DIGITALISERINGSSTYRELSEN

Fremtidens infrastruktur for digitale identiteter i Danmark

7. oktober 2019
CIU
J.nr. 2019 - 3661

Indledning

I løbet af den kommende årrække bliver den næste generation af Danmarks digitale infrastruktur opbygget.

Den næste generation, som erstatter NemID med MitID og opgraderer NemLog-in (NemLog-in3), er allerede ved at blive implementeret. Noget videreføres, mens andet laves helt om. Visionen på tværs af de to projekter er at skabe langsigtede løsninger med høj grad af sikkerhed, fleksibilitet og gode brugeroplevelser. Der eksisterer betydelige afhængigheder mellem MitID og NemLog-in. Læs her om de store linjer for de løsninger, der vil komme til at forme den fremtidige infrastruktur for digitale personidentiteter, signering og brugerrettighedsstyring i Danmark.

Udbuddene kort fortalt

Digitaliseringsstyrelsen har gennemført udbud for både MitID-projektet og NemLog-in-projektet i løbet af 2018 og 2019.

MitID

MitID afløser og udbygger sammen med NemLog-in den funktionalitet, der i dag ligger i NemID. MitID rummer alene en løsning for elektronisk validering af en persons identitet, og bliver udviklet gennem et partnerskab mellem de danske pengeinstitutter repræsenteret ved FR1 af 16. september 2015 A/S (herefter kaldet FR1) og den offentlige sektor repræsenteret ved Digitaliseringsstyrelsen. MitID stilles dermed til rådighed for både den offentlige og private sektor. Der blev indgået kontrakt med leverandøren af MitID, Nets DanID A/S, i marts 2019.

NemLog-in

I modsætning til den eksisterende NemID-løsning, indeholder MitID ikke en signatur- og erhvervsløsning. Erhvervsdelen og signaturløsningen anskaffes alene i regi af den offentlige sektor og indgår som en del af NemLog-in-projektet. NemLog-in varetager endvidere rollen som MitID broker for alle offentlige tjenesteudbydere (TU'ere). NemLog-in blev udbudt via to separate udbud; et udbud af NemLog-in drift og et udbud af NemLog-in udvikling og forvaltning.

Digitaliseringsstyrelsen har i maj 2018 tildelt kontrakten om drift af NemLog-in til NNIT A/S. Digitaliseringsstyrelsen har i december 2018 tildelt kontrakten om nyudvikling, videreudvikling, vedligeholdelse og forvaltning af NemLog-in til Nets DanID A/S.

Øget ejerskab af de fremtidige fællesoffentlige digitale løsninger

For at sikre mulighed for videreudvikling af de eksisterende løsninger og en tættere integration mellem dem, er det et væsentligt mål for de fremtidige løsninger, herunder MitID, NemLog-in og Næste generation Digital Post, at Digitaliseringsstyrelsen opnår en høj grad af rettigheder og ejerskab ift. løsningerne. Samtidig ønsker Digitaliseringsstyrelsen at kunne anvende kommercielle standardkomponenter, således at standardfunktionaliteter i de fællesoffentlige digitale løsninger ikke skal udvikles fra bunden. Derfor er der for alle dele af de fremtidige løsninger, der ikke allerede forud for de enkelte udbud er udviklet som standardkomponenter, stillet krav til leverandørerne om at Digitaliseringsstyrelsen har de fulde rettigheder i et omfang, som muliggør ubegrænset videre brug, drift og videreudvikling – også efter kontraktens udløb.

MitID projektet

Baggrund

Digitaliseringsstyrelsen og Finans Danmark har via datterselskabet FR1 indgået et partnerskab om fælles udvikling og drift af MitID, som er en ny, central identitetsgarant for digitale personidentiteter. Kontrakten for det kommende MitID blev underskrevet i marts 2019 og skal erstatte det nuværende 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 personidentiteter i kernen som udgangspunkt kan benyttes på tværs af sektorer og tjenesteudbydere, uanset hvilken aktør der har registreret og indrulleret den pågældende person.

