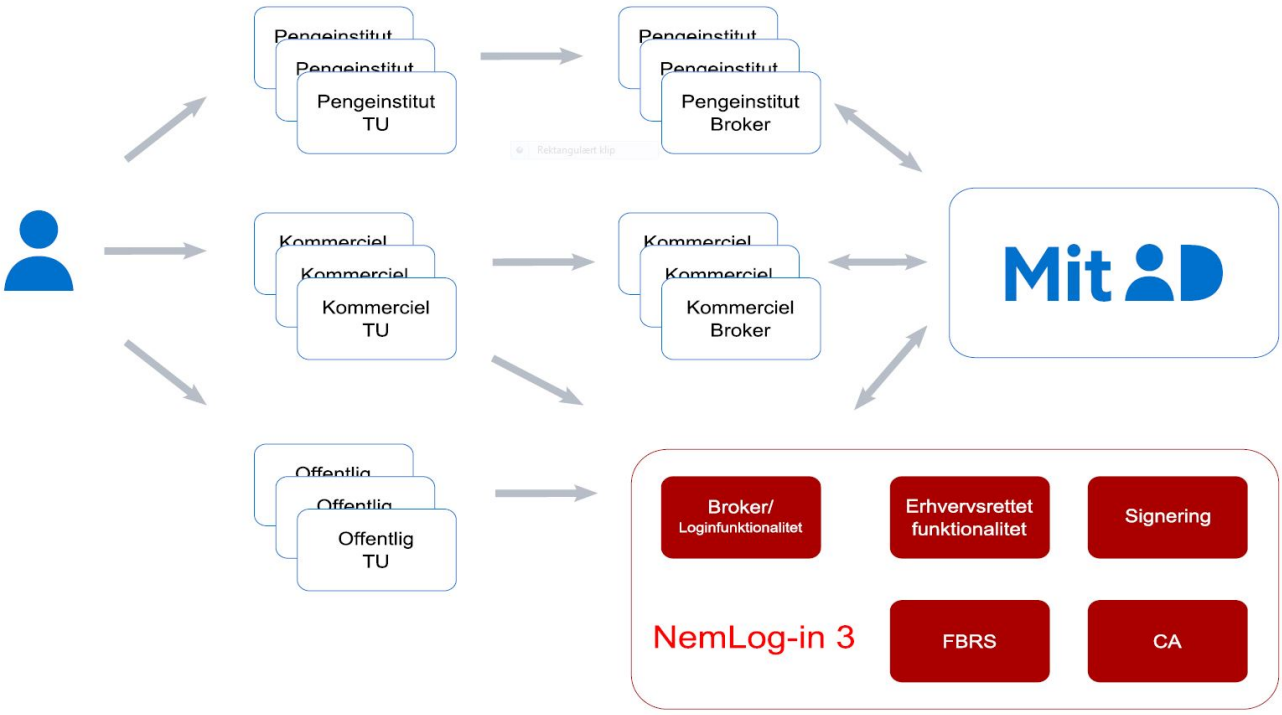
smartphonebaseret autentifikationsfaktor, en passwordbaseret autentifikationsfaktor og en fysisk autentifikationsfaktor til erstatning af NemID-nøglekortet. Der vil også være krav om akkreditivunderstøttelse af særlige behov, fx hos frekvente brugere, der skal autentificere sig mange gange om dagen, og brugere med handicap.

Overgangen fra NemID til MitID vil betyde en række ændringer i infrastrukturen:

- MitID-personidentiteter er ikke længere nødvendigvis certifikatbaserede (PKI).
- Dokument- og transaktionssignering er ikke en del af MitID-kernen, men håndteres individuelt af MitID-aftageres egne løsninger.
- En ny løsning til erstatning af NemID's identitetsgarant for medarbejderidentiteter (NemID Medarbejdersignatur) er ikke en del af MitID-kernen, men vil blive udbudt af Digitaliseringsstyrelsen som et delprojekt under NemLog-in3-udbuddet.
- MitID-kernen skal udvikles, så eksterne parter, såkaldte "identitetsbrokere" (brokere), kan lave deres egne klientløsninger med slutbruger-autentifikation via MitID-kernen.

*Obligatorisk brug af identitetsbrokere*

I MitID infrastrukturen vil det som udgangspunkt ikke længere være muligt for almindelige tjenesteudbydere (TU) at tilslutte sig kernen direkte. I stedet skal de gå igennem en certificeret identitetsbroker, der håndterer selve autentifikationsprocessen af slutbrugeren og den underliggende tekniske integration til kernen. Brokeren agerer som proxy identitetsgarant mellem TU og MitID og udsteder sin egen autentifikationsbillet til TU i fx SAML-format. Alternativt kan TU selv indgå en brokeraftale med MitID, hvilket dog vil indebære væsentligt skærpede sikkerhedskrav sammenlignet med eksempelvis den eksisterende NemID-tjenesteudbyderaftale.



