Digitaliserings-
styrelsen

Vejledning til
National Standard for
Identiteters Sikringsniveauer (NSIS)

Status: Version 2.5 (Høringsversion)

Version: 03.05.2024

1 Indledning

1.1 Ændringshistorik

Dato	Version	Ændringer
08.11.2022	2.3	Kravformuleringer er opdateret til at afspejle NSIS version 2.0.2 Referencer til hjemmesider og øvrige dokumenter opdateret og udbygget. Enkelte slåfejl er rettet. I indledningen til kapitel 3 er det forklaret, hvilke krav en lokal IdP skal overholde. Indledningen til afsnit 3.1.3 er udbygget med henblik på at præcisere, hvornår verifikation af juridiske enheder er relevant. I afsnit 4.1.3 er det præciseret, at en anmelder som i al væsentlig blot agerer som indkøber af en løsning, ikke er omfattet af kravene til ISO 27001-certificering eller tilsvarende på sikringsniveau Høj. Afsnit 4.1.7 om anmeldelse og revision er opdateret: • Det er præciseret, at det er tilladt at anvende andre formater end det Excel-baserede kontrolskema, blot tilsvarende indhold fremgår. • I krav 3 om intern revision er det præciseret, at kravet alene gælder niveau Lav, og der er indført krav om årlig genbekræftelse af anmeldelser på niveau Lav. • I krav 5 og 6 er det præciseret, at man kan anvende alternativer til kontrolskemaet med samme indhold (se også den opdaterede vejledning til dette punkt). Indledningen til kapitel 5 er udbygget med henblik på at forklare begrebet 'erhvervsbruger'. Indledningen til kapitel 6 er udbygget med henblik på tydeligere at beskrive identitetsbrokernes rolle, herunder at de udstiller en autentifikationsservice og indgår i tillidskæden for tjenesteudbydere.
30.01.2023	2.3a	Der er fjernet et overskydende "eller" fra krav 3.2.3 punkt 4. Opdateringen er mao. kun sproglig.

Dato	Version	Ændringer
12.06.2023	2.4	Vejledningen er udbygget til flg. krav: • 3.2.3 punkt 4) • 3.3.1 punkt 3) • 4.1.1 punkt 2) • 4.1.2 punkt 1) • 4.1.7 punkt 3) og 4) Der er tilføjet vejledning til flg. krav: • 3.2.3 punkt 6) • 4.1.5 punkt 5)
24.07.2023	2.4a	Rettet trykfejl i ændringshistorik til version 2.4, hvor henvisningen til 4.1.1 punkt 1) er ændret til punkt 2).

Dato	Version	Ændringer
03.05.2024	2.5	Opdateret efter survey og erfaringsopsamling med revisorer og andre interessenter: • Kontrol af legitimation (3.1.2) ved verifikation af fysiske personer samt retningslinjer for validering af digitale kørekort • Levering og aktivering (3.2.2), herunder fortolkning af kravene ved elektroniske udleveringsprocesser • Der er indført eksempler på hvornår automatisk spærring kan være aktuel (3.2.3) • Sikkerhed af autentifikationsmekanismer er udbygget (3.3.1) • Sikkerhedstest af autentifikationsmekanismer er udbygget (3.3.1) • Håndtering af underleverandører og deres ansvar er mere detaljeret beskrevet (4.1.1) • Der er beskrevet eksempler på alternativer til ansvarsforsikringer (4.1.1 punkt 4) • Bestemmelser vedr. oplysningspligt er udbygget (4.1.2) • Vejledning til ISMS er udbygget (4.1.3) • Krav til fysisk sikkerhed er udbygget (4.1.5 punkt 3) • Beskrivelser af betroede medarbejdere og baggrundstjek er udbygget (4.1.5 punkt 5) • Vejledning til nøglelængder og kryptografi er udbygget (4.1.5 punkt 7) • Håndtering af medarbejderidentiteter (kapitel 5) er væsentligt udbygget herunder vedrørende spærring og brug af autoritative kilder og procedurer for medarbejderes livscyklus. • Vejledning vedrørende omveksling af eIDAS til NSIS sikringsniveauer er indført til afsnit 6.1 og 6.2. • Forhold vedr. sessionstyring for brokere er udbygget (6.5). • Logningskrav er udbygget (6.7).

1.2 Forord

Dette dokument indeholder vejledning til version 2.1 af National Standard for Identiteters Sikringsniveauer (NSIS). Hensigten med vejledningen er at give supplerende beskrivelser og konkrete eksempler, der underbygger og illustrerer hensigten med kravene i standarden. Dette er særligt relevant, idet NSIS er opbygget som en resultatbaseret standard[1], der angiver krav til *hvad* der skal opnås i form af sikkerhedsmæssige egenskaber uden at blive præskriptiv omkring, *hvordan* kravene skal imødekommes. Denne tilgang er i overensstemmelse med tilgangen i kommissionens gennemførelsesforordning 2015/1502 [LoA] under [eIDAS]-forordningen om Sikringsniveauer for Elektroniske Identifikationsmidler, og giver en høj grad af frihed og fleksibilitet for de løsninger, som skal opfylde kravene.

Vejledningen er tænkt som et levende dokument, som løbende kan opdateres og udbygges med beskrivelser og eksempler i takt med, at området udvikler sig og praksis etableres, hvor den underliggende NSIS-standard ventes at være mere stabil.

Dokumentet er opbygget efter den samme kapitelstruktur, som findes i NSIS, med henblik på at gøre det enkelt at sammenholde de to dokumenter. Det er dog ikke til alle afsnit eller alle krav fundet nødvendigt med supplerende vejledning, og der er således fokuseret på udvalgte områder, der via høringsprocesser, feedback eller på anden måde har vist behov for uddybning og forklaring.

1.3 Forskelle på eIDAS og NSIS

I forbindelse med tidligere høringer af NSIS har vist sig, at der har hersket en vis usikkerhed om relationen mellem [eIDAS] og NSIS, herunder krav vedr. Sikringsniveauerne. For at tydeliggøre forskellene og dermed også eksistensberettigelsen for NSIS, er formålene med de to tillidsrammeværk sat op mod hinanden i tabellen nedenfor.

Formålet med Sikringsniveauerne i [eIDAS] er overordnet at definere krav til nationale elektroniske identifikationsordninger, der anmeldes af det enkelte medlemsland til kommissionen med henblik på gensidig anerkendelse i grænseoverskridende transaktioner. Verifikation af kravenes opfyldelse sker gennem en peer-review proces organiseret i et samarbejde mellem medlemslandene (eIDAS Cooperation Network). Medlemslandet, der anmelder en elektronisk identifikationsordning, er ansvarligt for fejl og svigt over for de øvrige medlemslande (*relying parties*).

Formålet med Sikringsniveauerne i NSIS er at definere krav til lokale Elektroniske Identifikationsordninger, der anvendes til transaktioner mellem parter i Danmark. Elektroniske Identifikationsordninger behøver ikke være udviklet eller finansieret af det offentlige - endsige være nationale. Anmeldelsen foretages af den organisation, som udbyder ID-tjenesten, og verifikation af kravene sker via en ledelses- samt revisorerklæring. Anmelderen er selv ansvarlig for fejl og svigt over for anvenderne.

[1] På engelsk: “outcome based”.

Område	eIDAS	NSIS
Anmelder	Medlemsland	Udbyder (fx privat part)
Kustode	EU Kommissionen	Digitaliseringsstyrelsens NSIS Tilsyn
Formål	Grænseoverskridende transaktioner[2]	Nationale og lokale transaktioner
Ansvarlig for fejl	Medlemslandet (anmelder)	Anmelderen
Verifikation af krav	Peer-review proces mellem medlemslande (inkl. relevante erklæringer[3])	Selvdeklarering (niveau Lav) og intern revision Ekstern revision samt ledelseserklæring (niveau Betydelig og Høj)
Brugerpopulationer	Store (hele befolkningsgrupper er typisk omfattet af de ordninger, et medlemsland anmelder)	Store og små

Sammenholdt kan man sige, at NSIS og [eIDAS] har forskellige formål, regulerer forskellige brugssituationer, anmeldes af forskellige parter og benytter forskellige verifikationsmekanismer for at sikre kravopfyldelsen. Det er naturligvis muligt, at en national, dansk Elektronisk Identifikationsordning kan blive anmeldt under begge rammeværk, men det forventes, at en række decentrale ordninger i Danmark (fx Lokale IdP'er) alene vil blive anmeldt under NSIS. Det kun Digitaliseringsstyrelsen, som kan anmelde til Kommissionen på vegne af Danmark, og der kan kun anmeldes nationale eID-ordninger.