Om MitID løsningen

MitID-projektet vil fokusere på de dele af den fremtidige digitale infrastruktur, hvor partnerskabet har fælles behov samt på elektronisk validering af en persons identitet. Øvrige elementer af den fremtidige digitale infrastruktur, fx inden for autorisation, fuldmagt, dokumentsignering og transaktionsgodkendelse, vil blive udviklet separat af de enkelte parter eller andre private aktører.

NemID, der er drevet af Nets DanID A/S, består af to forskellige dele: "bank-løsningen" og den offentlige, PKI-baserede "OCES-løsning". Den opdeling forandres med MitID-løsningen. MitID-projektet udvikler en fælles identitets- og autentifikationsløsning med en identitetskerne, der understøtter autentifikation og livscyklushåndtering af digitale personidentiteter. Dette omfatter bl.a. registrering af personidentiteter samt indrullering, opdatering og spærring af elektroniske identifikationsmidler (tidligere kaldet akkreditiver).

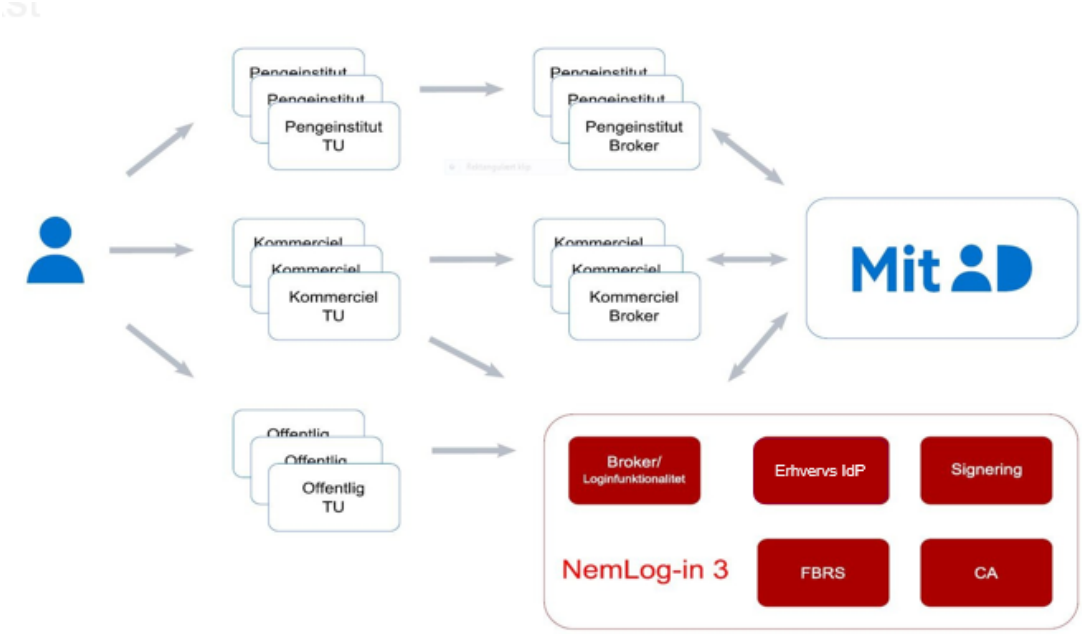
Til brugerne skal der udvikles et sæt standard MitID elektroniske identifikationsmidler, som skal kunne udvides løbende i takt med den generelle teknologiske og forretningsmæssige udvikling. Der kommer et smartphonebaseret

identifikationsmiddel, et passwordbaseret identifikationsmiddel, samt flere fysiske identifikationsmidler bl.a. til svagtseende, som erstatning af de nuværende NemID elektroniske identifikationsmidler.

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

- MitID-kernen skal udvikles, så eksterne parter, såkaldte "identitetsbrokere" (brokere), kan lave deres egne løsninger med slutbruger-autentifikation via MitID-kernen.
- Certifikat, signering og offentlig erhvervsfunktionalitet indeholdes i fremtiden i NemLog-in-løsningen.

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



Figur 1: Tilslutning af tjenesteudbydere (TU'ere)

I den eksisterende identitetsinfrastruktur er størstedelen af de offentlige tjenesteudbydere tilsluttet NemID-løsningen via den fællesoffentlige login-

portal/identitetsbroker, NemLog-in, ligesom en række private tjenesteudbydere benytter tilsvarende kommercielle løsninger, i stedet for at implementere NemID-klienten i egne onlineløsninger via den såkaldte "NemID TU-pakke".