DIGITALISERINGSSTYRELSEN

I den eksisterende identitetsinfrastruktur er offentlige tjenesteudbydere for langt størstedelens vedkommende tilsluttet NemID-løsningen via den fællesoffentlige login-portal/identitetsbroker, NemLog-in, ligesom en række private TU benytter tilsvarende kommercielle løsninger i stedet for selv at implementere NemID-klienten i deres egne onlineløsninger via den såkaldte "NemID TU-pakke".

En af de store fordele ved broker-modellen er, at den enkelte TU slipper for at forholde sig til den tekniske integration til den bagvedliggende identitetsgarant. I stedet kan de koble op hos den valgte broker mod en ofte simplere snitflade, der typisk er baseret på internationale, åbne standarder. Dette betyder samtidig, at det kun er broker-aktører, der behøver at forholde sig til ændringer i fx MitID-snitflader og sikkerhedsprocedurer.

Det forventes, at der vil blive tre forskellige kategorier af identitetsbrokere, der vil betjene TU i forskellige sektorer. Dels brokere til den offentlige sektor (NemLog-in samt evt. andre), dels brokere til enkeltbanker eller bank-datacentraler, og endelig kommercielle brokere til TU fra andre dele af den private sektor. Kernen stiller en klient[1] til rådighed for brokerne, men hver broker har mulighed for at implementere sin egen klient til autentifikation via kernen og kan dermed udvide eller tilpasse funktionaliteten efter behov.

*EU-regulering*
Et af de områder, der har udviklet sig væsentligt siden introduktionen af NemID, er den EU-lovgivning, der regulerer området.

**eIDAS-forordningen**
For den offentlige sektor er det især eIDAS-forordningen, der har betydning. Her defineres krav og standarder til de nationale, offentlige selvbetjeningsløsninger, der muliggør brug af digitale identiteter på tværs af EU's medlemslande. Fra 18. september 2018 er offentlige TU i alle EU-lande forpligtet til at modtage og anerkende officielle, digitale identiteter fra andre EU-lande på linje med landets egne digitale identiteter.

Danmark forventer at anmelde MitID som national eID-løsning, så identiteter herfra anerkendes på tværs af EU. Digitaliseringsstyrelsen har udarbejdet en National Standard for Identiteters Sikringsniveau (NSIS), der definerer de krav, der skal gælde for danske eID-løsninger, så de lever op til eIDAS' tre sikringsniveauer (eller LoA - Level of Assurance) for digitale identiteter. Fremover skal alle offentlige TU, brokere og identitetsløsninger, der skal benytte den nationale infrastruktur, forholde sig til denne standard, når de udvikler nye tjenester. De data, som kan tilgås via disse tjenester, skal være beskyttet med autentifikation på et tilstrækkeligt højt sikringsniveau.

**Betalingstjenesteloven**
For den finansielle sektor indføres fra 2018 en række nye krav med det reviderede betalingstjenestedirektiv (også kaldet PSD2). Direktivet stiller bl.a. detaljerede krav til, hvordan autentifikation og transaktionsgodkendelse skal foretages i forbindelse med udbud af betalingstjenester, fx betalinger via netbank. Parterne bag FR1 vil alle skulle leve op til disse regler gennem den danske lovgivning i "revideret lov om betalinger", der træder i kraft 1. januar 2018. MitID skal understøtte disse regulatoriske krav.

[1] Klient skal forstås som den del af MitID, der præsenterer en login-prompt for slutbrugerne og håndterer kommunikationen med MitID-kernen.

DIGITALISERINGSSTYRELSEN

**Persondataforordningen**
Fra 2018 træder en ny persondataforordning (også kaldet GDPR) i kraft. Den vil få indvirkning på alle offentlige og private tjenester, der håndterer persondata, dvs. også MitID. Persondataforordningen er mere vidtgående i sine operationelle krav til aktørerne end den hidtidige regulering, og der er markant større sanktionsmuligheder.

*Registreringsautoriteter*
Personidentiteter vil blive registreret i MitID-kernen på nogenlunde samme måde som i dag. Mindre tilpasninger skal dog sikre, at registreringsprocesserne vil leve op til de krav, der er defineret i NSIS-standarden. Læs mere i Digitaliseringsstyrelsens NSIS-vejledning.

MitID skal understøtte registrering af personidentiteter op til det højeste NSIS-sikringsniveau (4/høj). Det forventes, at hovedparten af personidentiteterne fremover vil blive registreret på NSIS-sikringsniveau 3 (betydelig).