Endelig kan det nævnes, at NSIS i modsætning til [eIDAS] stiller krav til Identitetsbrokere, da disse udgør en væsentlig byggeblok i dansk identitetsinfrastruktur. Behovet er særligt udtalt, da Danmark er langt fremme med en moderne, fødereret infrastruktur – samt digitalisering i det hele taget.

1.4 Terminologi

Denne vejledning anvender samme terminologi som NSIS-standarden, hvorfor der henvises til denne for forklaring af begreber. Begreber med stort begyndelsesbogstav er defineret i NSIS.

For læsere, der er bekendt med den amerikanske NIST 800-63 standard, er det relevant at bemærke, at begrebet 'Elektronisk Identifikationsmiddel' i NSIS anvendes synonymt med begrebet 'Authenticator' i [NIST] - og altså ikke begrebet 'Credential', som i [NIST] anvendes som betegnelse for *bindingen* mellem en Identitet og en eller flere 'Authenticators'. Begreberne Akkreditiv og Credential anvendes ikke længere i NSIS.

[2] Inden for EU/EØS.

[3] Se retsakten vedr. anmeldelse for detaljer.

Endvidere kan det nævnes, at vejledningen for enkelthedens skyld anvender begreberne 'anmelder af Elektronisk Identifikationsordning' og 'udsteder af Elektroniske Identifikationsmidler' som synonyme. I praksis kan ejeren af et system være en anden part, end den som driver systemet, hvorved disse roller kan være adskilt.

NSIS har ikke et begreb, der direkte modsvarer begrebet 'Credential' i [NIST] (altså selve bindingen), men beskriver i stedet krav til kvaliteten af den Identitet, der udtrykkes som resultatet af autentifikationsprocessen.

Med "Pas" menes et ICAO 9303 kompatibelt rejsepas, der er udstedt af en offentlig myndighed i hjemlandet. Et Pas kan være udstedt med eller uden chip. Et ICAO 9303 kompatibelt nationalt identitetskort med chip og billede udstedt af en offentlig myndighed i hjemlandet, der kan anvendes som rejsedokument i Schengenlande, betragtes som ækvivalent med et pas med chip, hvad angår chip-indholdet.

2 Livscyklus for Elektroniske Identifikationsmidler

Dette kapitel i NSIS om livscyklus indeholder ikke normative krav, og der er derfor ikke for nuværende fundet behov for yderligere vejledning. Beskrivelsen har således alene til formål at illustrere de forskellige stadier i livscyklus for Elektroniske Identifikationsmidler, herunder sammenhænge og ansvarsområder.

3 Normative krav

Dette kapitel indeholder vejledning til kravene relateret til udstedelse og anvendelse af Elektroniske Identifikationsmidler – altså krav til Elektroniske Identifikationsordninger. Kravene til Identitetsbrokere beskrives i kapitel 6. Derudover fremgår generelle krav til begge i kapitel 4.

En organisation med en lokal IdP skal opfylde kravene til *både* a) NSIS Identifikationsordning (da anmelderens organisation typisk udsteder lokale identifikationsmidler til egne brugere) og b) NSIS Identitetsbroker (da en lokal IdP udstiller en autentifikationsservice som videreformidler identiteter til tredjeparter). En lokal IdP er altså omfattet af kravene i NSIS kapitel 3, 4, 5 og 6 (evt. fraregnet kapitel 3.1.3).

En organisation, som anmelder en Elektronisk Identifikationsordning, kan benytte sig af eksterne parter eller underleverandører til at udføre delprocesser fx i forbindelse med verifikation af brugernes Identitet (*Identity Proofing*). I den forbindelse må organisationen som anmelder redegøre for dette underleverandørforhold - herunder hvorledes de samlede krav til Elektroniske Identifikationsordninger på det anmeldte Sikringsniveau er overholdt fx ved at inddrage relevant dokumentation fra de eksterne parter, relevante aftaler mellem parterne etc. Det er således et krav, at dokumentation og revisionserklæringer dækker samtlige krav til Elektroniske Identifikationsordninger, herunder også de krav som løftes af service- eller underleverandører.

Bemærk at tjenesteudbydere (herunder digitale selvbetjeningsløsninger og Apps), der alene modtager identiteter, er ikke underlagt krav i NSIS. De skal alene forholde sig til hvilke sikringsniveauer, de vil modtage, og afvise brugere der er autentificeret på et for lavt niveau.

3.1 Registreringsprocessen

I kravene til registreringsprocessen opereres med begrebet '*autoritativ kilde*'. Eksempler på disse kan være myndighedsudstedte identitetsdokumenter som fx pas, kørekort, militært ID-kort etc., eller et centralt, elektronisk register hos en myndighed som fx CPR- og CVRregistrene. Under alle omstændigheder bør en anmelder klart beskrive i anmeldelsen, hvilke autoritative kilder, man baserer sig på, samt hvilken tillid, der fordres til disse. Her er det fx relevant at belyse, hvor svære benyttede fysiske dokumenter er at forfalske, processerne for validering af dokumenter, samt processerne omkring dataintegritet i anvendte centrale registre.

Digitaliseringsstyrelsen udarbejder ikke en central liste over autoritative kilder, og det er således op til anmelderen at beskrive og risikovurdere de kilder, der lægges til grund for en konkret registreringsproces.

Registreringsprocessen leder frem til et givet sikringsniveau for identiteten (også benævnt IAL). Denne værdi påvirkes ikke direkte af, at et anvendt legitimationsdokument (fx pas) spærres på et senere tidspunkt. Det afgørende er således, at den fremlagte dokumentation var gyldig på tidspunktet for udstedelsen af det Elektroniske Identifikationsmiddel. Bemærk dog, at det i forbindelse med udløb af det Elektroniske Identifikationsmiddel kan komme på tale at genvalidere identiteten.

3.1.1 Ansøgning

Niveau: Betydelig	Krav: 4) Ansøgeren skal afkræves accept af betingelser og tilkendegive at have læst dem.
Vejledning: Ansøgerens accept af betingelser på niveau Betydelig bør realiseres som en aktiv handling af brugeren fx ved krav man i digitale processer afkrydser et felt, der ikke i udgangspunktet er afkrydset. Desuden kan det overvejes, at brugeren ikke kan trykke "Acceptér", før hele teksten som minimum har været vist én gang. En anden tilgang kan være at anvende en digital signatur, men det kræver, at brugeren allerede har fået udstedt et Elektronisk Identifikationsmiddel, som kan anvendes til dette. For ansøgningsprocesser baseret på fysisk fremmøde, kan der være andre overvejelser, eksempelvis udlevering af betingelser på papir, som skal underskrives for at sikre dokumentationssporet. Anmeldere bør endvidere overveje, hvordan man over for en revisor vil dokumentere brugerens accept ved fx at indrette systemet med relevante logninger, hvorledes accepten sammenknyttes med en given bruger mv. Hvis accepten indebærer samtykke til behandling af personoplysninger, bør Datatilsynets og Justitsministeriets vejledning om dette iagttages.	

3.1.2 Verifikation af Identitet (fysiske personer)

For en Lokal IdP vil verifikation af den fysiske persons identitet ofte ske som en del af oprettelsen af en erhvervsbruger dvs. opfyldelsen af 3.1.2 og 5.2 vil ofte realiseres med en samlet proces for brugeroprettelse. Krav gående på brugeroprettelsesprocessen for erhvervsbrugere findes i kapitel 5.2.

Niveau: Lav	1) Der skal gennemføres en verifikation, og der skal foreligge en beskrivelse af verifikationsprocessen, herunder de forudsætninger, der lægges til grund.
Vejledning: Det forventes, at personidentifikationsdata samt øvrige attributter for identiteten verificeres efter en beskrevet procedure. Verifikationen kan foretages på baggrund af forelagt legitimation (fx navn, fødselsdato og CPR-nummer), på baggrund af autentifikation med andre elektroniske identifikationsmidler, ved opslag i autoritative kilder, samt ved fremsendelse af valideringslink/kode, der skal responderes på. Fremsendelse af valideringslink kan fx anvendes til at verificere, at ansøgeren har kontrol over en opgivet e-mail adresse.	