En af de store fordele ved broker-modellen er, at den enkelte tjenesteudbydere 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 har behov for, 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 tjenesteudbydere 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 tjenesteudbydere 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 tjenesteudbydere 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 vil anmelde MitID som national eID-løsning, så identiteter herfra skal 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, for at leve op til eIDAS' tre sikringsniveauer[2] (eller LoA - Level of Assurance) for digitale identiteter. Fremover skal alle offentlige tjenesteudbydere, brokere og identitetsløsninger, der skal benytte den nationale infrastruktur, forholde sig til denne standard, når de vurderer deres tjenester og de data, som kan tilgås via disse tjenester for at sikre, at de er beskyttet med autentifikation på et tilstrækkeligt højt sikringsniveau.

---

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

[2] Niveau Høj, Betydelig eller Lav.

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. Alle som foretager betalingsformidling vil skulle leve op til disse regler gennem den danske lovgivning i "revideret lov om betalinger", der trådte i kraft 1. januar 2018. MitID skal understøtte disse regulatoriske krav i det omfang de relaterer sig til MitID funktionalitet.

Databeskyttelsesforordningen
I 2018 trådte den nye persondataforordning (også kaldet GDPR) i kraft. Den har indvirkning på alle offentlige og private tjenester, der håndterer persondata. Dvs. at GDPR er relevant for den digitale infrastruktur, herunder også MitID og NemLog-in. Persondataforordningen er mere vidtgående i sine operationelle krav til aktørerne end den hidtidige regulering, og der er markant større sanktionsmuligheder.

Registreringsenheder
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 via digst.dk.

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

Ligesom i den eksisterende NemID-løsning vil der blive udpeget aktører, der vil agere som registreringsenheder (RA) med mulighed for at oprette nye personidentiteter i løsningen. Afhængigt af hvilket sikringsniveau de enkelte registreringsenheder 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, og Kriminalforsorgen, vil også fremover fungere som RA. Pengeinstitutter kan også varetage rollen som RA.

I forhold til slutbrugere, der skal bruge MitID i erhvervsmæssig sammenhæng, vil NemLog-in3 tilbyde en registreringsportal som en del af den fremtidige erhvervsidentitetsløsning.

MitID vil desuden tilbyde online registrering, så slutbrugere selv kan registrere og indrullere sig på de lavere sikringsniveauer (op til NSIS-sikringsniveau betydelig) uden personligt fremmøde hos en RA, hvis slutbrugeren har et CPR nummer og relevante legitimationsdokumenter.

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 adgangspunkt til identitetsinfrastrukturen for alle offentlige tjenester.

Samtidig udvides NemLog-in-løsningen med en ny identitetsgarant og administrationsportal for erhvervsidentiteter. Herved samles alle dele af funktionaliteten omkring erhvervsidentiteter og administration fremover i NemLog-in.

Målet er at skabe en mere sammenhængende brugeroplevelse for erhvervsbrugere og administratorer i virksomheder, som i fremtiden kan varetage brugeradministration og rettighedsadministration 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 deres private MitID identifikationsmidler i en erhvervsmæssig kontekst.

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 ved hjælp af brugernes eksisterende NemID. Læs mere nedenfor om migrering af erhvervsidentiteter.

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. Dette afhænger af om tjenesteudbydere integrerer direkte med NemID-løsningen via dennes TU-pakke, eller om tjenesteudbydere benytter en mellemliggende identitetsbrokerløsning, som fx NemLog-in. I det sidste tilfælde vil opgaven for den enkelte tjenesteudbydere kunne minimeres, da migreringsrelaterede ændringer et langt stykke hen ad vejen kan begrænses til brokerniveauet, så tjenesteudbydere 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 tjenesteudbydere.

NemLog-in3-projektet

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, hvorfor løsningen er blevet genudbudt. Som en del af NemLog-in3 skal der udvikles en løsning for erhvervsidentiteter.