Ligesom i den eksisterende NemID-løsning vil der blive udpeget aktører, der vil agere som registreringsautoriteter (RA) med mulighed for at oprette nye personidentiteter i løsningen. Afhængigt af, hvilket sikringsniveau de enkelte registreringsautoriteter ønsker at registrere personidentiteter på, skal aktørerne leve op til en række krav.

De offentlige myndigheder, der virker som kontaktpunkter for borgere, fx kommunernes borgerservice, fængselsmyndigheder og flygtningemyndigheder, vil formentlig også fremover fungere som RA.

I forhold til slutbrugere, der skal bruge MitID i erhvervsmæssig sammenhæng, vil NemLogin3 tilbyde en registreringsportal som en del af den fremtidige erhvervsidentitetsløsning.

Private aktører kan også blive certificeret til at varetage rollen som RA op til et valgfrit NSIS-sikringsniveau (certificeringskravene vil afspejle det ønskede sikringsniveau). Det kunne fx være pengeinstitutter, der løser en tilsvarende opgave i det nuværende NemID, eller private aktører fra andre sektorer i samfundet.

MitID vil desuden kunne automatisere registreringsprocesser online, så slutbrugere selv kan registrere og indrullere sig på de lavere sikringsniveauer (op til NSIS-sikringsniveu 3) uden personligt fremmøde hos en RA.

*MitID i fællesoffentlig kontekst*
Med introduktionen af MitID er strategien fra offentlig side at fortsætte udviklingen i retning af en mere fleksibel og modulær arkitektur i den fællesoffentlige infrastruktur for digitale identiteter, signering og brugerrettighedsstyring.

Set fra en tjenesteudbydervinkel kommer NemLog-in-løsningen til at spille en endnu mere central rolle i den fremtidige infrastruktur, end den gør i dag. Dette skyldes bl.a., at NemLog-in i rollen som MitID-broker i fremtiden vil være det primære adgangspunkt til identitetsinfrastrukturen for offentlige tjenester.

Samtidig udvides NemLog-in-løsningen med en ny identitetsgarant og administrationsportal for erhvervsidentiteter som et supplement til MitID-kernen. Herved samles alle væsentlige dele af funktionaliteten omkring erhvervsidentiteter og administrationen heraffremover i NemLog-in. Målet

er at skabe en mere sammenhængende brugeroplevelse for erhvervsbrugere og administratorer i virksomheder. I fremtiden kan brugeradministration og rettighedsadministration varetages ét sted. Den fleksible og modulære infrastruktur, der specificeres for både MitID og NemLog-in giver samtidig bedre mulighed for at udnytte funktionalitet på tværs af de to løsninger. Et af de konkrete mål er at give erhvervsbrugere mulighed for at benytte samme typer af akkreditiver i en erhvervsmæssig kontekst, som de benytter med deres private personidentitet.

*MitID i den finansielle sektors kontekst*
Finans Danmark vil sammen med Digitaliseringsstyrelsen løfte opgaven med at sikre danskernes fremtidige digitale identitetsløsning. Finans Danmark er interesseorganisation for bank, realkredit og kapitalforvaltning i Danmark og varetager blandt andet sektor- og digitale infrastrukturprojekter på tværs af pengeinstitutterne i Danmark.

Den digitale udvikling i Danmark har i vid udstrækning været båret af en unik treenighed med veludviklede offentlige selvbetjeningsløsninger, en digital og sikker betalingsinfrastruktur samt en høj datakvalitet og sikkerhed for brugerne ved anvendelse af den CPR-bundne digitale identitet i form af NemID. Med introduktionen af MitID er det fortsat den finansielle sektors ønske at løfte denne samfundsopgave og gennem moderne, brugervenlige interfaces at vedblive at sikre hyppig, sikker anvendelse og udbredelse af danskernes digitale hverdag. Samtidig har MitID givet mulighed for at formalisere et eksisterende operationelt samarbejde, og FR1 deler den fællesoffentlige vision om en mere fleksibel og modulær arkitektur i den fællesoffentlige infrastruktur for derved at optimere ikke blot brugerrejsen, men i ligeså høj grad for at effektivisere den løbende udveksling af data mellem offentlige og private aktører.

Bankerne er parallelt med den fælles interesse i en digital infrastruktur garanter for en vedblivende konkurrencedygtig og moderne udvikling af broker-infrastrukturen op imod MitID. Forventeligt vil der i den finansielle sektor blive udviklet et antal brokerløsninger for at understøtte de bagvedliggende og til tider proprietære bankløsninger, hvor den individuelle kundeoplevelse fortsat vil variere fra bank til bank.