Niveau: Lav	2) Ansøgeren (Entiteten) skal med overvejende sandsynlighed vurderes at være i besiddelse af almindeligt anerkendt dokumentation for sin Identitet.
Vejledning:	

Dette kan fx være sundhedskort, pas, kørekort, dåbsattest eller forskudsopgørelse. Verifikation af identiteten kan i særlige tilfælde baseres på tidligere autoritativ digital registrering af identiteten hos en myndighed. Forbindelsen mellem ansøgeren og registreringen skal kunne verificeres med overvejende sandsynlighed i forbindelse med fysisk fremmøde. Et eksempel på dette kunne være, at ansøgeren er registreret med billede eller i sammenhæng med andre oplysninger hos myndigheden, som kan verificeres troværdigt fx via kontrolspørgsmål om sager, ydelser eller andet, der er registreret om den påståede identitet hos den offentlige myndighed, og hvor svarene ikke må antages at være kendt af uvedkommende. Den offentlige myndighed kunne eksempelvis være Kriminalforsorgen, en kommune eller lign.

Niveau: Betydelig	4) Det skal verificeres, at ansøgeren er i besiddelse af nationalt anerkendt foto- eller biometrisk dokumentation for sin Identitet (fx pas eller kørekort). Hvor ansøgeren ikke er i besiddelse af dette, kan anvendes tilsvarende identifikationsprocesser, som benyttes ved udstedelse af dansk pas eller kørekort.

Vejledning:

Udgangspunktet i krav 4 er, at identitetssikringen tager afsæt i pas eller kørekort.

Her bør kontrollen som minimum omfatte:

1. Legitimationen ikke er udløbet.
2. Legitimationen indeholder fornavn, efternavn og evt. CPR-nummer, og bør kontrolleres mod en autoritativ kilde. Dette kan ske via opslag i CPR-registret eller hvis man i samme ombæring ønsker at oprette en medarbejderidentitet (se kapitel 5), kan det verificeres, at oplysningerne modsvarer en kendt fysisk person registreret i organisationens autoritative personale- eller HR-register.
3. Personen kan svare på kontrolspørgsmål – for fysiske personer evt. med afsæt i CPR-registrets oplysninger og for erhvervsbrugere (se kapitel 5) evt. med afsæt i HR-registreringen om f.eks. titel, nærmeste leder, ansættelsessted, ansættelsestidspunkt mv.
4. Billedet på legitimationen ligner med betydelig sikkerhed brugeren.
5. Legitimationen fremstår ikke beskadiget eller som forsøgt ændret eller forfalsket.

Når der ikke kan anvendes pas eller kørekort, kommer anden del af kravet i spil: "Hvor ansøgeren ikke er i[4] besiddelse af dette, kan anvendes de samme identifikationsprocesser, som benyttes ved udstedelse af dansk pas eller kørekort". Disse identifikationsprocesser skal samlet set sikre, at identitetssikringen bringes op på niveau betydelig, men de præcise processer for pas og kørekort kan dog ikke umiddelbart direkte overføres. Eksempelvis kræver pasudstedelse afgivelse af fingeraftryk, og at ansøger medbringer eller får taget et billede. Man kan derfor

som udgangspunkt benytte de samme legitimationsdokumenter som ved pasudstedelse, men identifikationsprocesserne bør tilpasses således, at identiteten verificeres på sikringsniveau betydelig, jf. nedenfor.

Her er det endvidere vigtigt at være opmærksom på, at alternative legitimationsdokumenter til pas og kørekort kan være lettere at forfalske, og at der derfor bør tages højde for dette – eksempelvis ved krav om fremvisning af flere originaldokumenter, brug af kontrolspørgsmål, vidner mv. (se vejledning til punkt 5 og 6 nedenfor). Pasbekendtgørelsen § 6 stk 2. oplister eksempelvis "original dåbs-, navne- eller fødselsattest, sundhedskort eller anden egnet legitimation samt "billedlegitimation" som legitimationskrav for udstedelse af pas, hvis man ikke allerede har et gyldigt pas.

Andre autoritative kilder

I visse tilfælde er ansøgere ikke i besiddelse af legitimationsdokumenter, og alternative procedurer må derfor anvendes til identitetssikring. Som på sikringsniveau Lav kan verifikation af en identitet på niveau Betydelig baseres på tidligere registreringer om identiteten hos en myndighed eller anden autoritativ kilde, når der kan etableres en forbindelse mellem ansøgeren og registreringen. På niveau Betydelig skal forbindelsen mellem ansøger og registrering efterprøves til et niveau, hvor risikoen for impersonering er meget lav. Dette kan eksempelvis opnås ved at kombinere flere uafhængige elementer som kontrolspørgsmål, sammenligning af ansøger med billede eller underskrift fra tidligere registrering, anvendelse af vidner som attesterer ansøgers identitet eller besiddelse af øvrige dokumenter, hvor identiteten fremgår. Den anvendte registrerings identitetssikringsprocedure skal derudover være nationalt anerkendt gennem udmøntning i lov, bekendtgørelse, cirkulære eller tilsvarende vejledning. Et eksempel på dette er Kriminalforsorgens cirkulæreskrivelse nr. 9272 af 30. april 2015, der anvendes til udstedelse af identifikationsmidler til domfældte.

Niveau: Betydelig	5) Dokumentation kontrolleres for at fastslå, at den er ægte, eller det vides i henhold til en autoritativ kilde, at dokumentationen eksisterer og er relateret til en fysisk person.

Vejledning:

Krav 5) handler primært om at sikre, at den forelagte dokumentation er ægte og ikke forfalsket. Krav 5 bør dog ses i sammenhæng med krav 6, da de mulige kontrolforanstaltninger i nogen grad overlapper.

Ved brug af pas:

Hvis der anvendes et pas som legitimationsdokument, går kravet på validering af passet som gyldig, autoritativ kilde. Hvis passet er ICAO 9303 kompatibelt og har RFID-chip, anbefales det at passets chip læses og signaturen valideres, for at opfylde krav 5. Derudover bør der foretages validering af ansøgeren mod billedet gemt på passets chip.

Hvor elektronisk validering af et pas ikke er mulig, bør der foretages manuel validering af passet i henhold til passets fysiske karakteristika, som beskrevet i PRADO, samt validering af ansøgeren mod passets billedside. Derudover bør der tilføjes supplerende kontrolelementer, med henblik på at opnå tilstrækkelig høj sandsynlighed for, at identitetssikringen er på det ønskede niveau. Bemærk, at denne sammenligning er en manuel kontrol som jævnfør krav 7) kræver specielt uddannet personale, der har modtaget instruktion i at verificere ægtheden af dokumenter og detektere svindel.

Ved brug af digitalt kørekort:

Ved præsentation af dansk digitalt kørekort bør dette verificeres digitalt ved scanning af QR-kode med kontrollantens egen kørekort app. Slutbrugeren skal åbne sin app, vælge 'Kontrol' og vælge ID, så QR-koden vises. Kontrollanten scanner herefter QR-koden med egen kørekort app. Her skal der fremgå et grønt checkmark og ordet 'Gyldig' i bunden af skærmen. Det overførte navn og CPR-nummer skal modsvare brugerens oplysninger.

Uden brug af pas / kørekort:

Som nævnt under krav 4) er det vigtigt at være opmærksom på, at alternative legitimationsdokumenter end pas og kørekort kan være lettere at forfalske, og at der derfor bør tages højde for dette gennem yderligere tiltag. Disse yderligere tiltag kan fx være krav om fremvisning af flere legitimationsdokumenter end i pas/kørekort identifikationsprocesserne. Det anbefales, at der forevises mindst 2 originale legitimationsdokumenter fx person-, dåbs- fødsels- eller navneattest samt enten sundhedskort eller bopælsattest.

Derudover anbefales, at identifikationsprocessen også indeholder supplerende kontrolelementer som fx kontrolspørgsmål, i det omfang dette er muligt. Alternativt kan anvendes andre supplerende kontrolelementer som fx et vidne. Bemærk, at vidner i sig selv normalt ikke bør betragtes som en autoritativ kilde, men som en supplerende kontrolforanstaltning.

Muligheden for at anvende kontrolspørgsmål afhænger naturligvis af, om der er adgang til pålidelige datakilder om ansøgerne (fx CPR-registret), og værdien af spørgsmålene vil desuden afhænge af, om ansøgningen sker ved fysisk fremmøde eller on-line. For en on-line ansøgning kan en ondsindet person potentielt have mulighed for at fremsøge svar på kontrolspørgsmål via internettet, hvorfor værdien forringes, mens man ved fysisk fremmøde vil få vanskeligere ved at svare korrekt.

Inden for den finansielle sektor findes en række krav til kundekendskabsprocedurer under hvidvaskloven. Finanstilsynet har udgivet en informativ vejledning til hvidvaskloven[5] med en række eksempler på indhentning og kontrol af identitetsoplysninger, som kan være relevante at overveje.

