DIGITALISERINGSSTYRELSEN

Notat

22. april 2021
DIGST

Redegørelse vedrørende Digitaliseringsstyrelsens håndtering af sikkerheden i NemKonto og NemID

Indhold

0. Resumé

Finansministeren var i samråd den 25. februar 2021 om sikkerheden i NemID og NemKonto om afluring af personlige data via installationer på bibliotekernes computere, og hvilke tiltag regeringen igangsætter for at undgå svindel med blandt andet NemID.

På samrådet blev der refereret til Danmarks Radios aktindsigt og udsendelse om svindel med NemKonto – herunder udsagn om, at Digitaliseringsstyrelsen gennem årene skulle have modtaget 30 advarsler, som Digitaliseringsstyrelsen havde siddet overhørig. Finansministeren lovede i den sammenhæng en redegørelse for de henvendelser, der er kommet, og hvordan de er blevet håndteret.

Digitaliseringsstyrelsen har i det følgende udarbejdet en redegørelse om NemKonto og NemID. Særligt på baggrund af omtalen på samrådet af de 30 henvendelser er der udarbejdet et overblik *jf. tabel 1*, samt en detaljeret gennemgang af forløbet og håndteringen af de modtagne henvendelser om svindel med NemKonto, afledt af identitetstyveri af NemID fra borgere. For så vidt angår NemID er der i redegørelsen særligt fokuseret på de indsatsområder og tiltag ift. sikkerhed, som er gennemført.

Digitaliseringsstyrelsens konklusion er, at der i det materiale, som der blev refereret til på samrådet, indgår 21 henvendelser fra interessenter og borgere, der berører svindel med NemKonto som følge af identitetstyveri af NemID. De 21 henvendelser har affødt forløb med dialog mellem henvenderen og Digitaliseringsstyrelsen og derved yderligere mailudveksling. Hvis man indregner disse yderligere underliggende mails, indgår der i styrelsens optælling i alt 38 indgående henvendelser.

Dialogforløbene har bl.a. omhandlet problematikker om svindel med NemKonto afledt af identitetstyveri af NemID. Digitaliseringsstyrelsen har vurderet de indkomne henvendelser, forholdt sig aktivt til og svaret på disse, samt på baggrund af henvendelserne inviteret til dialog med de centrale interessenter. Dialogerne har været udtryk for et ønske i Digitaliseringsstyrelsen og hos de centrale interessenter om at adressere og håndtere de påpegede problemstillinger.

Det bemærkes dog, at der er fundet en enkelt henvendelse fra februar 2016, hvor der ikke i journalsystemet kan findes oplysninger om selve henvendelsen eller besvarelse heraf umiddelbart efter henvendelsen i 2016. Der kan derfor først findes svar herpå afsendt efter en rykker med genfremsendelse i juli 2017.

I Digitaliseringsstyrelsen arbejdes med en intern frist, som betyder, at alle henvendelser skal besvares inden for ti kalenderdage. Der kan være tale om endelige svar eller kvitteringssvar. Som opfølgning på redegørelsen vil Digitaliseringen skærpe opfølgningen på denne svarfrist.

Undervejs har Digitaliseringsstyrelsen på baggrund af henvendelserne aktivt taget stilling til de indkomne forslag, afsøgt løsningsmuligheder, foretaget analyse fx af problematikken om 3. mands konti samt fx opfordret interessenter til at erfaringsudveksle om løsningsmuligheder. I forløbet har der også været dialog med leverandøren af NemKonto-løsningen om muligheder for at udtrække data fx til brug for at finde markører på, hvor der evt. kunne være foregået svindel med borgeres NemKonto, og foretage ændringer i systemet.

Senest er det besluttet at udsende papirbaserede aktiveringsbreve i forbindelse med ændringer af NemKonto i selvbetjeningsløsningen, så en ændret NemKonto først bliver aktiv efter brug af en aktiveringskode, som fremsendes til borgerens postadresse.

Der er dog også forslag om tiltag i NemKonto-løsningen, som ikke er blevet vurderet virksomme. Andre forslag indgår som indspil i Ny NemKonto-projektet, der har været forberedt i flere år, og i 2021 opnåede bevilling på finansloven.

Digital svindel med en borgers NemKonto kan alene ske som følge af identitetstyveri af NemID. Også derfor har det været særligt vigtigt for Digitaliseringsstyrelsen ikke kun at fokusere på håndtering i NemKonto-løsningen, men også at sætte ind med tilretninger og udvikling af NemID-løsningen.

Redegørelsen viser, at Digitaliseringsstyrelsen løbende i perioden som redegørelsen omfatter - fra medio 2015 og frem til og med februar 2021 - har implementeret en række forskelige ændringer i selve NemID-løsningen med det formål at styrke sikkerheden og nedbringe omfanget af svindel. Herunder kan nævnes tilpasning af arbejdsgange i forbindelse med udstedelse af NemID, domænebeskyttelse, implementering af NemID Nøgleapp og gennemførsel af informationsindsatser om sikker og korrekt brug af NemID, målrettet borgere med henblik på at imødegå svindel med NemID.

Sikring af NemID-løsningen imødegår både mulighed for svindel med borgeres NemKonto samt de selvbetjeningsløsninger, som NemID giver adgang til, fx borgeres private netbank, borger.dk, Digital Post mv.

På området for NemID er der særligt redegjort for de hovedudfordringer med svindel, som indgår i Digitaliseringsstyrelsen risikoanalyse, og de sikkerhedsindsatser, der har været iværksat på NemID-løsningen. Der er også redegjort for, hvordan Digitaliseringsstyrelsen har forholdt sig til fem forslag fremsat af leverandøren Nets til håndtering af svindel med NemID, og som der blev spurgt til på samråd den 25. februar 2021. Af de fem forslag var nogle tidligere blevet undersøgt og vurderet i forhold til økonomi og løsningens levetid, mens andre af forslagene er blevet indarbejdet i det kommende MitID, der lanceres i 2021.

Sikkerheden i de digitale løsninger skal have meget høj prioritet i Digitaliseringsstyrelsen, og der skal arbejdes struktureret med sikkerheden bredt i styrelsen og i samarbejde med leverandørerne.

Det er på den baggrund besluttet at sætte yderligere initiativer i værk af hensyn til at understøtte fokus på sikkerhed og af hensyn til at sikre trygheden omkring løsningerne. Der er tale om følgende initiativer:

- Der er i de seneste år gennemført audit på et udvalg af de store infrastrukturløsninger i Digitaliseringsstyrelsen. På baggrund af dette forløb er det besluttet, at der vil blive igangsat en audit på NemKonto hurtigst muligt, hvor det undersøges, om der er sikkerhedsmæssige udfordringer forbundet med, at borgeres NemKonto kan tilknyttes en 3. mands bankkonto. På baggrund af denne audit vurderes, om der er behov for ændringer i forhold til NemKonto.

- Der foretages inden sommerferien en sikkerhedstest af NemKonto - en såkaldt penetrationstest.

- Det er besluttet, at der for at styrke tiltag mod svindel på NemKonto indføres en proces med udsendelse af fysiske aktiveringsbreve ved ændringer af NemKonto i selvbetjeningsløsningen. Dette betyder, at en ændring af NemKonto foretaget i selvbetjeningsløsningen først kan effektueres, når borgeren har aktiveret den nye NemKonto med en kode, der fremsendes pr. post til deres adresse. Løsningen er implementeret pr. 19. april 2021.

- Digitaliseringsstyrelsen arbejder med en intern frist, som betyder, at alle henvendelser skal besvares inden for ti kalenderdage. Som opfølgning på redegørelsen vil Digitaliseringsstyrelsen skærpe opfølgningen på denne svarfrist.

- Styrkelse af arbejdet med aktiv opfølgning på henvendelser om svindel. Det vil ske på de tilbagevendende systemnære sikkerhedsmøder i Digitaliseringsstyrelsens informationssikkerhedsudvalg. Det indebærer et yderligere topledерfokus på området.

Endvidere foretages der i forbindelse med udviklingen af MitID (afløseren for NemID) en række yderligere sikkerhedstiltag. Når MitID lanceres udfases bl.a. nøglekortet, og der indføres adviseringer, øget sikring mod identitetstyveri ved udstedelse og genvalidering af brugerne i forbindelse med overgangen fra NemID til MitID.

Det er Digitaliseringsstyrelsens konklusion, at sikkerheden i såvel NemKonto som NemID er meget høj, og at Digitaliseringsstyrelsen løbende har forholdt sig aktivt til og besvaret henvendelser om mulig svindel. Digitaliseringsstyrelsen har gennem årene gennemført tiltag, der er blevet vurderet virksomme i forhold til at forebygge og modvirke svindel på såvel NemKonto som NemID. Der er løbende fo-

retaget en række ændringer i løsningerne for at imødegå udviklingen i de it-kriminelles metoder. Men der er også tale om komplekse løsninger, og de gentagne dialoger og vurderinger har vist, at ikke alle ændringsforslag er virksomme over for svindel eller hensigtsmæssige set i forhold til den it-løsning - eller den forretningsmæssige kontekst, som et forslag ville skulle implementeres i.

1. Baggrund

NemID-løsningen er en digital infrastruktur, der giver borgerne mulighed for at autentificere sig i en række selvbetjeningsløsninger og signere digitalt. NemKonto-løsningen er en digital infrastruktur, der muliggør udbetalinger fra det offentlige og private til borgere, virksomheder og foreninger, idet løsningen rummer oplysninger, der kobler CPR- og CVR-numre med tilhørende kontonumre på NemKonti hos borgere og virksomheder. NemKonto-løsningen kan tilgås på system-til-system-basis, men har også tilknyttet en selvbetjeningsløsning, hvor borgere kan logge ind med NemID og registrere en given bankkonto som NemKonto. Man kan ikke igennem selvbetjeningsløsningen få adgang til de bagvedliggende data i NemKonto-løsningen i øvrigt.