Afhængig af den konkrete kontekst vil de tekniske krav til autentifikationsprocessen derfor også variere fra brokerløsning til brokerløsning. Dette afspejles i MitID-arkitekturen ved at denne specificeres, så den giver mulighed for at kunne benyttes via flere forskellige anvendelsesmodeller med forskellige grader af fleksibilitet for de aktører, der agerer som identitetsbrokere i MitID-infrastrukturen.

*PKI/CA-funktionalitet*
Modsat den nuværende NemID-løsning vil der ikke blive stillet krav om, at MitID-kernen skal være baseret på certifikatbaserede (PKI) identiteter. OCES-certifikatporteføljen udgår ikke, men forventningen er, at politikkerne revideres og tilpasses de fremtidige behov. Dette betyder bl.a. at:

De fremtidige certifikatpolitikker (CP) i stedet for den nuværende DS-844-standard bliver baseret på den tilsvarende ETSI-standard (319 411).

Kravene til OCES person- og medarbejdercertifikater (POCES og MOCES) skærpes, så certifikaterne fremover vil bestå af kvalificerede certifikater i stedet for ikke-kvalificerede certifikater.

Der laves nye tilpassede certifikatpolitikker/certifikatprofiler for signering via engangscertifikater med MOCES /POCES.

DIGITALISERINGSSTYRELSEN

MOCES-infrastrukturen tilpasses, så der ikke længere er understøttelse for lokalt installerede nøglefiler i software på PC og lignende. MOCES vil kun understøtte decentrale løsninger, der tilbyder hardwarebaseret beskyttelse af privatnøgler, fx Central Signaturserver eller tilsvarende. Det sker for at sikre et ensartet betydeligt eller højt sikringsniveau for PKI-baseret autentifikation.

CP for FOCES og VOCES forventes at blive opdateret, så der understøttes RA-specifikke X.509 v3 attribute extensions.

*Migrering af brugere fra NemID til MitID*
Sammen med leverandøren af det kommende MitID skal der udarbejdes en plan for migrering af personidentiteter fra NemID til MitID. For at sikre en høj udbredelsesgrad af MitID og for at nedbringe mængden af besvær for den enkelte slutbruger, skal migreringsprocessen foregå så smidigt som muligt. Det forventes dog ikke, at alle eksisterende NemID-identiteter vil kunne overføres til MitID i forholdet én til én. Læs mere nedenfor om migrering af erhvervsidentiteter.

## NemLog-in3-udbuddet

*Baggrund*
NemLog-in spiller en central rolle i Danmarks digitale infrastruktur ved at gøre det muligt for danske borgere og virksomheder at logge ind på offentlige selvbetjeningsløsninger. Digitaliseringsstyrelsen ønsker at videreføre og videreudvikle NemLog-in, hvilket kræver, at løsningen sættes i ny-udbud, da kontrakten med den nuværende leverandør, NNIT, udløber i 2019 . Desuden skal der udvikles en løsning for erhvervsidentiteter i samarbejde med MitID.

NemLog-in3-projektet gennemføres via to udbud:

- Et udbud af drift
- Et udbud af udvikling og forvaltning.

Nedenfor omtales projektet samlet. Få et overblik over opdelingen mellem de to udbud på side 11.

*Overordnet scope*
NemLog-in videreføres og vil fortsat fungere i de roller, som den gør i dag. Den vil altså være den primære fælles identitetsbroker/IdP-løsning og integrationspunkt for offentlige TU og selvbetjeningsløsninger og tilbyde den samme række af services, som den gør i dag. Det er fx loginportal med Single-sign-on (SSO) funktionalitet, central brugerrettighedsstyring (FBRS), signeringstjeneste (inkl. signaturvalidering og evt. langtidsopbevaring), fuldmagtsfunktionalitet og Security Token Service (STS) funktionalitet.

Det forventes ikke, at der bliver ændret grundlæggende på den funktionalitet, NemLog-in allerede tilbyder i den eksisterende infrastruktur til offentlige TU. Til gengæld vil der ske en række udvidelser med ny funktionalitet samt tilpasninger af den eksisterende funktionalitet.

De største tilføjelser bliver:

- Der oprettes en ny løsning for erhvervsidentiteter, inkl. tilhørende administrationsportal for erhvervsidentiteter til erstatning for den OCES-baserede "NemID Medarbejdersignatur" løsning.

DIGITALISERINGSSTYRELSEN

- CA-funktionalitet (OCES), der i den nuværende infrastruktur leveres som en del af NemID, vil i fremtiden blive en del af scopet for NemLog-in3-udbuddet.
- Signeringsløsningen skal opgraderes og moderniseres væsentligt i forhold til nye signeringsstandarder mv.

En anden stor ændring bliver, at der vil blive åbnet for, at private TU skal kunne benytte dele af NemLog-in-løsningen.