[5] https://www.finanstilsynet.dk/~/media/Tilsyn/hvidvask/Vejledning-til-hvidvaskloven-oktober-2018.pdf?la=da

Anmeldere bør endvidere overveje, hvordan man over for en revisor vil dokumentere, at de planlagte kontroller faktisk er udført (mao. dannelse af revisionsspor).

Niveau: Betydelig	Krav: 6) Der er taget skridt til at nedbringe risikoen for, at den pågældende persons Identitet ikke er den, den påstås at være, under hensyntagen til risikoen for at den fremlagte dokumentation kan være blevet tabt, stjålet, suspenderet, tilbagekaldt eller være udløbet. Ansøgerens identitet valideres i henhold til en autoritativ kilde, og i det omfang det er muligt, tages der skridt til at sikre, at ansøgeren ikke er markeret som død eller forsvundet.
Vejledning: Dette krav handler om at sikre, at et legitimationsdokument, som er fundet gyldigt jævnfør krav 5), ikke er meldt tabt/stjålet. Ved brug af danske pas: Som eksempel på foranstaltninger kan her nævnes, at danske pas/kørekort anvendt som dokumentation bør kontrolleres for spærring i centrale registre, således at risikoen for anvendelse af stjålne/tabte dokumenter mindskes. Danske pas bør således verificeres mod Rigspolitiets pasregister, medmindre der foretages andre tilsvarende mitigerende foranstaltninger. Udenlandske pas: For udenlandske pas kan det være vanskeligt at få adgang til at autoritativ information om passtatus fra centrale registre. Her vil en grundig validering af den fysiske person mod passets elektroniske billede kunne træde ind som mitigering mod, at et stjålet eller bortkommet pas anvendes uretmæssigt.	

Niveau: Høj	Krav: 9) Ansøgeren kan identificeres som havende den påståede Identitet ved sammenligning af et eller flere af personens fysiske kendetegn med en Autoritativ kilde. Sammenligningen skal udføres enten via personligt fremmøde eller en anden mekanisme, der giver en ækvivalent sikkerhed.

Vejledning:
Kravene på niveau Høj forudsætter sammenligning af fysiske kendetegn fra personen med en *autoritativ kilde*, der som tidligere nævnt kan være et myndighedsudstedt identitetsdokument eller et centralt, elektronisk register. I mange sammenhænge vil kontrol af fysiske kendetegn på et Sikringsniveau Høj forudsætte personligt fremmøde, men NSIS er åbent for alternative løsningsmuligheder, der kan give et ækvivalent Sikringsniveau fx gennem brug af biometri. Ved anvendelse af biometri er det afgørende at sikre sig, at der faktisk er tale om friske data fra ansøgeren selv og ikke "stjålne" biometriske data - eller data formidlet gennem et man-in-the-middle angreb. Der bør således altid være etableret en autentificeret og beskyttet kanal mellem den sensor, som optager de biometriske data, og det sted / den proces, hvor de biometriske data verificeres.

Niveau: Høj	Krav: 10) Der er med meget høj sandsynlighed et fysisk match mellem ansøgeren og den præsenterede dokumentation (fx match af billede og underskrift).
Vejledning: Hvis passet er den eneste autoritative kilde, der er adgang til, bør verifikation ske ved, at passets digitale billede, udlæses fra passets chip og benyttes som kilde til opfyldelse af dette krav for at opnå en meget høj sandsynlighed for verifikation af et fysisk match mellem ansøgeren og billedet i den autoritative kilde. Dette anbefales, fordi det digitale billede er af høj kvalitet og derfor egner sig bedst til sammenligning med den fysiske person, og fordi det digitale billede er digitalt sikret og derfor med meget høj sandsynlighed vil være det korrekte billede. Det anbefales at anvende programmatisk ansigtsgenkendelsesteknologi ifm. det fysiske match mellem ansøgeren og det digitale billede, for at fastslå overensstemmelse mellem ansøgeren og det udlæste digitale billede med en meget høj sandsynlighed. Den programmatiske ansigtsgenkendelsesteknologi bør som minimum operere med en FMR (False Match Rate) i henhold til NIST 800-63B, ”Use of biometrics”. Hvis det er nødvendigt at benytte manuelle procedurer for at fastslå overensstemmelse mellem ansøgeren og det udlæste digitale billede, bør dette gennemføres af specielt uddannet personale efter faste tjekprocedurer udformet og registreret i systemet for at sikre en meget høj sandsynlighed for korrekt match. I forbindelse med manual validering anbefales det at tage udgangspunkt i beskrivelsen i eIDAS gennemførelsesforordningens (2015/1502) krav i sektion 2.1.2 på sikringsniveau høj, krav 1 alternativ a og tilhørende vejledning i ”Guidance for the application of the levels of assurance which support the eIDAS Regulation” og vejledningssektion 2.4.5 om krav til uddannelse af personale, når der benyttes manuelle procedurer til at fastslå overensstemmelse mellem ansøgeren og billedet.	

Endelig kan det nævnes, at NSIS gør det muligt at udstede nye Elektroniske Identifikationsmidler på baggrund af en autentifikation med et andet, gyldigt Elektronisk Identifikationsmiddel, der er udstedt under en anmeldt Elektronisk Identifikationsordning, og som opfylder kravene på mindst samme Sikringsniveau. Et eksempel på dette kunne være, at man ved udstedelse af et Elektronisk Identifikationsmiddel til erhvervsbrug lader brugeren autentificere sig med et Elektronisk Identifikationsmiddel udstedt til brugeren i egenskab af privatperson. Herved behøver man ikke på ny foretage Identitetssikring af den fysiske person men kan koncentrere sig om at verificere tilknytningen til den juridiske enhed samt evt. udstedelse af et nyt Elektronisk Identifikationsmiddel. Dette betyder, at der kan etableres mere smidige løsninger, og brugerne undgår potentielt at skulle stille op til flere, identiske registreringsprocesser.

3.1.3 Verifikation af Identitet (juridiske enheder)

Verifikation af juridiske enheder er relevant, hvis man udsteder identifikationsmidler til andre organisationer eller medarbejdere i fremmede organisationer[6] eksempelvis i rollen som FullService Lokal IdP. Her er det således relevant at sikre sig, at man udsteder til den rigtige organisation. Et eksempel på dette er MitID Erhverv løsningen, som tilbyder at udstede identifikationsmidler til alle organisationer med et CVR-nummer. Udsteder man kun identifikationsmidler inden for egen organisation, er kravene i dette afsnit ikke relevante.

Niveau: Lav	Krav: 4) Det kan antages, at registreringen gennemføres af en person, der er autoriseret til dette af den juridiske enhed.
Vejledning: På niveau Lav er det tilstrækkeligt, at den fysiske person selv erklærer (fx på tro-og-love og evt. under et anmelderansvar), at vedkommende er autoriseret til at agere på vegne af den juridiske enhed. I den forbindelse skal personen være autentificeret, så vedkommende kan gøres ansvarlig for misbrug, hvilket ligeledes må forventes at have en præventiv effekt.	

Niveau: Lav	Krav: 5) Personen, der gennemfører registreringen, er autentificeret på Sikringsniveau Lav eller højere.
Vejledning: Den (fysiske) person, der gennemfører registreringen på vegne af den juridiske enhed, skal ved on-line registrering autentificeres via et Elektronisk Identifikationsmiddel på mindst samme Sikringsniveau som den juridiske enhed registreres	

[6] Dvs. ikke vikarer eller konsulenter som gives identitet i egen organisation.

på. En person autentificeret på Sikringsniveau Lav må eksempelvis ikke gennemføre registreringer af juridiske enheder på niveau Betydelig eller Høj. Tilsvarende logik gælder de højere Sikringsniveauer.