1.1 Håndtering af henvendelser i Digitaliseringsstyrelsen

Henvendelser om svindel med NemKonto afledt af svindel med NemID er blandt redegørelsens hovedfokusområder. Af den grund præsenteres Digitaliseringsstyrelsens proces for håndering af henvendelser.

Digitaliseringsstyrelsen modtager et stort antal henvendelser fra borgere, myndigheder, private virksomheder og interesseorganisationer. Henvendelser kan fx vedrøre råd og vejledning om de løsninger, som Digitaliseringsstyrelsen er ansvarlig for, eller forbedringsforslag.

Digitaliseringsstyrelsen modtager henvendelser telefonisk eller gennem it-løsningernes funktionspostkasse, via Digitaliseringsstyrelsens hovedpostkasse eller henvendelser videreformidlet fra fx Finansministeriets departement. Som offentlig myndighed følger det af god forvaltningsskik, at henvendelser skal behandles inden for rimelig tid og ikke må trække unødigt ud.

Henvendelser og svar journaliseres i Digitaliseringsstyrelsens journalsystem, der løbende er blevet opdateret og udskiftet. Henvendelser kan således fremsøges i enten det nuværende eller et af de to tidligere journalsystemer. Fremsøgning af henvendelser forudsætter korrekt journalisering.

Henvendelser fra borgere, der har brug for support i forhold til en løsning, som fx NemID eller NemKonto, håndteres af Digitaliseringsstyrelsens Visiteringsenhed, der som oftest guider borgerne videre til den relevante supportfunktion eller straks-afklarer det givne spørgsmål. Systemspecifikke henvendelser, forbedringsforslag mv. videregives til det relevante team, som har ansvar for den givne løsning. På baggrund af henvendelserne udarbejdes et svar, og det vurderes i hvert

enkelt tilfælde, om der skal foretages yderligere håndtering eller opfølgning fx i forhold til løsningens leverandør.

Digitaliseringsstyrelsens Visiteringsenhed behandlede i 2020 over 6.000 telefoniske og over 4.000 skriftlige supporthenvendelser fra primært borgere vedrørende Digitaliseringsstyrelsens it-løsninger. Dertil kommer henvendelser fra eksterne interessenter og myndigheder, der er tilgået Digitaliseringsstyrelsen ad de nævnte kanaler ovenfor.

2. NemKonto

NemKonto-løsningen har juridisk ophæng i Lov 1203 af 27. december 2003. Loven indebærer, at borgere over 18 år, virksomheder og foreninger er forpligtet til at have en NemKonto, som det offentlige kan udbetale til, og at det er borgernes ansvar at opdatere NemKonto ved eksempelvis bankskifte. Ud over håndtering af offentlige betalinger kan NemKonto-løsningen også anvendes af private udbetalere og betalingsformidlere.

NemKonto-løsningen er finansieret af statslige midler og betalinger fra private udbetalere. KMD har udviklet løsningen, og har i dag IBM som underleverandør af drift og vedligehold. Kontrakten med KMD er uden udløb. Der arbejdes på et Ny NemKonto-projekt med henblik på at konkurrenceudsætte løsningen samt etablere en mere tidssvarende NemKonto-løsning *jf. afsnit 2.6*.

2.1 Håndtering af henvendelser om svindel med NemKonto

Der kan ikke svindles digitalt med en borgers NemKonto, medmindre en it-kriminel har skaffet sig adgang til en borgers NemID brugernavn, kode og nøglekort, dvs. foretaget identitetstyveri.

Det har været muligt at fremsøge 21 henvendelser fra interessenter og borgere, der berører svindel med NemKonto som følge af identitetstyveri af NemID. De 21 henvendelser har affødt forløb med dialog mellem henvenderen og Digitaliseringsstyrelsen og derfor yderligere mailudveksling. Hvis der indregnes disse yderligere underliggene mails, optælles i alt 38 indgående henvendelser.

I afdækningen af modtagne henvendelser vedrørende svindel med NemKonto, er Digitaliseringsstyrelsens journalarkiv gennemsøgt tilbage til 2015. Henvendelserne kommer i høj grad fra den finansielle sektor, særligt fra Finans Danmark, Finans og Leasing og enkelte pengeinstitutter. Derudover er der henvendelser fra skattemyndighederne og enkelte borgere. Supporthenvendelser fra fx borgere, der er bekymrede for, om de er blevet svindlet eller søger vejledning i, hvordan svindel i mødegås, er ikke medtaget i opgørelsen af henvendelser. Det er vurderingen, at håndteringen af henvendelser i Digitaliseringsstyrelsen er systematisk og robust samt har en hensigtsmæssig systemunderstøttelse.

Opgørelsen over henvendelser om svindel med NemKonto fremgår af *tabel 1*. Da henvendelserne typisk indgår i dialogforløb som led i en dialog, der dækker et antal henvendelser, er henvendelserne sorteret efter afsender og dernæst modtagedato i Digitaliseringsstyrelsen, hvorefter antallet af indgående henvendelser i korrespondancen fremgår:

Tabel 1

Henvendelser vedrørende sikkerheden i NemKonto

Fra	Dato		Tema	Se afsnit
Henvendelser i DR-aktindsigt		**korrespondancens indgående henvendelser**		
Advokat	21.4.-24.4.2020	1	3. mandskonti	2.3.2
Basisbank	06.06.- 30.08.2019	3	3. mandskonti	2.3.2
Borger	06.03.-27.04.2020	2	3. mandskonti	2.3.2
Borger	05.03.2020	1	3. mandskonti	2.3.2
Borger - Kunde i Danske Bank	08.01.2020	1	Notifikation	2.3.1
Coop bank	22.4.2020	3	Datadeling	2.3.3
Danske Bank	08.01 -10.1.2019	4	Ændring af NemKonto - Konkret mistanke	2.2: Finans Danmark
Dansk Kredit Råd	07.09.2018	1	Invitation til at deltage i møde	
Finans og Leasing	01.02.2016 og 06.07-18.09.2017	3	3. mandskonti, Datadeling	2.3.2, 2.3.3
Finans Danmark	12.10.2018	2	3. mandskonti, Datadeling, Notifikation	2.3.1, 2.3.2, 2.3.3
Finans Danmark	8.3.2018-24.7.2018	5	3. mandskonti, ændring af konti	2.3.1, 2.3.2, 2.3.3
Finans Danmark, Dansk Kreditråd	06.07-16.07.2018	2	Svindel med NemID og NemKonto	2, 3
Finans og Leasing	11.3.2019	1	3. mandskonti	2.3.2
Finans og leasing	17.06-22.6.2020	2	3. mandskonti	2.3.2
Forum for økonomisk IT-kriminalitet (FIT)	18.05.-25.05.2020	2	3. mandskonti	2.3.2
Forum for økonomisk IT-kriminalitet (FIT), afsendt af Finans og Leasing	3.6.2020	1	3. mandskonti	2.3.2
KMD	3.6.-18.06.2020	2	Datadeling	2.3.3
NemID produktgruppemøde den 25. april 2018	25.4.2018	1 Mødereferat	3. mandskonti	2.3.2
NemID produktgruppemøde den 30. nov. 2017	30.11.2017	1 Mødereferat	3. mandskonti	2.3.2
Nets	22.1.2018	1	3. mandskonti	2.3.2
Politiet	12.09.2019	1	Efterforskning i sag om bedrageri/svindel	
Total : 21 henvendelser.		***38 henvendelser (ekskl. mødereferater).***		
Supplerende *materiale**				
Finans og Leasing	04.06.2015	1	Datadeling	2.3.2
Finans og Leasing	29.09.2017	1	3. mandskonti	2.3.2
Finans og Leasing	19.12.2019	2	3. mandkonti, datadeling	2.3.2, 2.3.3.
Skattestyrelsen	12.10.2018	1	Datadeling	2.3.3
Finans og Leasing	21.10.2020	1	Opfølgning på møde	
Finans og Leasing, Finans Danmark	24.11.2020-25.11.2020	2	Høringssvar udkast om bekendtgørelse om NemKonto-ordningen	

*Supplerende materiale udgør materiale, som ikke indgik i det materiale, Danmarks Radio tidligere har fået aktindsigt i, men som vurderes at være relevant ift. redegørelsen. Digitaliseringsstyrelsen har derfor foretaget en ny delafgørelse om materialet, som er sendt til Danmarks Radio. Hertil kommer dialog som har fundet sted efter afgørelsen om den oprindelige aktindsigt blev sendt til Danmarks Radio. Høringssvar til udkast om bekendtgørelse om NemKonto-ordningen er desuden tilføjet i tabellen under 'Supplerende Materiale'.

Digitaliseringsstyrelsen har optalt antal dage fra den første henvendelse i en tråd er modtaget, til der er svaret på den. I fem af henvendelserne er der ikke svaret inden for 10 dage, som er styrelsens interne frist for svar.

Digitaliseringsstyrelsen har deltaget i møder med interessenter som fx bankernes interesseorganisation Finans Danmark (FIDA); interesseorganisationen for finansieringsselskaber, Finans og Leasing; enkelte pengeinstitutter samt i Forum for Økonomisk it-kriminalitet (herefter FIT), hvor Finans Danmark og Finans og Leasing deltager sammen med bl.a. Rigspolitiet og Skatteforvaltningen. Dette med henblik på at afdække problemstillingen med svindel med NemID og efterfølgende svindel med NemKonto og for aktivt at afsøge løsningsmuligheder og afklare problemets omfang.