I forhold til eksisterende komponenter kan nævnes bl.a. følgende ændringer:

- NemLog-in loginportalen skal opdateres, så den understøtter autentifikation via MitID.
- FBRS skal opdateres, så komponenten vil være bedre integreret med den fremtidige løsning for erhvervsidentiteter.
- Den nuværende fuldmagtskomponent skal opdateres, så den understøtter fremtidige behov og bliver mere brugervenlig.

Nedenfor følger en kort gennemgang af de væsentligste NemLog-in-komponenter, og hvordan deres rolle vil være i den fremtidige infrastruktur.

*Loginportal med Single Sign On*
NemLog-ins eksisterende loginportal vil blive opdateret, så den understøtter autentifikation via MitID. Det vil kun i mindre omfang påvirke eksisterende TU, da den nuværende SAML-snitflade så vidt muligt opretholdes. Enkelte attributter i den nuværende snitflade kan ikke opretholdes, da de er snævert knyttet til OCES-certifikater. NemLog-in bliver således en brokerløsning i forhold til MitID-infrastrukturen og vil fungere som det primære adgangspunkt for offentlige TU med uændret funktionalitet ift. Single Sign On (SSO). Derudover vil portalen også kunne benyttes af private TU til at blive tilsluttet MitID infrastrukturen.

Ud over private personidentiteter fra MitID vil loginportalen også understøtte autentifikation af erhvervsidentiteter. Afhængig af erhvervsbrugerens (og organisationens) præferencer vil erhvervsbrugeren enten kunne autentificere sig via en erhvervsidentitet, der er koblet til erhvervsbrugerens private MitID-akkreditiver, eller via dedikerede erhvervsakkreditiver. Sidstnævnte vil, som beskrevet nedenfor, enten kunne stamme fra MitID eller være MOCES PKI-baserede akkreditiver. Der indføres dermed en løsere kobling mellem erhvervsidentiteter og akkreditiver, end det er tilfældet nu, hvilket giver en mere fleksibel infrastruktur.

Såfremt brugeren har tilknyttet sine private MitID-akkreditiver til en eller flere erhvervsidentiteter, vil loginportalen håndtere, hvilken kontekst brugeren i den konkrete session skal agere i. Den SAML-autentifikationsbillet, der leveres videre til TU, kommer dermed til at være forskellig, afhængig af om brugeren vælger at agere som privatperson eller som medarbejder. Denne funktionalitet er fra marts 2017 allerede delvist implementeret i NemLog-in loginportalen i den såkaldte "NemID Privat til Erhverv"-løsning, hvor fuldt ansvarlige deltagere og andre personer med fulde tegningsrettigheder til en virksomhed har mulighed for at logge ind som medarbejder med deres private NemID.

Der er på sigt planer om, at NemLog-in kan agere som broker for lokale Identity Providers (idP) – reguleret inden for rammerne af NSIS-standarden. Dette tænkes realiseret ved, at der åbnes for føderering mellem NemLog-in og andre IdP'er. Herved opnås på sigt mulighed for autentifikation med andet end MitID-akkreditiver – fx akkreditiver udstedt lokalt i en organisation, der har sin egen Identity Provider.

DIGITALISERINGSSTYRELSEN

*Signering i den fremtidige infrastruktur*
Der skal udvikles en signeringskomponent baseret på CEN-standarden for Remote Signing (CEN EN 419 241), der forventes publiceret i slutningen af 2017. Komponenten vil blive bygget som en del af NemLog-in3-udbuddet, så den bedst muligt kan integreres med den signeringsservice, der allerede findes i NemLog-in.

Signering vil basere sig på slutbrugerautentifikation via MitID-kernen eller anden identitetsgarant, fx NemLogin3 for erhvervsidentiteter. Komponenten forventes at understøtte signaturformaterne PAdES og XAdES, samt evt. andre efterspurgte signeringsdokumentformater. Den vil til forskel fra den nuværende løsning være baseret på kvalificerede engangscertifikater, der vil blive udstedt af infrastrukturens CA-komponent. Ved at anvende kvalificerede certifikater i signeringstjenesten opnås den fordel at kommercielle de facto standardprodukter, som fx Adobe PDF Reader, vil kunne verificere validiteten af signerede dokumenter direkte, uden at der skal benyttes særlige værktøjer hertil.

*Den fremtidige erhvervsløsning*
Til erstatning for NemID Medarbejdersignatur vil der i NemLog-in3 blive oprettet en helt ny identitetsgarant til erhvervsbrugere.

Denne erhvervsidentitetsgarant vil håndtere den fulde livscyklus for erhvervsidentiteter og blive designet, så den kan integreres med MitID, hvor det er relevant.