Niveau: Betydelig	Krav:
	6) Der er taget rimelige skridt til at sikre, at registreringen gennemføres af en person, der er autoriseret til dette af den juridiske enhed. Ægtheden af autorisationen skal verificeres.
Vejledning: Hensigten med kravet er at sikre, at registranten faktisk repræsenterer den juridiske enhed, som tilsluttes, og er autoriseret til at agere på dennes vegne. Autorisationen kan foreligge på forskellige måder som fx: a) Personen kan være udpeget til at kunne repræsentere den juridiske enhed generelt eller har en position i den øverste ledelse fx som medlem af direktionen. For visse virksomhedsformer kan persontilknytninger og tegningsregler slås op i CVR-registret, der kan fungere som autoritativ kilde, hvilket kan danne grundlag for en automatiseret verifikation af autorisationen. For virksomhedsformer uden persontilknytning registreret i CVR (fx fonde og visse foreninger) kan der gennemføres en manuel kontrol af personens tilknytning til virksomheden/organisationen på baggrund af forelagt dokumentation fx i form af stiftelsesdokumenter, referat fra generalforsamlinger eller -bestyrelsesmøder, ansættelseskontrakter etc. Dette kunne eksempelvis være en verifikation af, at en person er formand for en grundejerforening. b) Personen er eksplicit bemyndiget af den juridiske enhed til at gennemføre registreringen på dennes vegne fx gennem en papirbaseret- eller digital fuldmagt. Her verificeres som minimum, at underskriveren af fuldmagten kan udstede fuldmagten (svarende til tilfælde a), at fuldmagten vitterligt anvendes af den person, der er udpeget i fuldmagten samt inden for det område, der angivet i fuldmagten. Inspiration til relevant dokumentation kan ses på https://www.mitid-erhverv.dk/tilslutning/krav/	

Niveau: Høj	Krav:
	8) Der er gennemført en stærk validering af, at registreringen gennemføres af en person, der er autoriseret til dette af den juridiske enhed.
Vejledning: Begge eksempler nævnt under niveau Betydelig kan anvendes på niveau Høj med flg. skærpelser:	

a) Den fysiske person er autentificeret på niveau Høj med CPR-nummer, og CPR-nummeret fremgår af CVR-registret med en rolle, der kan repræsentere den juridiske enhed generelt eller som medlem af den øverste ledelse, således at der er eftervist en stærk kobling mellem den autentificerede person og persontilknytningen for den enhed person registreret i CVR.
b) Fremlagte fuldmagter udstedt af den juridiske enhed er kontrolleret som værende ægte og gyldige, herunder at de er underskrevet eller digitalt signeret af en person, der kan repræsentere den juridiske enhed (tilfælde a).
    - Papirbaserede fuldmagter rummer påtegning af vitterlighedsvidner grundet den øgede mulighed for forfalskning (ikke nødvendigt for digitale fuldmagter, som er underskrevet med digital signatur med et sikkerhedsniveau svarende til OCES eller kvalificerede signaturer).
    - Der er indført skærpede kontroller til at forhindre falske fuldmagter fx i det papirbaserede tilfælde ved gennemførsel af stikprøvekontrol med kontrolopringning til virksomheden, verifikation af håndskrevne underskrifter mod kendte underskriftseksemplarer etc.

3.2 Udstedelse og håndtering af Elektroniske Identifikationsmidler

3.2.1 Styrke af Elektroniske Identifikationsmidler

Niveau: Lav	Krav: 2) Det Elektronisk Identifikationsmiddel er udformet således, at udstederen tager rimelige skridt til at kontrollere, at det kun er den Person, som det tilhører, der har kontrol over og er i besiddelse af det.
Vejledning: Kravene til udformningen af det Elektronisk Identifikationsmiddel går primært på at beskytte indehaveren af et Elektronisk Identifikationsmiddel mod, at uvedkommende får adgang til at benytte dette og dermed udgive sig for indehaveren. Brugerens muligheder for at bevare kontrollen med sit Elektroniske Identifikationsmiddel afhænger af en række faktorer, herunder om det Elektronisk Identifikationsmiddel er modstandsdygtigt ved anvendelse i fjendtlige miljøer (fx log-in fra en PC med en keylogger installeret, som opsnapper kodeord). Ved vurdering af indehaverens mulighed for enekontrol må det forudsættes, at et Elektronisk Identifikationsmiddel er blevet udleveret til rette vedkommende - så kravene går med andre ord på *anvendelse* af et Elektronisk Identifikationsmiddel efter udleveringen. Der er i NSIS separate krav til udleveringsprocessen, som adresseres nedenfor. Der er i NSIS ikke nogen krav til, at et Elektronisk Identifikationsmiddel skal beskyttes teknisk mod frivillig overdragelse fra en legitim bruger til en tredjepart. Dette bør naturligvis være i klar modstrid med brugsvilkårene, men det kan være	

teknisk vanskeligt at gardere sig imod med mindre der benyttes biometriske faktorer, hvilket ikke er et krav på nogen af Sikringsniveauerne, og selv da er der ingen garantier, hvis personen aktivt medvirker. Til gengæld vil det evt. være muligt at opsamle loginformation, der kunne indikere, at et Elektronisk Identifikationsmiddel blev benyttet af mere end én person (fx samtidig brug fra forskellige lokationer etc.). Krav til *fraud detection* er dog ikke en del af NSIS. Endelig bør udformningen være således, at brugerne ikke kunne frakoble vigtige sikkerhedsmekanismer som fx slå passwordvalidering fra, eksportere nøgler til en svagere beskyttelse etc.

Niveau: Betydelig	Krav: 3) Det Elektroniske Identifikationsmiddel skal gøre brug af mindst to Autentifikationsfaktorer fra forskellige kategorier.
Vejledning: Niveau Betydelig forudsætter anvendelse af et Elektronisk Identifikationsmiddel med mindst to faktorer fra forskellige kategorier (multi-faktor autentifikation.) Det er her tilladt at opfylde kravet ved at kombinere Elektroniske Identifikationsmidler (til et samlet Elektronisk Identifikationsmiddel) eller benytte ét Elektronisk Identifikationsmiddel, der i sig selv tilvejebringer flere faktorer fra forskellige kategorier. Kravet om forskellige kategorier af Autentifikationsfaktorer henviser til kategorierne: a) »indehaverbaseret Autentifikationsfaktor«: en Autentifikationsfaktor i form af en unik fysisk enhed, som Entiteten skal bevise at være i besiddelse af b) »vidensbaseret Autentifikationsfaktor«: en Autentifikationsfaktor, som Entiteten skal bevise at have kendskab til (fx et kodeord), og som er hemmelig c) »iboende Autentifikationsfaktor«: en Autentifikationsfaktor, der er baseret på et unikt fysisk træk hos en fysisk person, og som Entiteten skal bevise at have (fx biometri) Dette betyder med andre ord, at to forskellige passwords ikke vil leve op til kravene, da de regnes for tilhørende samme kategori. Derimod vil et kodeord (kategori b) kombineret med et OTP nøglekort (kategori c) kunne regnes som to faktorer fra forskellige kategorier. En hardwareenhed beskyttet med password vil i de fleste tilfælde kunne regnes som to faktorer, idet enheden regnes som en indehaverbaseret faktor og kodeordet som en vidensbaseret faktor. Hvis den ene faktor leveres fra et *´multi purpose device'* som fx en smart phone, vil oplåsning af enheden normalt ikke kunne regnes som en faktor i sig selv, idet denne handling ikke nødvendigvis er relateret til selve autentifikationen. Oplåsning skal med andre ord være en specifik handling, der er knyttet til selve autentifikationen (fx startet fra den pågældende App). Dette kendes eksempelvis fra MitID App'en, som kræver brugerautentifikation i App'en uanset om enheden generelt er låst op eller ej.	

For en nøglefil vil det i udgangspunktet gælde, at den ikke kan regnes som en ihændehaverbaseret faktor, med mindre det kan sikres, at kun brugeren har adgang til filen. Dvs. filer på fællesdrev, roaming løsninger etc. hvor adgang til nøglefilen reduceres til et password[7], regnes ikke som en ihændehaverbaseret faktor.

NSIS definerer ikke eksplicitte krav til kvaliteten af den enkelte faktor i Elektroniske Identifikationsmidler som fx længden eller entropien af kodeord eller engangskoder, perioder for udskiftning etc. Her må udstederen af et Elektronisk Identifikationsmiddel foretage en konkret risikovurdering, der tager afsæt i den specifikke implementering inkl. mitigerende kontroller (fx muligheden for at spærre det Elektroniske Identifikationsmiddel ved forsøg på omgåelse af en Autentifikationsfaktor). Risikovurderingen bør dokumenteres og vedlægges anmeldelsen. Som eksempler kan nævnes:

- Løsninger med central verifikation af kodeord og mulighed for central spærring kan give en forholdsvis stærk beskyttelse mod gæt af kodeord eller udtømmende gennemsøgning, hvorfor længden alt andet lige ikke behøver at være den samme som ved decentral verifikation (fx lokalt på brugerens enhed). Til gengæld må man så overveje risikoen *for denial of service* angreb, hvor en legitim brugers kodeord/konto spærres ved gentagne forkerte forsøg på autentifikation.