I det følgende gennemgås henvendelserne i *tabel 1*, grupperet efter interessent:

Finans Danmark

- November 2017: Møde om NemID-nøgleapp, hvor eksempler på svindel med NemID og NemKonti, som flyttes til 3. mandskonti blev omtalt.
- Januar 2018: Produktgruppemøde om NemID-nøgleapp, hvor mulige scenarier for svindel med NemID drøftes, herunder efterfølgende svindel med NemKonto og håndtering heraf.
- April 2018: Produktgruppemøde, hvor svindel med NemID drøftes, herunder at omfanget af phishing-sager ses at være dalende, men at der er en stigning i voice-phishing (svindel over telefonen).
- Marts 2018 og frem: Dialog som leder op til et møde 1. maj 2018. På mødet angives, at der er kendskab til ca. 50 sager, hvor NemID anvendes til at ændre en NemKonto som led i svindel. Svindlen kan bestå i, at der fx optages kviklån. FIDA tilkendegiver dog også i henvendelsen fra marts 2018, at det er en meget lille del af de samlede ændringer af NemKonti, der foretages af kriminelle. Muligheder for håndtering drøftes. Digitaliseringsstyrelsen kontakter KMD for afklaring om mulighed for dataudtræk med henblik på indikation af svindel, *jf. afsnit 2.3.3*.
- September 2018: Digitaliseringsstyrelsen deltager i et møde i september 2018 med oplæg om danskernes informationssikkerhed.
- April 2018: Nordea henvender sig til Digitaliseringsstyrelsen med henblik på etablering af kontakt til Skattemyndighederne, da Nordea ser tegn på svindel med udbetalinger fra SKAT.
- Januar 2019: Digitaliseringsstyrelsen modtager henvendelse fra Danske Bank, hvor der omtales mistanke om uberettiget anvendelse af NemID til at ændre en kundes NemKonto. Digitaliseringsstyrelsen går i dialog om sagen, som viser sig ikke at være aktuel grundet misforståelse hos den konkrete borger.
- April 2020: Dialog med COOP bank om en forespørgsel på, om der er en service, som udstiller NemKonto i forhold til et CPR-nummer, samt mulighed for straksbetalinger.

Finans og Leasing

- Juni 2015: Finans og Leasing henvender sig til Digitaliseringsstyrelsen med et spørgsmål til data omkring NemID og NemKonto. Spørgsmålene besvares.
- Februar 2016: Finans og Leasing henvender sig til Digitaliseringsstyrelsen om muligheder for, at banker kan få adgang til data om borgeres NemKonto med henblik på at modvirke svindel, og der spørges ind til et planlagt forum til bekæmpelse af svindel. Der er ikke i journalsystemet fundet oplysninger om selve henvendelsen eller besvarelse umiddelbart i 2016. Der er fundet svar afsendt efter en rykker med genfremsendelse i juli 2017. Det fremgår af senere korrespondance, at det efterspurgte forum (netværk til bekæmpelse af it-relateret kriminalitet), faktisk blev nedsat i foråret 2016. Mailen fra februar 2016 er den eneste, hvor der ikke er fremfundet en besvarelse, som er afsendt umiddelbart efter henvendelsen, men først efter rykkeren, jf. nedenfor.
- Juli 2017: Finans og Leasing rykker for svar på mailen fra februar 2016, og der genfremsendes notat fra Finans og Leasing med problemstillinger og forslag til tiltag i relation til NemID og NemKonto. Digitaliseringsstyrelsen udarbejder et notat, hvor der svares på de konkrete punkter, blandet andet at Digitaliseringsstyrelsen og KMD har analyseret på muligheder for at tilpasse NemKonto-løsningen *jf. afsnit 2.3*.
- September 2017: Dialogen fortsætter. Finans og Leasing redegør for kendskab til 20-30 sager, hvor en NemKonto er ændret til at pege på en konto med tilknytning til en it-kriminel. Finans og Leasing redegør også for, at denne type svindel ser ud til at være blevet mindre, og at det aktuelle billede er, at en it-kriminel stjæler et NemID, og opretter fx et kviklån med brug af det stjålne NemID. Lånet udbetales via låntagers NemKonto, hvorefter offerets NemID misbruges til at overføre midlerne fra bankkontoen til den it-kriminelle.
- Marts til juli 2019: Dialog mellem Finans og Leasing og NemID om mulighed for et møde efter folketingsvalget i sommeren 2019 om tiltag mod svindel fra Finans og Leasing. Efter folketingsvalget svarer Digitaliseringsstyrelsen Finans og Leasing på deres forslag *jf. afsnit 2.3*.
- Juni til august 2019: Dialog med Basisbank om en svindelsag, og sager med brug af 3. mandskonti til svindel.
- Oktober 2019: Møde afholdes mellem Finans og Leasing og Digitaliseringsstyrelsen om tiltag mod svindel. Finans og Leasing spørger til mulighed for manuelle kontroller før udlevering af NemID og ændring af NemKonto. Det aftales, at Finans og Leasing skal vende retur med bearbejdet forslag. Forslagene blev drøftet på møde i FIT i maj 2020.
- Juni 2020: Efter henvendelse fra Finans og Leasing oplyser Digitaliseringsstyrelsen, at styrelsen stadig afventer Finans og Leasings aftalte bearbejdning af forslag fra 2019. Digitaliseringsstyrelsen drøfter muligheder med KMD omkring mulige tiltag og det er aftalt, med Finans og Leasing, at afholde et opfølgende møde inden sommeren 2021.

FIT (Forum for Økonomisk IT-kriminalitet)

- Maj 2020: NemKonto tages op i en drøftelse i FIT, der blandt andet kom ind på spørgsmålet om, hvorvidt man i NemKonto-løsningen har adgang til at se

ejerskabet for en given konto. På baggrund af mødet fremsendte Finans og Leasing en række konkrete spørgsmål omkring oplysninger i NemKonto. Digitaliseringsstyrelsen er fortsat i dialog med Finans og Leasing om konkrete NemKonto-data.

Andre henvendelser og håndteringen heraf

- September 2019: Politiet henvender sig vedrørende mulighed for indsigt i NemKonto-oplysninger i forbindelse med efterforskning af en sag. Der henvises til at politiet kan få indsigt i NemKonto-oplysninger ved henvendelse til leverandøren, KMD.

Borgerhenvendelser

- Juni 2019: Digitaliseringsstyrelsen reagerer på at der på Twitter beskrives en sag, hvor udviklingshæmmet har fået franarret sit NemID, der efterfølgende er brugt til at skifte NemKontoen og optage kviklån.
- Marts 2020: Dialog med borger, som har spørgsmål omkring identitetstyveri. Borgeren spørger til adviseringsmulighed via e-Boks (Digital Post) ved ændring af NemKonto *jf. afsnit 2.3.1*. Der følges op med svar til borgeren.
- April 2020: Advokat spørger til kontrol af anvisninger af NemKonto via selvbetjening, særligt med henblik på sager om svindel med NemID *jf. afsnit 2.3.2*. Der følges op med svar.
- Januar 2020: Borger spørger til mulighed for at godkende ændring af NemKonto, så løsningen udstyres med et signeringsmodul som i en netbank. Der følges op med svar.
- Marts 2020: Borgerhenvendelse til Justitsministeriet om digital sikkerhed oversendes til finansministeren for besvarelse. Borger har været udsat for identitetstyveri, inkl. ændring af NemKonto. Finansministeren besvarede henvendelsen.

Gennemgangen viser at Digitaliseringsstyrelsen har reageret på indkomne henvendelser om svindel og er gået i aktiv dialog med interessenterne blandt andet med fokus på at afsøge problemomfang og undersøge markører for svindel samt muligheder for håndtering af påpegede problemstillinger.

2.2 Digitaliseringsstyrelsens behandling af forslag til ændringer i NemKonto

Som det fremgår af hændelsesforløbene i foregående afsnit, har Digitaliseringsstyrelsen løbende haft aktiv dialog med de centrale interessenter vedrørende NemKonto-løsningen. For at opretholde sikkerheden i NemKonto-løsningen bredt set gennemgår løsningen en løbende, tilbagevendende sikkerhedsindsats i regi af Digitaliseringsstyrelsen og leverandøren. Dette er nærmere beskrevet i afsnit 2.5. Af de indkomne forslag til håndtering, er det langt fra alle, der vurderes virksomme eller hensigtsmæssige i forhold til fx brugere eller intentioner i lovgivningen. Der er også indkomne forslag, der vurderes teknisk eller økonomisk uhensigtsmæssige at implementere i den eksisterende og komplekse NemKonto-løsning. Andre input er spillet ind i arbejdet med Ny NemKonto. Da digital svindel med en borgers

NemKonto kun kan forekomme afledt af identitetstyveri af NemID, har Digitaliseringsstyrelsen sat ind over for svindel med NemID med en række forskellige tiltag. Ved at reducere svindel med NemID bliver der effektivt sat ind ift. at reducere risikoen for svindel med NemKonto.

Vurdering af input og overvejelser om tiltag til at forbedre sikkerheden i regi af NemID fremgår af afsnit 3 og uddybes i afsnit 3.2.

Omdrejningspunkterne for de ovenfor beskrevne henvendelser kan overordnet fordeles på følgende temaer vedr. svindel, *jf. tabel 1*:

1. Forslag om at indføre notifikation til borgere ved ændring af NemKonto, fx via NemSMS eller Digital Post.

2. Advarsler om svindel med 3. mands konti og forslag til at begrænse muligheden for anvisning af 3. mands konti, herunder mulighed for at begrænse at flere anviser samme bankkonto.

3. Forslag til højere grad af datadeling eller udstilling af data fra NemKonto-løsningen.

2.2.1 Forslag til forbedring af sikkerhed ved at indføre notifikation ved ændring af NemKonto, fx via SMS eller Digital Post
Svindel med en borgers NemKonto kan først finde sted, når en borger har fået franarret sit NemID. It-kriminelle vil dermed have mulighed for at tilgå borgerens Digital Post og for at ændre det telefonnummer, der skal modtage NemSMS. Tiltag af denne type vil derfor næppe være virksomt. Borgerne har ikke afgivet telefonnumre i NemKonto-systemet, men selv hvis de havde, ville it-kriminelle også kunne ændre dette, såfremt de havde foretaget identitetstyveri af NemID og dermed kunne logge ind i selvbetjeningsløsningen.