Erhvervsløsningen vil tilbyde fire former for akkreditiver til en erhvervsidentitet:

1. Automatisk kobling mellem privat personidentitet/akkreditiv og virksomheder, hvor personen kan tegne virksomheden alene. Dette er løsningen, der allerede er sat i drift med NemID fra marts 2017.
2. En dedikeret erhvervsidentitet, hvor der registreres en relation mellem personens private MitID og CVR-numre for de virksomheder/organisationer, personen er tilknyttet (mapning mellem MitID og CVR-nummer).
3. En dedikeret erhvervsidentitet med tilhørende akkreditiver, der oprettes i MitID. Disse akkreditiver kan være delt mellem flere erhvervsidentiteter eller kan være dedikerede til én specifik erhvervsidentitet.
4. MOCES PKI-baseret akkreditiv (nøglepar med tilhørende OCES-certifikat).

I forhold til punkt 2 vil der gælde et dobbelt frivillighedsprincip, så denne mulighed kun vil være tilgængelig, hvis både medarbejder og virksomhed accepterer autentifikation via medarbejderens private MitID-akkreditiver.

En central komponent i erhvervsløsningen bliver en administrationsportal for virksomheder, hvor virksomhedens administrator vil kunne administrere virksomhedens medarbejderes erhvervsidentiteter og de tilhørende roller og rettigheder, som er oprettet i FBRS-komponenten.

**Fælles aftaleindgåelse for virksomheder på tværs af systemer**
For at mindske de administrative byrder for virksomheder, arbejdes der på at lave en fælles håndtering af aftaleindgåelse for virksomheder på tværs af de fællesoffentlige infrastrukturløsninger, NemLog-in, MitID og Digital Post. I stedet for at indgå individuelle brugsaftaler med de enkelte infrastrukturløsninger er planen, at der fremadrettet kun skal indgås én aftale, og at dette så vidt muligt gøres digitalt.

DIGITALISERINGSSTYRELSEN

**Registreringsautoriteter i erhvervsløsningen**
Virksomheder og andre organisationer med et tilknyttet CVR-nummer vil fortsat have mulighed for at oprette medarbejderidentiteter som med den hidtidige administrator-rolle i NemID Medarbejdersignatur. Dog vil der ske en ændring i forhold til opretholdelse af de sikringsniveauer for personidentiteter, der defineres med NSIS-standarden. Virksomheder vil som udgangspunkt kun kunne udstede erhvervsidentiteter til deres medarbejdere på det NSIS-sikringsniveau, de kan certificeres til. Efterfølgende vil det være muligt at hæve sikringsniveauet for en sådan identitet til det ønskede niveau, fx ved at medarbejderen validerer sin erhvervsidentitet ved hjælp af sin private personidentitet (eller en anden personlig erhvervsidentitet).

Hvis virksomhed og/eller medarbejder ønsker at benytte MOCES-akkreditiv, vil erhvervsløsningen facilitere oprettelse af MOCES-certifikat i infrastrukturens CA-komponent.

*Fælles brugerrettighedsstyring*
En central komponent i den eksisterende NemLog-in løsning er den fælles brugerrettighedsstyringskomponent (FBRS). Den fungerer som brugeradministrationskomponent for en lang række offentlige tjenester og onlineløsninger rettet mod virksomheder. FBRS bygger pt. på den ID-nøgle (RID), der findes i NemID Medarbejdersignatur-løsningen. Via FBRS' administrationsportal har virksomheder og organisationer mulighed for i en samlet portal at administrere rettigheder på tværs af tilkoblede onlineløsninger for alle de medarbejdere, virksomheden har oprettet i NemID Medarbejdersignatur-løsningen.

Der er ca. 250.000 virksomheder og organisationer i den nuværende FBRS-løsning. Hvis medarbejdere fra disse virksomheder autentificerer sig via NemLog-in loginportalen, medsendes automatisk alle relevante rettigheder som en del af autentifikationsbilletten til den enkelte løsning.

I den fremtidige infrastruktur vil FBRS blive tættere integreret i den fremtidige erhvervsidentitetsgarant, der erstatter NemID Medarbejdersignatur.

For at forbedre brugeroplevelsen for administratorer i virksomheder og organisationer bliver FBRS opdateret på en række punkter. Den skal fx service-enables, så rettigheder kan administreres fra eksterne systemer via API, og der skal bygges en ny administrationsportal, så virksomheder eller organisationer får en mere intuitiv portal til håndtering af erhvervsidentiteter og de tilknyttede rettigheder.

En anden planlagt udvidelse er, at FBRS skal kunne håndtere mere finkornede rettigheder i form af dataafgrænsninger som supplement til de nuværende statiske roller.