Se endvidere vejledningen til de øvrige niveauer nedenfor.

Niveau: Betydelig	Krav: 4) Det Elektroniske Identifikationsmiddel er udformet således, at det kan antages, at det kun kan bruges, når det er den person, som det tilhører, der har kontrol over og er i besiddelse af det.
Vejledning: Dette krav indebærer, at et tabt eller stjålet Elektronisk Identifikationsmiddel ikke umiddelbart kan anvendes af uvedkommende dvs. at en af Autentifikationsfaktorerne skal være en vidensbaseret eller iboende Autentifikationsfaktor der sikrer, at de ikke kan anvendes af andre personer.	

Niveau: Høj	Krav: 5) Det Elektronisk Identifikationsmiddel skal være beskyttet mod kopiering og manipulering af angribere med stor Angrebskapacitet.

[7] Også selvom adgangen til nøglefilen udløses af et andet password end det, der kan dekryptere nøglefilen.

	6) Det Elektronisk Identifikationsmiddel er udformet således, at den Person, som det tilhører, kan beskytte det sikkert mod, at andre bruger det.

Vejledning:

Terminologien vedrørende angrebskapacitet under punkt 5) er hentet fra ISO 15408 "Information technology – Security techniques – Evaluation criteria for IT security" samt ISO/IEC 18045 "Information technology – Security techniques – Methodology for IT security evaluation". Standarderne er frit tilgængelige på www.commoncriteriaportal.org. Terminologisk skal 'stor Angrebskapacitet' forstås synonymt med 'høj Angrebskapacitet'.

Ved Angrebskapacitet (*attack potential*) forstås her et mål for indsatsen, der skal bruges for at angribe løsningen, udtrykt i termer af angriberens ekspertise, tid, ressourcer og motivation. Annex B.4 i ISO/IEC 18045 / CEM indeholder vejledning til, hvordan man beregner angrebskapacitet nødvendig for at identificere og udnytte en sårbarhed i en autentifikationsmekanisme. Metoden tager udgangspunkt i evaluering af en række aspekter herunder:

a) Tiden som må påregnes anvendt til at identificere en sårbarhed og gennemføre et angreb.
b) Graden af specialistekspertise fx om sikkerhed og kryptografi, som kræves at gennemføre et angreb.
c) Krav til viden om løsningen, som forudsættes, herunder den interne opbygning og sikkerhedsmekanismer.
d) Behov for '*window of opportunity*' for at kunne gennemføre et angreb (fx adgang til Elektroniske Identifikationsmidler eller central infrastruktur i løsningen).
e) Behov for særlig software / hardware som forudsætning for at kunne gennemføre angreb - fx kunne et scenarie kræve konstruktion af specialhardware til at gennemføre angrebet med.

Ovennævnte parametre tildeles en numerisk værdi og summen af disse giver angrebskapaciteten (fx giver en score i intervallet 20-24 udslag i '*High attack potential*').

Som et eksempel kan nævnes, at et papirbaseret nøglekort med engangskoder kan kopieres/fotograferes/aflures, uden at dette kan ses bagefter (fx hvis indehaveren efterlader kortet i sin jakke/taske eller er uopmærksom ved brug), og derfor kræver et angreb kun et mindre '*window of opportunity*' men ingen særlig teknisk viden eller hardware/software.

Endvidere kan det som pejlemærke nævnes, at SMS- eller mail-baserede engangskoder og RFID-baserede 'dørkort', der let og hurtigt kan kopieres med simpel hardware, der kan købes til få hundrede kroner, normalt ikke kan betragtes som tilstrækkelige på sikringsniveau Betydelig. Derimod vil FIDO U2F tokens (herunder 'softtokens' og passkeys), nøglevisere og nøgleapps (baseret på RFC 6238) med en korrekt implementering ofte opfylde kravene på sikringsniveau Betydelig, da de kan yde en væsentlig bedre beskyttelse mod en række angreb.

På niveau Høj kræves meget stor resistens - selv mod angribere med høj angrebskapacitet. En fysisk chip med en kryptografisk nøgle kan designes, så den i prak-

sis er særdeles vanskelig at kompromittere, hvorfor et angreb kan kræve specialistviden, speciel hardware og lang tid. Sådanne hardware-enheder vil typisk have opnået certificeringer som fx Common Criteria, [FIPS 140-2], DS/EN 419211 mv.), der giver detaljerede krav og vejledning til design med høj grad af enekontrol (*sole control)*. Brug af certificerede enheder under anerkendte standarder vil generelt være en kost-effektiv måde at dokumentere opfyldelse af niveau Høj uden behov for omfattende, yderligere dokumentation. Alternativer med et ækvivalent Sikringsniveau er naturligvis også muligt uden certificering efter disse standarder, men det kræver så mere dokumentation og analyse i forbindelse med anmeldelsen.

Et særligt område, hvor det endnu ikke er almindeligt med certificering af kryptografiske processorer, er på mobile enheder som smart phones etc. Her kan man på niveau Høj skele til nedenstående krav som alternativ til certificeringer:

1. Kryptografiske nøgler må kun kunne anvendes, når enheden er låst op af brugeren, og kun fra den applikation, som har genereret nøglen.
2. Andre brugere (selv avancerede) med fysisk adgang til enheden skal ikke kunne tilgå eller bruge de kryptografiske nøgler eller kunne overføre nøglemateriale til andre enheder gennem fx device backup. Der skal bl.a. beskyttes mod brute force angreb.
3. Ondsindet kode installeret på enheden skal ikke kunne tilgå kryptografisk nøglemateriale eller anvende nøgler fra en anden applikation.
4. Nøgler skal være krypteret under lagring og fremgår aldrig i klar tekst i den del af enhedens hukommelse, som anvendes til applikationer.
5. Nøgler skal være placeret i en sikker container, der er isoleret fra resten af enheden (både operativsystem/kerne og applikationskode).
6. Nøgler skal være genereret i containeren og kan ikke importeres eller eksporteres fra sin container.

I ovenstående krav skal "nøgle" forstås bredt både som kryptografiske nøgler, secrets mv.

3.2.2 Levering og aktivering

Udlevering og aktivering af Elektroniske Identifikationsmidler til/for rette vedkommende er en kritisk del af en Elektronisk Identifikationsordnings sikkerhed. Udleveringen kan afhængig af det Elektroniske Identifikationsmiddels form ske på forskellige måder – herunder fx personlig udlevering, postforsendelse eller elektronisk overførsel (fx download af App). Ofte kombineres udleveringen med en efterfølgende aktiveringsproces, således at et Elektronisk Identifikationsmiddel ikke kan benyttes, før det er aktiveret. Dette nedbringer risikoen for, at uvedkommende kan benytte et opsnappet Elektronisk Identifikationsmiddel (fx fra en postforsendelse). Hvis et Elektronisk Identifikationsmiddel sendes i helt upersonaliseret form (fx et FIDO token), er der ingen krav til forsendelsen, da sikkerheden i dette tilfælde alene beror på aktiveringsprocessen, der knytter midlet til en identitet.

Niveau: Betydelig	Krav:

	2) Det Elektronisk Identifikationsmiddel leveres efter udstedelse via en mekanisme, som gør det muligt at antage, at det kun udleveres til den Person, som det tilhører.

Vejledning:

Ved design af udleverings- og aktiveringsprocesser bør en række risikominimerende tiltag overvejes, der kan indgå i den samlede risikovurdering:

- Det Elektroniske Identifikationsmiddel bringes under brugerens fulde kontrol via en sikker mekanisme baseret på den forudgående verifikation af identitet (jf. 3.1.2 eller 3.1.3) (evt. i forlængelse af denne) eller andre tilsvarende kontroller.
- Udleveringskanalen bør beskyttes bedst muligt – fx bør udlevering online ske over krypterede og autentificerede forbindelser.
- Ved print af koder og kodekort kan dedikerede, sikre printfaciliteter benyttes og forsendelser beskyttes med specielt udformet papir/kuverter, der gør det vanskeligt at se indholdet samt efterlader spor, hvis forsendelsen har været åbent af uvedkommende.
- Elektroniske Identifikationsmidler overleveres eller sendes i ikke-aktiveret tilstand, og aktiveringskode og Elektronisk Identifikationsmiddel kan fremsendes ad forskellige kanaler (fx den ene med post og den anden elektronisk). Ved fremsendelse af upersonaliserede (fysiske) identifikationsmidler går kravet på den aktiveringskode eller mekanisme, der kan binde identifikationsmidler til en identitet.
- En kontrol kan være, at brugeren skal legitimere sig / kvittere for modtagelse (tjener bl.a. audit formål).
- Postforsendelser kan sendes til en autoritativ adresse (fx folkeregister / CVR-adresse) og ikke en brugerangivet adresse, men risikoen for opsnappede leverancer bør håndteres.
- Der bør etableres en procedure for at spærre et Elektronisk Identifikationsmiddel automatisk, hvis det ikke aktiveres inden for et bestemt tidsrum fra afsendelsen/udleveringen.
- Bindingen mellem en enhed og en bruger skal etableres på en sikker måde, som modvirker at administratorer eller andre tredjeparter kan koble en enhed til en andens identitet og herefter anvende enheden til at impersonere denne bruger. Et eksempel på en tilstrækkelig binding vil fx være at aktivere en enhed udleveret til en medarbejder med dennes personlige MitID på mindst samme Sikringsniveau. Eksempler på en utilstrækkelig binding vil være at basere en mobil SMS-faktor på automatisk opslag i en elektronisk telefonbog eller at en it-administrator på egen hånd kan tildele en enhed til en bruger i et administrativt system, hvorefter denne uden yderligere skridt bliver aktiv for den pågældende Identitet.
- Det er endvidere relevant at sikre, at registrerede brugeridentiteter, der er resultatet af identitetssikringsprocessen, kun kan opdateres gennem autoriserede processer, der er underlagt NSIS revisionskrav. Dette gælder både identitetens stamdata (fx navn og CPR), bindingen til Elektroniske Identifikationsmidler samt registreringsstyrken (fx IAL).

Niveau: Høj	Krav: 3) Aktiveringsprocessen kontrollerer, at det Elektroniske Identifikationsmiddel kun blev udleveret til den Person, som det tilhører. 4) Udleveringen skal beskyttes mod angreb, hvor det Elektroniske Identifikationsmiddel stjæles under transport samt insider-angreb i udleveringsfunktionen hos udstederen ved fx at benytte to uafhængige forsendelseskanaler eller funktionsadskillelse.

Vejledning:

Punkt 4) er målrettet processer med fysisk udlevering af Identifikationsmidler, aktiveringskoder mv. hvor man på niveau Høj skal have implementeret kontroller mod insiderangreb, så en enkeltstående, ondsindet administrator hos udstederen ikke på egen hånd kan få udstedt eller tiltage sig et fungerende Elektronisk Identifikationsmiddel tilhørende en anden – fx implementeret gennem funktionsadskillelse, 'fire-øjne' princip mv.

Udleveringsprocessen kan også foregå elektronisk – eksempelvis ved at en aktiveringskode, der kan koble et ikke-personaliseret Identifikationsmiddel til en identitet, leveres af en sikker, elektronisk kanal. Her er det jævnfør punkt 3) vigtigt at sikre, at den elektroniske kanal giver høj sikkerhed for, at der sker udlevering til den rigtige person, og at aktiveringskoden ikke kan opsnappes af uvedkommende. Dette kan eksempelvis ske ved at autentificere brugeren på mindst samme NSIS sikringsniveau (fx med et andet Elektronisk Identifikationsmiddel), samt at aktiveringskoder leveres i en ubrudt og kryptografisk sikret session etableret på baggrund af denne autentifikation. Levering af en aktiveringskode via separat SMS eller (ukrypteret) e-mail betragtes ikke som tilstrækkeligt sikkert på niveau Høj.

3.2.3 Suspendering, spærring og genaktivering

Niveau: Lav	Krav: 1) Det skal være muligt for brugeren/ejeren af et Elektronisk Identifikationsmiddel at suspendere (midlertidigt forhindre anvendelse) og/eller spærre (permanent forhindre anvendelse) hurtigt og effektivt.
Vejledning: Et vigtigt element i sikkerheden for Elektroniske Identifikationsmidler er brugernes aktive medvirken, der bl.a. kan opnås gennem oplysningskampagner, awareness, brugervilkår mv. Særligt centralt er brugernes[8] mulighed for at spærre eller evt. suspendere deres Elektroniske Identifikationsmiddel ved mistanke om kompromittering. En sådan spærrefunktion hos udstederen bør være tilgængelig (fx via en hjemmeside) og kan gerne bestå af flere kanaler (fx også telefonisk henvendelse). Udstederen har en særlig pligt til at sikre, at et Elektronisk Identifikationsmiddel ikke kan anvendes efter spærring fx ved at udgive en spærreliste for PKI-baserede Elektroniske Identifikationsmidler eller ved at markere en bruger eller identifikationsmiddel som spærret – og fejl i forbindelse med dette vil normalt blive betragtet som en skærpelse i forhold til bestemmelser om ansvar og erstatningspligt.	

Niveau: Lav	Krav: 2) Der skal etableres foranstaltninger, som sikrer mod, at Elektroniske Identifikationsmidler spærres eller suspenderes uretmæssigt i et forsøg på at lukke en legitim Persons adgang.
Vejledning: I implementeringen af spærrefunktionen er det relevant at tage højde for risikoen for *denial-of-service* angreb, hvor uvedkommende forsøger at spærre andres Elektroniske Identifikationsmidler – fx ved at etablere mekanismer, der gør det vanskeligt at massespærre Elektroniske Identifikationsmidler samt kontroller der sikrer, at det er rette vedkommende (eller anden autoriseret part), der spærrer sit Elektroniske Identifikationsmiddel. I den forbindelse kan kontrolspørgsmål evt. spille en rolle.	

Niveau: Lav	Krav: 4) Udstederen af et Elektronisk Identifikationsmiddel, skal på eget initiativ spærre et Elektronisk Identifikationsmiddel:

[8] Samt evt. andre autoriserede parter som fx en relevant myndighed.

	○ hvis der er mistanke om kompromittering eller tab af kontrol over dette, ○ hvis der konstateres fejl i det Elektroniske Identifikationsmiddel (fx forkerte data), ○ hvis der ikke længere foreligger en gyldig aftale[9] mellem udsteder og ansøger
Vejledning: En udsteder af Elektronisk Identifikationsmidler skal selvstændigt spærre et Elektronisk Identifikationsmiddel ved begrundet mistanke om kompromittering - en situation kendt fra kreditkort, som kan blive præventivt spærret af udstederen, hvis fx en netbutik har fået kompromitteret de handlendes kreditkortinformationer. Dette kan eksempelvis være relevant, hvis udstederen har konstateret en sikkerhedshændelse hos sig selv (evt. hos underleverandører), som har (eller med stor sandsynlighed har) kompromitteret sikkerheden af de udstedte Elektronisk Identifikationsmidler eller brugeridentiteter. Et andet eksempel kan være, at en tjenesteudbyder retter henvendelse om mistænkelig brugeradfærd for en eller flere brugere, der er autentificeret med Elektroniske Identifikationsmidler fra udstederen. Et tredje eksempel kan være suspension ved konstatering af for mange på hinanden følgende afviste loginforsøg eller ved andre spor af mistænkelig brugeraktivitet, der kan konstateres i logs, via SIEM systemer etc. Ved mindre alvorlige scenarier eller mistanke kan en suspendering være et alternativ til spærring. En suspendering er mindre indgribende for brugeren og kan give tid til at undersøge omstændighederne nærmere, inden der gribes til en endegyldig spærring. Det anbefales, at der udformes en procedure for spærring, som sikrer konsekvent og personuafhængig håndtering. Muligheden for proaktiv spærring fra udstederens side afhænger naturligvis af de konkrete forhold – herunder adgang til viden og logfiler om brugen af Elektroniske Identifikationsmidler, efterretninger etc. En udsteder er naturligvis ikke forpligtet til at agere på viden, som denne ikke har. I tilfældet med en Lokal IdP, hvor Elektroniske Identifikationsmidler udstedes inden for egen organisation, kan mulighederne for at opdage kompromittering være bedre grundet nærhed mellem bruger og udsteder. Dette krav hænger sammen med afsnit 4.1.6 krav 4, som stiller krav til løbende opdatering af sikkerheden i løsningen samt håndtering af hændelser og brud. Opdagelse af en sikkerhedshændelse kan således medføre behov for spærring af Elektroniske Identifikationsmidler, hvis disse er berørt af hændelsen. Dette må bero på en konkret vurdering af hændelsens karakter og konsekvenser.	

Niveau: Betydelig	Krav: 6) Suspenderings- og spærrefunktion skal være til rådighed døgnet rundt og have en høj grad af tilgængelighed.

[9] Lovgivning kan træde i stedet for en aftale.