Udsendelse af meddelelser i forbindelse med ændring af NemKonti har været overvejet, men blev på tidspunktet vurderet ikke at være hensigtsmæssigt. Digitaliseringsstyrelsen har ikke modtaget oplysninger om et omfattende omfang af svindel fra Rigspolitiet, fx i regi af FIT. Digitaliseringsstyrelsen afventede derfor Ny NemKonto-projektet med henblik på at kunne indføre en adviseringsmodel.

Det bemærkes, at Digitaliseringsstyrelsen for at styrke tiltag mod svindel har valgt at gennemføre en proces for udsendelse af fysiske aktiveringsbreve ved ændringer af NemKonto via selvbetjening i den nuværende løsning, hvilket implementeres i april 2021. Det er i den forbindelse vurderet, at det øgede besvær, dette giver for ca. 100.000 borgere om året, i den nuværende situation opvejes af den øgede tryghed, som det ekstra sikkerhedstjek gennem aktiveringsbrevet giver.

2.2.2 Advarsler om svindel med 3. mands konti og forslag til at begrænse muligheden for anvisning af 3. mands konti, herunder mulighed for at begrænse, at flere anviser samme bankkonto

Forslag herom vedrører muligheden for, at borgere registrerer en bankkonto, som ikke er i deres navn (3. mandskonto), som deres NemKonto. Fx har Finans og Leasing foreslået, at det ikke skal være muligt at skifte NemKonto, samt at det kun skulle være muligt, at ét CPR nummer peger på én NemKonto. Og endelig går et forslag ud på, at man kun skal kunne vælge en anden NemKonto blandt andre konti, som man selv er ejer af i en bank.

De nævnte forslag indebærer, set fra et borgerperspektiv, en rigiditet, som for en stor del må vurderes uhensigtsmæssig og i strid med intentionerne i lovgivningen om fleksibilitet i NemKonto-løsningen i forhold til borgerne. Fleksibiliteten skal muliggøre, at fx par kan have samme NemKonto. Dette har understøttet, at Digitaliseringsstyrelsen ikke er gået videre med disse forslag.

Digitaliseringsstyrelsen blev i 2018 af FIDA oplyst om en situation, hvor der er lavet mere end 100 udbetalinger til forskellige CPR-numre via NemKonto til den samme bankkonto. Digitaliseringsstyrelsen gennemførte derfor i 2018 en stikprøvekontrol på situationer, hvor mange borgere havde ønsket den samme bankkonto som deres NemKonto. Stikprøvekontrollen viste, at der ikke var tegn på svindel i de gennemgåede cases. Stikprøvekontrollen fandt, at udenlandske firmaer eller lønbureauer ofte får udbetalinger til flere CPR-numre via NemKonto til samme bankkonto på vegne af en række arbejdstagere, der arbejder eller har arbejdet i Danmark. Der er tale om firmaer, der tager sig af danske forhold omkring fx skat med videre på vegne af arbejdstageren.

Meldinger til Digitaliseringsstyrelsen fra interessenterne har ikke entydigt kunnet fastlægge omfanget af svindelen. Volumen i størrelsesordenen 20-50 svindelsager med NemKonto har været nævnt, ligesom det har været fremført, at der kan være et mørketal. På baggrund af dette samt arbejdet med et kommende udbud af NemKonto-løsningen, har vurderingen været, at ressourcerne mere hensigtsmæssigt kunne benyttes til at sikre forbedringer i den nye løsning fremfor at foretage tilretninger, der måske først ville slå igennem tæt på tidspunktet for lancering af en ny NemKonto-løsning. Intentionen var derfor at sikre håndtering af problematikker rejst af fx FIDA og Finans og Leasing gennem arbejdet med en ny NemKonto-løsning.

Der er med Finansloven for 2021 opnået bevilling til at påbegynde udbud af ny NemKonto-løsning, som forventes i drift i 2023. Der introduceres forinden i april 2021 udsendelse af fysiske aktiveringsbreve ved ændringer af NemKonto, jf. afsnit 2.3.1 for uddybning.

2.2.3 Forslag til højere grad af datadeling eller udstilling af data fra NemKonto-løsningen
Data kan være en måde at finde markører på cases, hvor der foregår svindel med NemKonto. Der sker i dag i nogen grad en dataudveksling mellem NemKonto-løsningen og pengeinstitutterne i form af de meddelelser, der sendes til bankerne i systemet om fx oprettelse og ændring af NemKonti. Dog er der i NemKonto ikke

data, der alene vil kunne identificere svindelsager, hvorfor de ville skulle køres sammen med data fra andre myndigheder og pengeinstitutter.

Nogle henvendelser har omhandlet forslag til registrering af nye data i NemKonto-løsningen, spørgsmål til data i NemKonto-løsningen eller forslag om at udstille data fra NemKonto-løsningen. NemKonto-løsningen er et ældre system, der giver meget begrænsede muligheder for at udtrække data, som kan indikere svindel gennem foretagelse af mønstergenkendelse i forhold til data eller anden avanceret databehandling. Implementeringen af disse forslag vil kræve store ændringer af den tekniske snitflade og er begrænset af, at nyudvikling i NemKonto-løsningen er begrænset som følge af udbudsreglerne. Det vurderedes derfor hensigtsmæssigt at indarbejde forslagene i den kommende Ny NemKonto-løsning. Digitaliseringsstyrelsen har, som gennemgangen oven for viser, aktivt taget stilling til forslag, men har også haft fokus på ikke at sætte tiltag i værk, hvis de har været forbundet med væsentlige uhensigtsmæssigheder.

2.3 Håndtering af NemKonto-svindel

Omfanget af svindel med NemKonto er generelt svært at fastlægge som følge af karakteren af data. Samlet er omfanget af svindel vurderet til at være meget lavt i forhold til det samlede omfang af transaktioner. Der har, i dialoger med Finans og Leasing samt Finans Danmark, været angivet kendskab til 30 eller 50 sager og kendskab til en mulig konto med 100 transaktioner (overførsler) rettet mod flere borgere, fra pengeinstitutternes side. Sagerne skal ses i sammenhæng med NemKonto-løsningens omfang, hvor der årligt foretages omkring 98 mio. udbetalinger fra offentlige myndigheder, ca. 30 mio. udbetalinger fra private udbetalere via NemKonto-løsningen, og der eksisterer mere end 6 mio. NemKonti i Danmark. I henvendelser om omfanget af svindel er der løbende gjort opmærksom på, at der kan være et mørketal, men det er også i andre henvendelser nævnt, at der har været perioder med dalende antal sager og en ændring i svindelmønstre.

For at opretholde sikkerheden i NemKonto-løsningen bredt set er løsningen omfattet af den løbende, tilbagevendende sikkerhedsindsats i regi af Digitaliseringsstyrelsen, som for NemKontos vedkommende er beskrevet i afsnit 2.4 samt kapitel 4. I forhold til svindel med NemKonto afledt af identitetstyveri har der desuden været fokus i Digitaliseringsstyrelsen på at nedbringe svindel med NemKonto ved at sætte ind over for svindel med NemID.

Gennem årene er der iværksat en række indsatser, som har skullet adressere identitetstyveri eller anden uretmæssig brug af NemID. Disse uddybes i kapitel 3, jf. nedenfor.

2.4 Generelle sikkerhedstiltag i NemKonto-løsningen

Digitaliseringsstyrelsen har løbende forholdt sig aktivt til sikkerheden i NemKonto-løsningen. I samarbejde med NemKonto-løsningens leverandør er der gennemført en række tiltag, der understøtter et højt sikkerhedsniveau i NemKonto-løsningen, heraf blandt andet følgende:

Sikkerhed i selvbetjeningsløsningen nemkonto.dk
På selvbetjeningsløsningen *nemkonto.dk*, hvor 16 pct. af de ca. 50.000 ændringer af NemKonti per måned gennemføres, er krypteringsstandarden (TLS) løbende løftet for at sikre, at udefrakommende ikke kan bryde ind i løsningen, mens en borger er ved at bruge den. Derudover er der sikret mod, at nemkonto.dk kan misbruges til phishing via DMARC-implementering eller blive udsat for angreb, der bevist overbelaster selvbetjeningsløsningen (DDoS-angreb). Der bliver løbende risikovurderet og taget stilling til om yderligere tiltag skal implementeres. De tiltag, der er gennemført, er med til at sikre, at man kun kan komme til borgerens data på nemkonto.dk med et NemID.

Transportlagsanalyse
Borgere kan alene få adgang til at se eller ændre egne kontooplysninger via NemKonto's selvbetjeningsløsning med brug af NemID. NemKonto-systemet i øvrigt interagerer med andre løsninger på system-til-system-basis. I foråret 2017 gennemførtes en sikkerhedsgennemgang af transportlagene i NemKonto, dvs. kommunikationen mellem NemKonto-løsningen og udbetaleres systemer. I rapporten blev det konkluderet, at en enkelt kommunikationsform burde udfases. Udfasningen pågår, og der udestår et begrænset antal udbetalere, der ikke har fortaget udfasningen endnu. Dette omfatter ikke borgeres anvendelse af NemKonto.

Derudover fremgik det af rapporten, at der var behov for at foretage opdatering af dokumentation og logning for to øvrige kommunikationsformer, hvilket blev gennemført.

Audit
I efteråret 2018 gennemførtes en audit af NemKonto-løsningen – dvs. en dybdegående undersøgelse - med særlig fokus på håndteringen af persondata (GDPR) og kontrolområder i ISO-27001-standarden for informationssikkerhed. Her blev der foretaget kontroller af håndteringen af GDPR og af de forskellige ISO-områder på tværs af løsningen. Auditten resulterede i en rapport uden forbehold, men med en række bemærkninger, primært til beskrivelse af arbejdsprocesser mv. hos leverandøren. Samtlige 20 bemærkninger på tværs af ISO-standarden og GDPR blev håndteret i henhold til anbefalinger fra revisor.

I 2021 gennemføres en ny audit i samarbejde med leverandøren og i 2. kvartal af 2021 en sikkerhedstest (penetrationstest) ved en ekstern specialist.