*Migrering af brugere fra "NemID Medarbejdersignatur" til den fremtidige erhvervsidentitetsgarant*
Hvad angår eksisterende erhvervsidentiteter i NemID Medarbejdersignatur er forventningen, at de som udgangspunkt alle skal migreres til den nye erhvervsløsning, så den enkelte virksomhed slipper for at oprette nye rettigheder til sine erhvervsidentiteter (medarbejderidentiteter) i FBRS og evt. andre, eksterne systemer. En ændring i relation til dette bliver, at de migrerede erhvervsidentiteter vil skulle indplaceres på et NSIS-sikringsniveau, som vil afhænge af bl.a. den registreringsproces, der har været fulgt for den enkelte erhvervsidentitet, da den blev oprettet i NemID.

Migrering dækker i NemLog-in-regi over en række aktiviteter, som har en vis fleksibilitet ift. tidsmæssig placering, men også hver især har bindinger og afhængigheder, fx til bestemte milepæle i MitID-projektet. Der er følgende migreringsaktiviteter:

DIGITALISERINGSSTYRELSEN

- Virksomheder skal indgå aftale om tilslutning til NemLog-in's system til håndtering af erhvervsidentiteter.
- Data om, hvem der er udpeget som NemID-administratorer, skal overføres fra den nuværende NemID Medarbejdersignatur-løsning.
- Erhvervsidentiteter skal migreres fra det nuværende system til NemLog-in. Her skal det sikres, at tilknyttede data (fx rettigheder i FBRS) bevarer relationen til erhvervsidentiteter.
- Certifikatbaserede (OCES) identiteter skal erstattes af nye tilsvarende oprettet i det nye CA under den reviderede certifikatpolitik
- Erhvervsidentiteter, der ikke skal have tilknyttet OCES-akkreditiver (privatnøgle+certifikat), vil skulle have tilknyttet MitID-akkreditiver i stedet for de nuværende NemID-akkreditiver.

*Adgang til MitID og NemLog-in-infrastrukturen for private tjenesteudbydere*
For at sikre, at private TU også i fremtiden vil have adgang til at benytte de tilgængelige services i den nationale eID-infrastruktur (fx autentifikation af brugere), vil NemLog-in tilbyde adgang for denne gruppe af TU via en identitetsbrokerløsning.

Afhængig af, hvor stor interessen fra det private marked bliver i forhold til at træde ind i rollen som identitetsbroker i MitID for private TU, er det sandsynligt, at der over tid vil blive tilbudt andre adgangspunkter end den her beskrevne i NemLog-in.

*eIDAS Gateway for integration med andre, nationale eID-løsninger fra resten af EU*
Som beskrevet ovenfor vil offentlige tjenesteudbydere fra 2018 være forpligtet til at anerkende digitale identiteter fra andre EU-lande, forudsat at disse er eIDAS-notificerede identitetsløsninger. Det indebærer, at offentlige tjenesteudbydere skal understøtte autentifikation med akkreditiver fra andre landes eIDAS-notificerede identitetsgaranter.

For at kunne håndtere dette etablerer Digitaliseringsstyrelsen en såkaldt "eID Gateway", der skal kunne håndtere identiteter fra andre EU-landes nationale identifikationsløsninger og omdanne dem til et format, der kan benyttes i danske offentlige selvbetjeningsløsninger. Gateway'en vil udbyde en SAML-baseret snitflade til danske tjenesteudbydere, der i så høj grad som muligt ligner den OIOSAML-snitflade, der allerede findes på NemLog-in, for herved at lade tjenesterne i vidt omfang genbruge deres eksisterende integrationer.

*Migrering af tjenesteudbydere til den kommende infrastruktur*
Afhængig af, hvordan tjenesteudbydere i dag benytter den eksisterende NemID-løsning, vil migrering til den fremtidige infrastruktur blive en større eller mindre opgave. Det afhænger af, om TU integrerer direkte med NemID via dennes TU-pakke, eller om TU benytter en mellemliggende identitetsbrokerløsning som fx NemLog-in eller NemAdgang. I det sidste tilfælde vil opgaven for den enkelte tjenesteudbyder kunne minimeres, da migreringsrelaterede ændringer et langt stykke hen ad vejen kan begrænses til brokerniveauet, så TU kan fortsætte med uændret (eller minimalt ændret) interface til infrastrukturen.

Da den fremtidige infrastruktur er en anden end den eksisterende NemID-løsning er det forventeligt, at alle private tjenesteudbydere skal indgå nye aftaler for at kunne benytte MitID. Afhængig af hvordan den enkelte identitetsbroker vælger at håndtere integrationen med MitID, kan der være afledte konsekvenser i form af fx snitfladeændringer for de tilknyttede TU.