Om NemLog-in løsningen

NemLog-in videreføres og vil fortsat fungere i de roller, som i dag. Det vil altså være den primære fælles identitetsbroker/IdP-løsning og integrationspunkt for offentlige tjenesteudbydere og selvbetjeningsløsninger og tilbyde den samme række af services som i dag. Det er fx loginportal med Single-sign-on (SSO) funktionalitet, fælles brugerrettighedsstyring (FBRS), signeringstjeneste (inkl. signaturvalidering), 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 tjenesteudbydere. 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 identitetsgarant (IdP) for erhvervsidentiteter, inkl. tilhørende administrationsportal for erhvervsidentiteter til erstatning for den OCES-baserede "NemID Medarbejdersignatur" løsning.
- CA-funktionalitet (OCES), der i den nuværende infrastruktur leveres som en del af NemID, vil i fremtiden blive en del af scopet for NemLog-in.
- Signeringsløsningen skal opgraderes og moderniseres væsentligt i forhold til nye signeringsstandarder mv.

En anden stor ændring bliver, at der åbnes op for, at private tjenesteudbydere skal kunne benytte dele af NemLog-in.

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

- NemLog-in loginportalen opdateres, så den understøtter autentifikation via MitID.

- FBRS opdateres, så komponenten bliver bedre integreret med den fremtidige portal til erhvervsidentitetsadministration.
- Tilslutning af tjenesteudbydere og især aftaleindgåelse for virksomheder, der ønsker at udstede erhvervsidentiteter (Brugerorganisationer) samles og strømlines væsentligt.

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 (SSO)
NemLog-ins eksisterende loginportal vil blive opdateret, så den understøtter autentifikation via MitID. Det vil kun i mindre omfang påvirke eksisterende tjenesteudbydere, 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-certifikaterne. NemLog-in bliver således en brokerløsning i forhold til MitID- infrastrukturen og vil fungere som det primære adgangspunkt for offentlige tjenesteudbydere med uændret funktionalitet ift. SSO. Derudover vil portalen også kunne benyttes af private tjenesteudbydere til at blive tilsluttet MitID infrastrukturen, dog uden mulighed for SSO.

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 elektroniske identifikationsmidler, eller via dedikerede MitID-erhvervsidentifikationsmidler. Der indføres dermed en løsere kobling mellem erhvervsidentiteter og identifikationsmidler end i dag, hvilket giver en mere fleksibel infrastruktur og brugeroplevelse.

Såfremt brugeren har tilknyttet sine private MitID identifikationsmidler 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 tjenesteudbydere, 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 identifikationsmidler– fx elektroniske identifikationsmidler udstedt lokalt i en

organisation, der har sin egen Identity Provider.

Signering i den fremtidige infrastruktur

Der skal udvikles en signeringskomponent baseret på den nye CEN-standard for Remote Signing (CEN EN 419 241). Komponenten vil blive bygget som en del af NemLog-in3-projektet, og erstatter den signeringsservice, der allerede findes i NemLog-in.

Signering vil basere sig på slutbrugerautentifikation via MitID-kernen eller anden identitetsgarant, fx NemLog-in3 for erhvervsidentiteter. Komponenten vil i første omgang understøtte signaturformaterne PAdES og XAdES. Den vil til forskel fra den nuværende løsning være baseret på kvalificerede engangscertifikater (korttidscertifikater), der vil blive udstedt af infrastrukturens CA-komponent (i NemLog-in). 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.

PKI/CA-certifikat funktionalitet i den fremtidige infrastruktur

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 certifikatpolitikkerne revideres og tilpasses de fremtidige behov. Dette betyder bl.a. at:

- Certifikatpolitik for OCES Person (POCES) videreføres ikke.
- Certifikatpolitikker for OCES funktionscertifikater (FOCES) og OCES virksomhedscertifikater (VOCES) samles i én opdateret certifikatpolitik for OCES virksomhedscertifikater.
- OCES certifikatpolitikkerne suppleres med nye offentlige certifikatpolitikker for kvalificerede certifikater for fysiske personer (borgere), fysiske personer associeret med en juridisk person (medarbejdere) og juridiske personer (virksomheder).
- Der er udarbejdet en ny offentlig politik for kvalificeret tidsstempling. Samtlige politikker opbygges efter en struktur fastlagt i internetstandarden RFC 3647.
- Kravene følger NSIS og eIDAS, som er mere outcome baserede.
- Politikkerne er bragt i overensstemmelse med europæiske standarder for politikker for tillidstjenester.
- Certifikatpolitikken for MOCES strammes op, så sikkerhedskravene til opbevaring og håndtering af nøglefiler tydeliggøres, hvilket begrænser muligheden for lokalt installerede nøglefiler i software på PC og lignende. Dette sker for at sikre et ensartet højt sikringsniveau.