Sikker administration af NemKonto-løsningen ved Kammeradvokaten
Op til 2018 blev forvaltningen af NemKonto-løsningen varetaget af et begrænset antal medarbejdere. Derefter blev der prioriteret flere ressourcer til området, og der blev igangsat gennemgange af løsningen med forskellige fokusområder. Sikkerhed i it-løsninger handler også om de administrative processer, der omgiver dem. Det var vurderingen, at selve forvaltningen af løsningen ville have gavn af et juridisk gennemsyn.

Kammeradvokaten analyserede fra ultimo 2018 til primo 2019 en række juridiske problemstillinger ved forvaltningen af NemKonto-ordningen. Forbedringstiltagene kredsede særligt om rammerne for manuelle anvisninger af NemKonti, etablering af procedurer for indsigtssager, samt tilsyn med KMD's support. De opfølgende tiltag på analysen er stort set gennemført, og i dag udestår kun enkelte justeringer omkring procesafgørelser hos leverandøren.

Eksempler på udviklingstiltag mhp. administrativ sikkerhed
Som eksempler på udviklingstiltag, der adresserer administrativ sikkerhed, kan nævnes implementering af 2. godkender på området for såkaldt *specifik konto* i NemKonto-løsningen; Der implementeres afsendelse af aktiveringsbrev til borgere, som ønsker en specifik konto (en specifik konto anvendes til at få en særskilt type udbetaling rettet mod en anden konto end borgerens NemKonto) anvist. En specifik konto kan altid kun anvises af en sagsbehandler i en udbetalende myndighed. Ved implementering af aktiveringsbreve for specifik konto skal borgeren godkende og aktivere kontoen som specifik konto via kode angivet i et aktiveringsbrev. Herved implementeres der for specifik konto samme godkendelses- og aktiveringsproces, som anvendes, når en sagsbehandler anviser en almindelig NemKonto.

Samlet set illustrerer ovenstående det kontinuerlige og brede fokus på sikkerhed i NemKonto-løsningen, som løbende udmøntes i faktiske sikkerhedstiltag.

2.5 Arbejdet med Ny NemKonto

NemKonto-løsningen er etableret på en kontrakt fra 2005, hvor den tekniske platform og funktionalitet løbende er blevet tilpasset. I dag er yderligere nyudvikling i NemKonto-løsningen begrænset som følge af udbudsreglerne. NemKonto-løsningen i dag er kendetegnet ved væsentlig kompleksitet, men også et omfang af teknisk gæld, blandt andet i form af en særdeles kompleks datamodel med hårde afhængigheder mellem elementer i løsningen. Derfor er det i stigende grad vanskeligt at videreudvikle på systemet og fx imødekomme efterspørgsel på udstilling af data.

Ny NemKonto-projektet skal sikre et kvalitetsløft af NemKonto-løsningen i form af en mere tidssvarende løsning, bedre mulighed for videreudvikling, nemmere administration og bedre brugerrejser og effektiviseringsgevinster i form af lavere driftsomkostninger. Ny NemKonto planlægges etableret gennem standardiserede og åbne snitflader, for at sikre fleksibilitet i forhold til brug af data og videreudvikling, som kan anvendes af udbetalere til at højne sikkerheden omkring udbetalinger.

I efteråret 2018 blev der igangsat en foranalyse og udviklet en tidlig prototype (proof of concept) for Ny NemKonto. I 2019 blev der nedsat et formelt projekt for Ny NemKonto, og etableret en styregruppe. På baggrund af projektets arbejde lå der i slutningen af 2019 et oplæg til videreførelse af projektet, herunder finansiering af aktiviteterne, som skulle søges. Bevilling til udviklingsprojekt blev i foråret

2020 indarbejdet i finanslovsforslaget for 2021, og efterfølgende opnået med Finansloven for 2021. Projektopstart blev således igangsat i 1. kvartal 2021.

3 NemID

NemID er den nationale elektroniske ID-løsning, som borgere anvender til login i både offentlige og private selvbetjeningsløsninger samt til netbank. NemID kan både anvendes som et sikkert login, til digital signering, samt validering af identitet. NemID blev lanceret den 1. juli 2010 i et samarbejde mellem staten og den danske banksektor. Løsningen er i dag et centralt element i den offentlige digitale infrastruktur og er en del af hverdagen for mange borgere og virksomheder. NemID har over 5,2 mio. brugere, og i 2020 blev der gennemsnitlig gennemført 38,5 mio. transaktioner om måneden.

NemID er sikret med en såkaldt to-faktor autentifikationsløsning, hvor borgeren har et element, som kun de kender: Brugernavn og adgangskode, samt et element, som borgeren er i besiddelse af fx nøglekort eller nøgleapp. Udover nøgleappen findes der andre supplementer til nøglekortet, herunder nøgleviser og en løsning for blinde og svagtseende borgere.

Den offentlige del af NemID er fællesoffentligt finansieret, hvor 40 pct. af midlerne fremkommer fra staten, 40 pct. fra kommunerne og 20 pct. fra regionerne. Det er Digitaliseringsstyrelsen, som er ansvarlig myndighed og håndterer leverandørstyring. Nets, der er leverandør og systemejer, har udviklet løsningen, er dataansvarlig og har ansvar for support.

Den eksisterende kontrakt med NemID udløber ultimo 2022. Udfasningen af NemID sker i forbindelse med overgangen til den næste generation af Danmarks nationale elektroniske identifikationsordning (eID), kaldet MitID og NemLog-in3, som Digitaliseringsstyrelsen lancerer i løbet af 2021.

3.1 Sikkerheden i NemID

NemID spiller, som nævnt, en hel central rolle for sikkerheden i NemKonto og i den samlede digitale infrastruktur. Der arbejdes løbende med sikkerhed på et højt niveau i NemID løsningen. Leverandøren er derfor også forpligtiget til at opretholde og levere en løsning, der opfylder god it-skik og gængse sikkerhedsstandarder. Dette er indarbejdet som elementer i kontrakten med leverandøren og afspejles i det daglige arbejde med løsningen. Digitaliseringsstyrelsen har fokus på, hvad leverandøren gør for at sikre bred tilgængelighed, høj oppetid af systemet, sikker opbevaring af data i løsningen samt opretholdelse af sikkerheden og beskyttelse mod uønsket adgang i løsningen. Leverandøren gennemfører blandt andet:

- Kode-reviews af NemID for at sikre, at systemet forsat er robust og ikke indeholder sårbarheder.
- Sårbarhedsscanninger samt årlig penetrationstest med henblik på at sikre, at NemID-systemet ikke indeholder sårbarheder, der kan udnyttes af hackere.
- Sporing af skadelig trafik og brugsmønstre i NemID-løsningens datacenter.

Ud over de ovennævnte aktiviteter, er der også implementeret en række konkrete tiltag i samarbejde med leverandøren, der forbedrer sikkerheden i NemID som fx:

- Implementering af DMARC-beskyttelse på flere NemID-domæner for at beskytte mod misbrug i forbindelse med fx phishing.
- Implementering af DDoS-beskyttelse, der beskytter mod ondsindet trafik mod NemID-løsningen og hermed øger løsningens robusthed i forhold til angreb fra uvedkommende.

Derudover har Digitaliseringsstyrelsen over årene foretaget en række ændringer, der har medført øgede krav til udstedelse af NemID, og som har imødegået forsøg på identitetssvindel i udstedelsessituationen:

- Ændring i krav til udstedelse, hvor der kræves fysisk fremmøde for øget validering af identitet inden udstedelse.
- Styrket identifikationskrav til udstedelse af NemID i borgerservice, der indebærer verifikation af pas/kørekort via NemID-portal ved opslag i politiets pas- og kørekortregister.
- Indførelse af enten kontrolspørgsmål baseret på cpr-data eller krav om vitterlighedsvidne ved udstedelse i borgerservice.
- Udvikling i NemID-portalen til borgerservicemedarbejder, der muliggør, at borgerservice kan sætte anmærkninger ved afvisning af udstedelse i NemID-portalen på tværs af alle kommuner. Dette er med til at forebygge uhensigtsmæssig udstedelse til borgere samt evt. misbrug af en borgers identitet.

Som del af robust forvaltning af NemID foretager leverandøren, Nets, tilbagevendende risikovurderinger, og der aftales løbende risikomitigerende tiltag. Udviklingen af NemID finder sted som en opvejning mellem reelle trusler, brugervenlighed, økonomi og løsningens levetid. Høj sikkerhed i NemID løsningen er derved et kontinuerligt fokus i forvaltningen af løsningen, der også udmønter sig i praktiske tiltag, der løbende har styrket sikkerheden og derigennem reduceret muligheden for svindel.

3.2 Risikohåndtering og mitigerende tiltag

I risikovurderingerne for NemID er det blevet konstateret, at NemID-løsningen er mest sårbar over for it-kriminelles forsatte forsøg på kompromittering af enkelte borgeres NemID-loginoplysninger med intention om at misbruge den pågældende identitet med økonomisk gevinst for øje. Da det ikke er muligt at sikre sig 100 procent mod svindel, kan it-kriminelle ikke stoppes fuldstændigt. Digitaliseringsstyrelsen arbejder altid i retning mod at nedbringe de eksterne trusler så effektivt som overhovedet muligt, netop for at gøre NemID mere sikker og dermed også de selvbetjeningsløsninger, der anvender NemID i forbindelse med login, fx NemKonto.

To områder har skilt sig ud som de vigtigste at adressere ud fra en risikobetragtning. Disse gennemgås her.

3.2.1 Keyloggere og mitigerende tiltag
En keylogger er en løsning, der installeres for at registrere alt, hvad der tastes på et tastatur, og kan være installeret i tastaturet, i computeren eller være en USB-nøgle, som er tilsluttet computeren. Hvis en borger bruger en computer, hvor der er installeret keyloggere, kan kriminelle opsnappe de oplysninger, som borgeren taster, fx NemID bruger-id, NemID-adgangskoder, kontonumre, adgangskoder til e-mail og lignende følsomme oplysninger. For at svindle med NemID er det dog ikke tilstrækkeligt at aflure borgernes bruger-id og adgangskode. De kriminelle skal også skaffe sig adgang til borgernes NemID nøglekort, hvilket de i de kendte sager har stjålet fra borgers postkasse.