DIGITALISERINGSSTYRELSEN

*Ejerskab til den fællesoffentlige infrastruktur*
For at sikre en mulighed for videreudvikling af eksisterende løsninger og tættere integration mellem løsninger, er det et mål for de fremtidige fællesoffentlige digitale løsninger, herunder NemLog-in3, MitID og Næste Generation Digital Post, at opnå en høj grad af rettigheder og ejerskab.

Samtidig ønsker Digitaliseringsstyrelsen at kunne anvende kommercielle standardkomponenter, så en standardfunktionalitet ikke skal udvikles fra bunden i de fællesoffentlige systemer, og så man ikke fra fællesoffentlig side skal bære de fulde omkostninger ved løbende vedligehold af fx kildekode.

For alle dele af de fremtidige løsninger, der ikke allerede forud for de enkelte udbud er udviklet som standardkomponenter og benyttes af en bred vifte af kunder, vil der blive stillet krav til leverandører om fulde rettigheder i et omfang, der muliggør ubegrænset videre brug, drift og videreudvikling – også efter kontrakternes udløb.

For overblikkets skyld opsummeres her, hvilket scope der forventes i de udbud, der skal videreføre funktionaliteten fra NemID og vedrører hhv. MitID og den fremtidige NemLog-in-løsning.

## Scope for de kommende udbud

*Scope for MitID-udbuddet*
I forhold til det eksisterende NemID er der tale om et ændret indhold i den kommende løsning.

Scope for udbuddet bliver i overordnede træk følgende:

- Udvikling af identitetsgarant og autentifikationsløsning for personidentiteter.
- Understøttelse af autentifikation og "livscyklushåndtering" for digitale personidentiteter under hensyntagen til forskellige anvendelsesmodeller hos identitetsbrokere og tjenesteudbydere.
- Facilitering af standardakkreditiver til løsningens brugere.
- Drift, vedligehold og videreudvikling af løsningen.
- Proces- og systemunderstøttelse for processer som registrering, indrullering, opdatering, spærring, etc. af personidentiteter og de hertil hørende akkreditiver (login-midler) med fokus på compliance i forhold til sikkerhedsmæssige krav.
- Facilitering af migrering til MitID af brugere fra NemID.

Læs mere på side 1.

*NemLog-in3 deles i to udbud*
Scope for den kommende NemLog-in3-løsning vil dels omfatte en videreførelse af de komponenter, der allerede findes i NemLog-in-løsningen.

Derudover vil scope blive udvidet, så funktionalitet og ydelser, der i dag varetages af den fællesoffentlige del af NemID, men som fremadrettet ikke bliver del af MitID-udbuddet, videreføres i regi af NemLog-in3. Dette gælder fx "NemID Medarbejdersignatur", PKI/CA, dokumentsigneringsfunktionalitet samt understøttelse af private tjenesteudbyderes adgang til MitID-infrastrukturen.

DIGITALISERINGSSTYRELSEN

For på bedst mulig vis at håndtere de interne og eksterne afhængigheder, der er identificeret for at kunne videreføre NemLog-in-løsningen, er det besluttet at opdele den fremtidige udgave af løsningen i to separate udbud: Et it-driftsudbud og et udviklings- og forvaltningsudbud.

*Scope for NemLog-in 3, driftsudbuddet*
Scope for dette udbud bliver videreførelse af driften af de forskellige komponenter i den eksisterende NemLog-in-løsning, samt løbende overtagelse og idriftsættelse af nye og/eller opdaterede komponenter i NemLog-in-løsningen fra den fremtidige NemLog-in-udviklingsleverandør.

*Scope for NemLog-in 3, udviklings- og forvaltningsudbuddet*
Scope for dette udbud forventes at bestå af en række udviklingsrelaterede ydelser og en række mere forvaltningsrelaterede ydelser.

Udviklingsrelaterede ydelser:

- Udvikling af en ny erhvervsidentitetsgarant.
- Udvikling af ny signeringstjeneste.
- Videreudvikling af funktionalitet i den eksisterende NemLog-in-løsning.
- Implementering af ny PKI/CA til videreførelse af OCES-certifikatinfrastruktur.
- Nyudvikling og videreudvikling i relation til understøttelse af private TU's adgang til NemLog-in-infrastruktur.

Forvaltningsrelaterede ydelser:

- Administration, support og generel understøttelse af offentlige TU's adgang til NemLog-in og MitID-infrastrukturen.
- Håndtering af forpligtelser relateret til rollen som identitetsbroker i forhold til MitID.
- Administration, support og generel understøttelse af private TU's adgang til NemLog-in og MitID-infrastrukturen
- Håndtering af forpligtelser relateret til rollen som CA i forhold til den fremtidige videreførelse af OCES-certifikatinfrastruktur.
- Ansvar for processer og samarbejde ifm. videreudvikling, test, release, idriftsættelse, ændringsanmodninger, hændelseshåndtering mm.