De fremtidige erhvervsidentiteter
Til erstatning for NemID til Erhverv (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.

Fire former for elektroniske identifikationsmidler vil fremover være tilgængelige for erhvervsidentiteter:

1. Automatisk kobling mellem privat personidentitet/elektronisk identifikationsmiddel og virksomheder, hvor personen kan tegne virksomheden alene. Dette er "NemID privat til erhverv" løsningen, der allerede er sat i drift med NemID fra 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 dedikerede erhvervsidentifikationsmidler, der oprettes i MitID. Disse elektroniske identifikationsmidler kan være delt mellem flere erhvervsidentiteter eller kan være eksklusive for én specifik erhvervsidentitet.

4. MOCES PKI-baseret identifikationsmiddel (nøglepar med tilhørende OCES-certifikat), som dog ikke direkte vil kunne anvendes til autentifikation i NemLog-in.

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

Den kommende erhvervsidentitetsadministration samler identitets- og rettighedsstyring for erhvervsidentiteter i én portal, 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, udarbejdes 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, skal der

fremadrettet kun indgås én aftale, og dette gøres så vidt muligt digitalt.

Registreringsautoriteter i erhvervsløsningen

Virksomheder og andre organisationer med et tilknyttet CVR-nummer vil fortsat have mulighed for at oprette erhvervsidentiteter svarende til funktionaliteten 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 være garant for koblingen mellem medarbejderen og virksomheden, mens identitetssikringen af medarbejderen som fysisk person beror på validering ved hjælp af medarbejderens private personidentitet (MitID eller anden digital identitet på samme sikringsniveau).

Hvis virksomhed og/eller medarbejder ønsker at benytte MOCES-certifikater, vil det være muligt at oprette disse i NemLog-ins CA-komponent via erhvervsidentitetsadministrationen.

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, som 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 samlet og mere intuitiv portal til håndtering af erhvervsidentiteter og de tilknyttede rettigheder.

Senere forventes en udvidelse, der sætter FBRS i stand til at 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 erhvervsidentitetsgarant, 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 bl.a. vil afhænge af 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 vil i store træk være følgende migreringsaktiviteter:

- Virksomheder skal indgå aftale om tilslutning til NemLog-in's system til håndtering af erhvervsidentiteter.
- Erhvervsidentiteter skal migreres fra det nuværende system til NemLog-in, hvor de oprettes i suspenderet tilstand. Her skal det sikres, at tilknyttede data (fx rettigheder i FBRS) bevarer relationen til erhvervsidentiteter.
- FOCES og VOCES certifikater skal erstattes af nye tilsvarende, oprettet i det nye CA under den reviderede certifikatpolitik.
- Erhvervsidentiteterne skal som udgangspunkt enten knyttes til et privat MitID identifikationsmiddel eller et dedikeret MitID identifikationsmiddel i stedet for de nuværende NemID identifikationsmidler.

Adgang til MitID og NemLog-in-infrastrukturen for private tjenesteudbydere

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

Afhængigt af hvor stor interessen fra det private marked bliver i forhold til at træde ind i rollen som identitetsbroker i MitID for private tjenesteudbydere, 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 er offentlige tjenesteudbydere fra 2018 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 elektroniske identifikationsmidler fra andre landes eIDAS-notificerede identitetsgaranter.

For at kunne håndtere dette har Digitaliseringsstyrelsen etableret 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. eID Gateway 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 i vidt omfang at lade tjenesterne genbruge deres eksisterende integrationer.

MitID vil blive eIDAS-notificeret, som den danske nationale identitetsgarant, og vil således kunne bruges af danske borgere med et MitID identifikationsmiddel mod offentlige tjenesteudbydere i andre EU-lande.