I løbet af de ti år, hvor NemID har eksisteret, har der været to forløb, hvor keylogging er brugt til at franarre borgere deres NemID bruger-id og adgangskoder. Det er sket i 2017 og 2020. Der er nogle ligheder, men også betydelige forskelle mellem de to forløb med svindel. Uddybning af keylogger-problemet og Digitaliseringsstyrelsens opfølgning og håndtering følger nedenfor – herunder Digitaliseringsstyrelsens aktive stillingtagen til fem forslag til indsatser fra Nets, som også har været drøftet i forbindelse med samrådet den 25. februar 2021.

Keylogging i 2017
I 2017 orienterede leverandøren, Nets, Digitaliseringsstyrelsen om tilfælde af misbrug af NemID nøglekort. Kriminelle havde anbragt keyloggere på offentligt tilgængelige computere, der aflæste indtastninger, hvorved kriminelle fik adgang til borgerens bruger-id og adgangskode til NemID. Gennem den daværende funktion i NemID om 'Mistet nøglekort' på www.nemid.nu, spærrede gerningsmændene borgeres nøglekort, hvorefter et nyt nøglekort automatisk blev fremsendt til borgerens folkeregisteradresse. Gerningsmændene fandt herefter frem til borgerens adresse og afventede postleveringen med det nye nøglekort. Derefter stjal de det nye nøglekort fra borgerens postkasse og fik således fuld adgang til vedkommendes NemID.

For at forhindre denne type svindel implementerede Digitaliseringsstyrelsen sammen med bankerne i 2017 en ændring på nemid.nu således, at et nyt nøglekort ikke automatisk blev fremsendt, når borgere spærrede deres nøglekort. Når borgeres nøglekort er blevet spærret, skal de nu aktivt ind og bestille et nyt nøglekort og i den forbindelse valideres med dansk pas eller kørekort, før et nøglekort bliver fremsendt.

Digitaliseringsstyrelsen gjorde tilbage i 2017 KL opmærksom på, at så længe sikkerheden ikke var intakt på bibliotekerne, ville tekniske ændringer i NemID-løsningen ikke kunne afværge de kriminelles handlinger 100 pct. Digitaliseringsstyrelsen opfordrede derfor KL til at styrke sikkerheden på de offentlige tilgængelige computere for at sikre disse mod de kriminelles metoder. KL oplyste, at de havde rejst problematikken og sendt materiale og etableret et netværk i kommunerne, hvor erfaringer med sikkerhedsforanstaltninger kunne deles på tværs. Digitalise-

ringsstyrelsen satte også fokus på emnet på det halvårlige møde i et NemID forum med borgerservicemedarbejdere, hvor Digitaliseringsstyrelsen, Nets og repræsentanter fra KL og flere af landets kommuner videndeler om arbejdet NemID.

Keylogging i 2020
I 2020 orienterede leverandøren, Nets, Digitaliseringsstyrelsen om, at Østjyllands Politi efterforskede en sag, som mindede om svindelsagen fra 2017, da misbruget igen skete ved, at gerningsmændene anbragte keyloggere på offentligt tilgængelige computere. Med informationer opsnappet på keyloggerne havde gerningsmændene efterfølgende overvåget borgerens brug af NemID-nøgler for at finde ud af, hvornår borgeren ville få tilsendt et nyt nøglekort. Da de indtastede brugernavn og adgangskode i et login-flow med NemID, fik de oplyst, hvor mange nøgler der var tilbage på det eksisterende nøglekort, og dermed kunne de kriminelle få information om, hvornår et nyt nøglekort blev afsendt. Gerningsmændene brugte disse oplysninger til at stå klar ved borgerens adresse og stjæle det nye nøglekort fra borgerens postkasse for at få adgang til vedkommendes NemID.

For at undgå yderligere svindel valgte Digitaliseringsstyrelsen og bankerne i samarbejde at fjerne visningen af nøgler, så det blev sværere for kriminelle at udregne, hvornår et nøglekort ville blive fremsendt til borgeren.

Digitaliseringsstyrelsen opfordrede KL til at styrke sikkerheden yderligere på de offentligt tilgængelige computere. KL berettede, at de igangsatte en række målrettede initiativer, herunder tekniske anbefalinger til kommuner, medarbejdervendte vejledninger samt opkvalificering af de it-ansvarlige på landets biblioteker og borgercentre. NC3 (Nationalt Cyber Crime Center i Rigspolitiet) har stået for undervisning, og Rigspolitiet har udarbejdet en vejledning, som er tilsendt alle kommuner.

KL har orienteret Digitaliseringsstyrelsen om, at der er blevet afholdt undervisning, og det forventes, at der gennemføres yderligere kurser i foråret 2021. Herudover har KL orienteret om, at der igen er blevet etableret et informationssikkerhedsnetværk på tværs af kommunerne, som understøtter vidensdeling på tværs og skærper sikkerhedsarbejdet. Hertil berettede KL, at mange kommuner eksempelvis fra 2017 og årene frem har implementeret et system (OS2BorgerPC), som blandt andet kan blokere for, at der kan indsættes fysiske USB-enheder som fx keyloggere i computeren. Andre kommuner har udviklet et nyt system sammen med en privat leverandør, hvor tastaturet er inkorporeret i skærmen, hvilket sikrer, at kriminelle ikke kan bruge keyloggere i tastaturet. Digitaliseringsstyrelsen har derved aktivt i samarbejdet med bankerne og leverandøren reduceret mulighed for svindel, og har fulgt op på sikkerheden omkring offentligt tilgængelige computere i dialogen med KL.

Håndtering af ændringsforslag fra Nets i forbindelse med keylogging
I forbindelse med keyloggersagen fra 2020 fremsendte Nets et forslag om at fjerne visning af antal nøglernøgler på nøglekortet, som et led i at imødegå fremtidig

svindel. Digitaliseringsstyrelsen havde en række bekymringer ved at fjerne visningen, da oplysningerne blandt andet tydeliggjorde, hvornår borgerne skulle holde øje med postkassen. Digitaliseringsstyrelsen stillede derfor Nets en række afklarende spørgsmål for at afsøge en dækkende løsning i forhold til de kriminelles svindelmetode. I dialogen valgte Nets at præsentere yderligere fem forslag til sikkerhed, der potentielt kunne imødegå udfordringen med kriminelle og keyloggere yderligere. Nets betryggede efterfølgende Digitaliseringsstyrelsen i, at løsningen med fjernelse af nøglevisningen ville afværge den metode, som de kriminelle har anvendt til at aflure forsendelsestidspunktet for nyt nøglekort til borgers postkasse uden nye risici. På baggrund af dette, samt yderligere oplysninger fra Nets om eksisterende sikkerhedsfunktioner i NemID løsningen, valgte Digitaliseringsstyrelsen at gennemføre forslaget om fjernelse af visning af antal nøgler på nøglekortet.

Nogle af de fem forslag var tidligere blevet undersøgt og vurderet i henhold til økonomi og løsningens levetid, mens andre af forslagene blev besluttet indarbejdet i det kommende MitID. I vurderingen af forslagene blev der også lagt vægt på tidsplanen for den kommende MitID-løsning, der skulle lanceres inden for et år fra forslagene blev fremlagt, og de økonomiske omkostninger set i relation til NemID's resterende levetid.

De fem forslag drejede sig om:

1. <u>It-sikkerheden omkring brug af offentligt tilgængelige computere.</u>
   I forbindelse med de to keyloggersager i 2017 og 2020 har Digitaliseringsstyrelsen i begge tilfælde opfordret KL til styrke sikkerheden yderligere på de offentligt tilgængelige computere. Dette forslag er der derved fulgt op på *jf. dette afsnit* om dialog med KL ovenfor.

2. <u>Fortsat oplysning til brugerne om valg af brugernavne og adgangskode, samt afskaffe brugen af CPR-nummer som bruger-id.</u>
   Digitaliseringsstyrelsen indarbejder løbende budskaberne om sikker brug af NemID, herunder gode råd til, hvordan man laver en sikker og unik adgangskode, i kampagner og diverse initiativer for at højne kendskabet til sikker adfærd på nettet. Dette skete også allerede inden, Nets fremlagde forslaget.

   En central løsning i NemID har altid været brug af CPR-nummer som bruger-id, og en afskaffelse af dette vil være en omfattende ændring i løsningen og med en lang tidshorisont for implementering.

   I NemID-løsning har brugerne dog mulighed for at slå denne funktion fra manuelt, så det ikke længere vil være muligt at anvende CPR-nummer til borgerens NemID. Dette har været implementeret i løsningen, allerede inden forslaget blev fremlagt.

Ved vurderingen af dette forslag blev der desuden lagt vægt på, at det i den kommende løsning, MitID, ikke vil være muligt at bruge CPR-nummer som bruger-id, og derved afskaffes denne funktion ved overgangen til MitID.

3. Udfasning af nøglekort.
Udfasning af nøglekortet i NemID ville være en vidtrækkende og fundamental ændring i løsningen, da nøglekortet udgør selve grundpillerne i den nuværende NemID-infrastruktur, og dermed også i den løsningsbeskrivelse, der indgik i udbuddet i 2008. Andre identifikationsmidler som nøgleviseren og nøgleappen, udstedes på baggrund af et eksisterende nøglekort. Derved ville udfasningen af nøglekortet være en helt fundamental ændring af løsningen, der er blevet anslået til at koste et 3-cifret millionbeløb og som ville have en lang udviklings- og implementeringstid. Det blev vurderet, at nøglekortet ikke kan udfases i medfør af NemID kontrakten, uden at dette ville give anledning til udbudsretlige problemer, samtidig med at det ville være økonomisk uforsvarligt ift. den nærtforestående overgang til MitID.

Ved vurderingen af forslaget blev der lagt vægt på, at NemID nøglekortet udfases med MitID, der lanceres i 2021. I MitID vil nøglekortet blive erstattet af en app, en nøgleviser eller chip.

4. Indføre notifikationer i forbindelse med udvalgte hændelser i NemID.
Der er i NemID-løsningen i dag en underretningsfunktion, der bevirker, at hvis en borger ændrer sit telefonnummer/e-mail i NemID, så vil der blive sendt en sms/mail til det oprindelige telefonnummer/mail, såfremt borgeren har registreret dette. Formålet er at advisere om et eventuelt svindelforsøg i de tilfælde, hvor borgere ikke selv har foretaget ændringen.

Der er dog i NemID-løsningen ingen notifikationer om borgeres adfærd med deres NemID, som fx advarsel ved login fra ny enhed. Digitaliseringsstyrelsens arbejdede på at indføre notifikationer omkring adfærdsændringer sammen med bankerne allerede i oktober 2019. Notifikationer om adfærd vil dog ikke have en funktion, medmindre der er indsamlet kontaktinformationer om brugeren, fx mailadresse eller telefonnummer, som der kan sendes hhv. mail eller sms til. I NemID-databasen er der ikke kontaktoplysninger på alle brugere, og førend dette eksisterer og er valideret tilstrækkeligt, vil der heller ikke kunne udsendes notifikationer til disse NemID-brugere om ændringer i løsningen. Denne leverance vil derfor have en lang implementeringstid.

Bankerne valgte at trække sig fra initiativet i marts 2020 grundet den nært forestående overgang til MitID-løsningen, hvilket betød, at Digitaliseringsstyrelsen ville skulle gennemføre finansieringen og implementeringen alene. På grund af den meget nært forestående overgang til MitID-løsningen efter afslutning af udbud og implementering samt økonomien forbundet hermed besluttede Digitaliseringsstyrelsen ikke at gå videre med initiativet.

5. Sætte brugere i karantæne/spærre/notificere bankerne, såfremt der detekteres en adfærd med en vis mængde logins, der ikke gennemføres.
   Der er ikke indført en karantænemulighed i NemID, men der er indarbejdet forskellige sikkerhedsmekanismer i NemID-løsningen i dag, særligt i forhold til spærring ved fx gentagne fejl-log-ins. Disse mekanismer var implementeret allerede inden, forslaget fra Nets blev fremlagt.

Digitaliseringsstyrelsen har altså samlet set foretaget en aktiv vurdering af relevans og hensigtsmæssighed af alle fem forslag. Nogle af forslagene var implementeret på tidspunktet for fremsættelse af forslagene, mens andre adresseres i den kommende MitID-løsning.

3.2.2 Phishing og mitigerende tiltag
I de tilbagevendende risikovurderinger for NemID udgør phishing den mest aktive trussel rettet mod NemID-slutbrugerne. Phishing er it-kriminelles forsøg på at narre brugerne til at give deres NemID-oplysninger (brugernavn, adgangskode, engangsnøgler), fx ved at gerningsmænd udgiver sig for at være fra politiet, Nets eller en navngiven bank, eller ved fx at oprette en falsk hjemmeside, der opfordrer borgerne til at uploade billede af deres nøglekort.

Digitaliseringsstyrelsen yder en særlig indsats sammen med leverandøren om at forsøge at nedbringe risiko for phishing ved at foretage nedtagning af blandt andet falske hjemmesidder, men også andre applikationer, der forsøger at franarre borgere deres NemID-oplysninger. Leverandøren har løbende gjort dette, både på egen foranledning og på opfordring fra Digitaliseringsstyrelsen.

Endvidere har Digitaliseringsstyrelsen et samarbejde med Center for Cybersikkerhed under Forsvarsministeriet (CFCS), som foretager overvågning af hjemmesider, der præsenterer en falsk NemID-loginklient. CFCS har med input fra Digitaliseringsstyrelsen formuleret en liste af søgeord med henblik på at spore falske hjemmesider. Screeningen fungerer således, at CFCS overvåger internettet ud fra en række bestemte søgeord og kompositioner, der optræder i bestemte sammenhænge. Herefter kan CFCS med korrekt lovhjemmel fortage en nedtagning af hjemmesiden, hvis den viser sig at være falsk, samt orientere og aktivere politiet i forhold til den videre efterforskning. CFCS udsender adviseringer om de konkrete phishing-forsøg til borgere i den gratis app 'Mit Digitale Selvforsvar'.

CFCS rapporterer løbende til Digitaliseringsstyrelsen om screening af aktuelle phishing-forsøg for at sikre, at Digitaliseringsstyrelsen er orienteret om aktuelle tendenser inden for phishing. Dette med henblik på at berige kommunikationen på hjemmesider og informere supportpersonale, så de kan vejlede borgere på bedste vis.

3.2.3 Brugeradfærd, phishing og mitigerende tiltag
Den kvartalsvise risikovurdering fra leverandøren har endvidere vist, at en af de største sårbarheder i NemID hænger sammen med brugernes adfærd som følge af

phishing, hvor borgeren bliver lokket eller kommer til at dele sine oplysninger, fx deres bruger-id via eksempelvis en falsk hjemmeside.

Ved udstedelse af NemID skal borgeren godkende regler for brug af NemID, hvori det påpeges, hvorledes borgeren skal anvende og opbevare deres NemID, samt at NemID'et aldrig må deles må andre eller på anden vis kopieres. Desværre har Digitaliseringsstyrelsen erfaret, at nogle borgere er tilbøjelige til at udlevere deres NemID-oplysninger til autoriteter, såsom deres bank. Dette udnytter kriminelle, der opsøger borgeren og udgiver sig for at være fra deres bank.

Digitaliseringsstyrelsen har også erfaret, at en række borgere affotograferer deres nøglekort for at opbevare det på telefonen, hvilket har gjort dem sårbare over for forsøg på kompromittering af deres NemID, hvis telefonen bliver stjålet eller kriminelle får adgang til deres fotos. Denne risiko har Digitaliseringsstyrelsen søgt adresseret gennem information til borgerne og tydelige brugervilkår for NemID.

Digitaliseringsstyrelsen har aktivt arbejdet på at imødegå risiko for uhensigtsmæssig brugeradfærd. Mest udtalt er det sket ved lancering af NemID nøgleappen, som ikke indeholder synlige nøgler, som en kriminel kan aflure. Hertil er appen beskyttet af en række sikkerhedsforanstaltninger, samt krav om app-kode, fingeraftryk eller ansigtsgenkendelse for at åbne appen, som gør, at borgeren sikkert kan have deres NemID på deres telefon.

Sikker og fornuftig adfærd er en central del af al it-sikkerhed. Ud over aktioner som fx nedtagning af falske hjemmesider har Digitaliseringsstyrelsen stort fokus på at holde borgerne løbende orienteret om sikker digital adfærd og give konkrete råd til, hvordan de kan sikre sig mod identitetssvindel, fx informationskampagner og undervisningsmaterialer bl.a. i samarbejde med KL, Finans Danmark og Politiet. Derved søger Digitaliseringsstyrelsen aktivt at forebygge og nedbringe identitetstyveri af NemID og ligeledes svindel med NemKonto.

Digitaliseringsstyrelsen har efter keylogging-sagerne haft skærpet fokus på, hvordan borgerne beskytter sig bedst muligt mod svindel af NemID, blandet andet ved oplysningstiltag på bl.a. nemid.nu, sikkerdigital.dk og borger.dk om sikker digital adfærd, hvor det påpeges, hvor vigtigt det er, at borgerne ikke deler deres NemID-oplysninger med andre.

Digitaliseringsstyrelsen har udarbejdet en række faste gode råd om NemID, der udsendes i kampagner, på sociale medier, i de skriftlige svar til borgere, samt ved alle advarsler, som CFCS udsender om NemID-relateret phishing-adviseringer i den gratis app 'Mit Digitale Selvforsvar'.

3.2.4 Support i forbindelse med svindel
Digitaliseringsstyrelsen tager altid henvendelser omkring svindel, herunder phishing, alvorligt og håndterer løbende de aktuelle henvendelser og trusler mod NemID i tæt samarbejde med leverandøren.

I 2017 sikrede Digitaliseringsstyrelsen, at der blev indgået en aftale med leverandøren på baggrund af en øget mængde kriminel aktivitet omhandlende phishing, hvor leverandøren forpligter sig til følgende:

- Understøtte borgere, der har været udsat for NemID-svindel, og sikre, at de får den rette support ift. deres NemID, således at alle forbehold tages for at forebygge yderligere svindel med NemID, samt sikre, at borgerne kan få genudstedt et nyt NemID.
- Bistå myndigheder om sager, hvor der foregår politimæssig efterforskning. Det omhandler bl.a. om at levere udtræk af specifik information til politiet til brug i deres efterforskning af svindelsager.

Disse tiltag er yderligere medvirkende til at sikre opklaring og aktiv support i tilfælde af identitetstyveri af NemID.

3.3 Håndtering af henvendelser i NemID

Anledning til redegørelsen var blandt andet et ønske om en detaljeret gennemgang af henvendelser om NemKonto omtalt i forbindelse med aktindsigt og nyhedsudsendelse af Danmarks Radio. Som supplement til den detaljerede gennemgang af henvendelser om NemKonto følger her en opsummering på håndtering af henvendelser om NemID.

Digitaliseringsstyrelsens Visiteringsenhed er som udgangspunkt første kontaktpunkt for de borgere, som ringer eller skriver ind til Digitaliseringsstyrelsen med spørgsmål til support. Visiteringsenheden har fra 2019 til 2021 modtaget over 9.000 supporthenvendelser angående NemID-løsningen.

De systemspecifikke henvendelser, som håndteres i NemID-teamet, omhandler bl.a. sikkerheden i løsningen, hvor borgere, virksomheder eller myndigheder har spørgsmål til sikkerheden i løsningen, herunder spørgsmål til tekniske foranstaltninger, lovgivning eller til reglerne for brug af NemID.

Digitaliseringsstyrelsen har i forbindelse med keylogger-sagerne i 2017 og 2020 modtaget henvendelser fra borgere angående sagerne. Dette var blandt andet henvendelser fra borgere, som havde fået spærret deres NemID eller henvendelser fra borgere, som var nervøse for, om deres oplysninger kunne blive misbrugt. Systemforvalterne i NemID-teamet vejledte borgerne angående hændelsesforløbet, hvad borgeren skulle gøre ift. NemID, samt hvad borgerne kan gøre for at beskytte deres NemID fremadrettet.

Digitaliseringsstyrelsen modtager også forbedringsforslag i forhold til NemID. Forslagene omhandler alt fra kommunikationsrettelser til tekniske forslag. På baggrund af de oplysninger, som Digitaliseringsstyrelsen indsamler om forslag, kan der indgås en dialog med leverandøren, hvis det vurderes, at forslaget kan implementeres i forhold til teknikalitet, lovgivning, økonomi og brugervenlighed. Hvis forslaget giver anledning til justering i løsningen, drøftes dette med leverandøren.

I nogle af henvendelserne til Digitaliseringsstyrelsen vedrørende NemKonto, har der også indgået forslag til NemID-løsningen. Disse har blandt andet berørt forslag i forhold til hhv. udsatte borgere, indsigt i NemID-oplysninger og andre offentlige data.

I forhold til udsatte borgere er det blevet foreslået, at det skulle være registreret i NemID-løsningen, om borgeren bor på fx et bosted og, at disse borgeres brug af NemID skulle begrænses ved, at de kun måtte bruge NemID gennem en person med fuldmagt til den udsatte borgers NemID. Der er allerede i dag en selvbetjeningsløsning, der kan understøtte fuldmagter fx ved brug af den fællesoffentlige digitale fuldmagtsløsning. Samtidig gælder det, at NemID er strengt fortroligt, og borgere aldrig må give andre adgang til deres NemID. Det blev derved vurderet, at den foreslåede model ikke bør implementeres i NemID.

Et andet område, som har været berørt i henvendelserne, er mulighed for indsigt i NemID-oplysninger til brug for øget sikring af låneaftaler. Her er det blevet foreslået, at det skulle være muligt for virksomheder at se, hvornår et NemID er udstedt, og hvornår det udløber. Virksomheder skulle også have mulighed for at tjekke NemID-anvendelseshistorik, dvs. om registrerede oplysninger, tlf.nr., e-mail osv. lige er blevet ændret. Digitaliseringsstyrelsen har i den sammenhæng oplyst, at oplysninger om et NemID kan tilgås via selvbetjeningen på nemid.nu af NemID-ejeren selv samt, at oplysninger om udstedelse og udløb af et NemID's OCES-certifikat kan fremsøges ud fra mail eller CVR-nummer i certifikatdatabasen af eksterne, hvis NemID-ejeren tillader dette. Ligeledes kan oplysningerne om, hvornår et NemID's OCES-certifikat er udstedt, tilgås af modtageparten, hvis NemID anvendes til signering, fx i forbindelse med en låneansøgning. I forhold til anvendelseshistorik viser denne ikke noget om de konkrete handlinger, der er foretaget på baggrund af et NemID. NemID er udelukkende en login- og signeringstjeneste, og derved ved NemID ikke, hvilken handlinger der er udført på baggrund af en NemID-transaktion. Det er derimod op til tjeneste- eller låneudbyderen at sikre, at borgeren må indgå bindende aftaler fx låneaftaler. Da det på tidspunktet for forslaget allerede var muligt at se, hvornår et certifikat er udstedt hvis NemID anvendes til signering, og da det er tjeneste- eller låneudbyderne, der skal sikre, at de pågældende borgere kan eksempelvis optage lån, var det vurderingen, at det ikke var relevant at gå videre med disse forslag.

I forhold til fx at verificere en eventuel låntagers adresse og opholdsgrundlag har der også været forslag i henvendelserne om, at NemID'et skulle kunne oplyse om bopælsadresse, eventuelt værgemål, opholdsgrundlag, samt et varsel på et eventuelt ophør af opholdsgrundlag. Det vurderes ikke, at NemID-løsningens formål er at sammenstille og vise oplysninger vedr. opholdsgrundlag, værgemål, bopælsadresse mv., men at løsningen skal sikre valideringen af borgeren, der ønsker at tilgå en digital selvbetjeningsløsning. Det var derved Digitaliseringsstyrelsens vurdering, at låneudbydere der havde behov for disse oplysninger ved udstedelse af lån, skulle sikre dem ad anden vej end gennem NemID.

Digitaliseringsstyrelsen har altså aktivt forholdt sig til en række forslag, der dog ikke er blevet vurderet virksomme eller af andre årsager er blevet vurderet uhensigtsmæssige i forhold til implementering.

3.4 MitID

Med den kommende MitID-løsning er der indarbejdet en række sikkerhedstiltag, der øger sikkerheden og minimerer muligheden for svindel og identitetstyveri.

Med MitID er de nye identifikationsmidler afgørende i forhold til løsningens generelle sikkerhed. Med MitID udgår nøglekortet, og en række nye identifikationsmidler introduceres. Det mest almindelige bliver at bruge MitID app, som i store træk kommer til at minde om NemID nøgleappen. Derudover introduceres fysiske identifikationsmidler til borgere, der ikke har lyst til eller mulighed for at bruge en app.

I MitID indføres sikkerhedstiltag, som gør det lettere for borgere at verificere, at MitID-oplysninger indtastes på en pålidelig hjemmeside. I MitID vises mitid.dk-domænet altid som det sidste led i browserens adresselinje, når der laves autentifikation, ligesom oplysninger om, hvilken handling borgerne er ved at foretage også vil fremgå, når de benytter MitID.

Derudover benyttes notifikationer til at sikre, at borgerne altid bliver orienteret om kritiske hændelser i MitID. Borgerne har endvidere mulighed for at tilvælge notifikationer for andre typer hændelser, såfremt dette ønskes. Notifikationer er relevante for den samlede sikkerhed og er et af de områder, hvor MitID adskiller sig fra NemID.

Slutteligt implementeres der i MitID en risikodatamodel, som samler og rapporterer data og på denne måde etableres et stort informationsgrundlag, der skal understøtte at der kan træffes sikkerhedsmæssige beslutninger på baggrund af et samlet risikobillede.

Identitetssikring

Kravene til MitID er skærpede, fordi sikkerheden på it-området har ændret sig meget, siden NemID blev lanceret i 2010. Med MitID stilles der derfor højere krav til sikringen af brugernes identiteter. Det betyder, at en række af de nuværende NemID-brugere skal have opdateret deres oplysninger og bekræftet deres identitet i forbindelse med overgangen til MitID.

4 Digitaliseringsstyrelsens generelle arbejde med it-sikkerhed

Sikkerhed i it-løsningerne er ikke kun et spørgsmål om at reagere på eksterne henvendelser, men kræver en systematisk, tilbagevendende sikkerhedsindsats. Digitaliseringsstyrelsens har gjort en række tiltag for at sikre et højt sikkerhedsniveau i løsninger som NemID og NemKonto. De vigtigste tiltag gennemgås nedenfor.

Digitaliseringsstyrelsen arbejder systematisk med at højne it-sikkerheden i de digitale løsninger, og arbejdet er forankret i særligt ISO 27001 (herefter ISO-standarden), persondataforordningen (herefter GDPR) og den løbende leverandørstyring.

ISO-standarden er en international standard, der er indført som fælles standard i hele staten. Standarden understøtter en operationel og risikobaseret tilgang til systematisk arbejde med it- og informationssikkerhed med udgangspunkt i et ledelsessystem, der forankrer arbejdet med it-sikkerhed på de forskellige ledelsesniveauer i en organisation.

Arbejdet med GDPR er særlig forankret i databehandleraftaler mellem Digitaliseringsstyrelsen og leverandørerne af it-løsningerne, hvor der behandles persondata. Gennem leverandørstyring arbejder Digitaliseringsstyrelsen med at sikre kontrakten med leverandøren, hvor en række sikkerhedselementer er fastsat, herunder håndtering af fejl i løsningen og rammer for løbende dialog med leverandøren om fx sikkerhed.

Digitaliseringsstyrelsen gennemfører årlige risikovurderinger af blandt andet NemID- og NemKonto-løsningen og har som led i det tilbagevendende sikkerhedsarbejde etableret en compliance-funktion. Fokus i arbejdet er på at opretholde og tilsikre stabil og sikker systemforvaltning af de digitale infrastrukturløsninger.

Ved hvert årsskifte udarbejdes der et årshjul med konkrete opfølgningsindsatser målrettet de større it-systemer som fx NemID og NemKonto på Digitaliseringsstyrelsens ansvarsområde relateret til ISO-standarden og GDPR. Dette er for at sikre, at Digitaliseringsstyrelsens fokus på it- og informationssikkerhed i leverandørstyringen både har en konkret og handlingsorienteret udmøntning. Ledelsesforankringen styrkes ved blandt andet en halvårlig status til Digitaliseringsstyrelsens Informationssikkerhedsudvalg, hvor direktør samt relevante vicedirektører og kontorchefer orienteres om og drøfter beslutninger vedrørende progression i styrelsens arbejde med it-sikkerhed bredt set.

For at sikre forankring af it- og informationssikkerhedsdagsordenen afholdes der sikkerhedsmøder på operationelt ledelsesniveau.

For at understøtte den løbende vurdering, evaluering og kontrol af it-og informationssikkerhedssituationen i de større it-løsninger i Digitaliseringsstyrelsen, som fx NemID og NemKonto, er der blandt andet implementeret løbende egenkontroller, afholdelse af penetrationstest (sikkerhedstests), eksterne audits samt gennemførsel af eksternt tilsyn ved indhentning af revisionserklæringer hos leverandøren ligesom der er afholdt beredskabsøvelse, der har omfattet bl.a. NemKonto.