Vejledning: Hvis suspenderings- og spærrefunktionen drives som en selvbetjeningsløsning kan tilgængeligheden af løsningen dokumenteres med f.eks. SLA'er og driftsrapporter, som viser den målte oppetid i forhold til et dokumenteret servicemål, suppleret med en test af at spærrefunktionen er funktionel. Der er således ikke et krav om døgnbemanding af personale.	

3.2.4 Fornyelse og erstatning

Niveau: Høj	Krav: 2) Hvor fornyelsen baseres på en gyldig elektronisk identifikation, skal personidentifikationsdata og eksistens af Entiteten verificeres på ny mod en Autoritativ kilde.
Vejledning: På niveau Høj skal man genverificere mod autoritative kilder ved fornyelse med henblik på at sikre, at ændringer i disse slår igennem på et Elektronisk Identifikationsmiddel.	

NSIS stiller ikke konkrete krav om udløbsperioder men lader dette være op til en konkret risikovurdering af den samlede implementering. Dette er begrundet i, at visse typer Elektroniske Identifikationsmidler bliver svagere i takt med at de anvendes (fx kodeord som anvendes hyppigt og på mange forskellige enheder), hvilket kan mitigeres med kortere intervaller for udløb/fornyelse, mens andre i højere grad bevarer deres styrke uanset hyppigheden af deres anvendelse (fx smart cards).

3.3 Anvendelse og autentifikation

3.3.1 Autentifikationsmekanismer

Niveau: Lav	Krav: 1) Frigivelsen af personidentifikationsdata finder sted efter en pålidelig kontrol af det anvendte Elektroniske Identifikationsmiddel og dets gyldighed og på en måde, hvor fortrolighed og integritet af afgivne data sikres. 2) Hvis personidentifikationsdata er lagret som en del af autentifikationsmekanismen, er disse oplysninger sikret på en måde, der beskytter dem mod at gå tabt eller blive kompromitteret, herunder ved offline analyse.

Vejledning:
Bemærk at der i NSIS ikke er krav om lagring af personidentifikationsdata i et Elektronisk Identifikationsmiddel eller frigivelse af sådanne data i forbindelse med en autentifikationsproces. Dette betyder, at autentifikationen *kan* være pseudonym mod en tjeneste - udstederen af identifikationsmidlet skal blot kende den fysiske Identitet bag et Elektronisk Identifikationsmiddel i forbindelse med udstedelsen samt have en separat log af denne. Hvis der er lagret (person)data relateret til identifikationsmidlet (fx i et X.509 certifikat), må disse ikke frigives (overleveres) til modtageren, før identifikationsmidlet er kontrolleret (i tilfældet med et certifikat vil det fx være at brugeren har autoriseret adgang til den tilhørende private nøgle).

Niveau: Lav	Krav:
	3) Autentifikationsmekanismen implementerer sikkerhedskontroller til at efterprøve Elektroniske Identifikationsmidler, således at det er højst usandsynligt, at det er muligt for en angriber med en øget basal Angrebskapacitet at gætte, lytte sig til, gengive eller manipulere kommunikationen og på den måde omgå autentifikationsmekanismen.
Vejledning: Bemærk at der med formuleringen "efterprøve" i kravet menes, at autentifikationsmekanismen i forbindelse med en konkret autentifikation af en slutbruger skal validere det specifikke Elektroniske Identifikationsmiddel tilhørende brugeren fx gennem en kryptografisk challenge / response protokol, og at denne validering skal sikre, at de nævnte sikkerhedsmæssige egenskaber vedr. integritet og fortrolighed opfyldes, herunder ved at forhindre / modstå fx 'replay' angreb. Samme formulering anvendes under punkt 5) og 6). Det er med andre ord et krav til valideringer og kontroller indbygget i autentifikationsmekanismen – ikke til sikkerhedstest. Kontrol af at kravet opfyldes kan ske gennem test, threat modelling, sårbarhedsstyring eller en risikoanalyse for autentifikationsmekanismen, herunder en vurdering af valideringer og kontroller indbygget i autentifikationsmekanismen set ift. ovennævnte trusler. Autentifikationsmekanismer kan normalt ikke fuldstændigt forhindre alle typer angreb – men kan kun modstå angreb til et givet niveau. En måde at udtrykke dette på er, at rangordne de forskellige mekanismer i henhold til deres modstandskraft mod angribere med en bestemt angrebskapacitet. Som tidligere nævnt er denne terminologi er hentet fra ISO 15408 og det anbefales at gennemgå denne standard som ramme for at forstå terminologien omkring angrebskapacitet. Ved estimering af modstandskraften er det relevant at se på trusler – ISO 29115 nævner fx flg. trusler: online guessing, offline guessing, kopiering af Elektronisk Identifikationsmiddler, phishing, aflytning, replay attack, session hijacking, man-in-the-middle, tyveri af Elektroniske Identifikationsmidler, spoofing og masquerading.	

I mange sammenhænge vil autentifikationsmekanismen blive leveret af en serviceleverandør eller et stykke standardprogrammel, og opfyldelsen kan i givet fald løftes gennem revisorerklæring fra leverandørerne. Ved indkøb af identifikationsmidler kan man med fordel anskaffe enheder / løsninger, som har anerkendte sikkerhedscertificeringer som FIPS 140, Common Criteria, FIDO certificering eller lignende, idet de sikkerhedsmæssige egenskaber så er verificeret af en uafhængig part, og hvor argumentation for opfyldelse af sikkerhedskrav i NSIS så kan opnås ved at henvise til denne certificering.

4 Organisatoriske- og tværgående krav

4.1.1 Generelle krav

Kravene i kapitel 4 skal opfyldes både af udstedere af Elektroniske Identifikationsmidler og Identitetsbrokere.

Niveau: Lav	Krav: 2) Organisationer, som leverer ID-tjenester, skal til enhver tid overholde gældende lov herunder den gældende regulering af databeskyttelse, forvaltningsloven (hvis offentlig myndighed), [eIDAS] forordningen samt anden relevant lovgivning.
Vejledning: Overholdelse af EU-forordning om eID og tillidstjenester er kun relevant for Elektroniske Identifikationsordninger, der anmeldes af Danmark til EU-kommissionen i regi af [eIDAS]-forordningen. Kun Digitaliseringsstyrelsen kan anmelde nationale, elektroniske identifikationsordninger, hvorfor anmeldelse kræver aftale med Digitaliseringsstyrelsen. Der er ikke krav om at bevise, man overholder loven, og det er normalt tilstrækkeligt at foretage en selvevaluering baseret på en lov-screening (fx årligt). Anmelderen skal selv foretage en vurdering af, hvilken lovgivning, der er relevant at overholde.	

Niveau: Lav	Krav: 3) Organisationer, som leverer ID-tjenester, er ansvarlige for opfyldelse af forpligtelser, som er overdraget til tredjepart.
Vejledning: Denne bestemmelse går alene på situationen, hvor organisationer anvender underleverandører til opfyldelse af **egne** forpligtelser i medfør af kravene i NSIS. Dette medfører altså ikke forpligtelser for modpartens tjenester ved indgåelse i føderation – eksempelvis når en Identitetsbroker stoler på en anden Identitetsbroker eller Elektronisk Identifikationsordning, hvor næste led i kæden er anmeldt under NSIS på et tilsvarende Sikringsniveau. Ydelser fra underleverandører, som er NSIS anmeldt i den leverede form, skal ikke dokumenteres, hvis de er optaget på NSIS-positivlisten på samme eller højere sikringsniveau som den aktuelle anmeldelse. I disse tilfælde er det tilstrækkelige at henvise til den relevante ID-tjeneste på NSIS-positivlisten samt hvilke krav, der håndteres for anmelderen. Detaljer om håndtering af revision af serviceleverandører, herunder genbrug af eksisterende erklæringer fra disse, er beskrevet i vejledningen til anmeldelses- og revisionsprocessen [REV]. Anvendes eksempelvis teknologi eller produkter fra en ekstern part til autentifikation i en Lokal IdP løsning (FIDO, Windows Hello etc.), er det relevant at dokumentere, hvilke krav i NSIS mødtet på den Lokale IdP, der håndteres den eksterne	

part. Dokumentationen skal være tilstrækkelig til, at anmelders revisor kan underskrive erklæringen om, at kravet er opfyldt for den Lokale IdP – eksempelvis at det valgte FIDO token lever op til fx relevante NSIS krav i afsnit 3.2.1 på det anmeldte sikringsniveau. Det vil bero på en konkret vurdering, hvilke krav i NSIS, der håndteres af underleverandøren, da dette kan variere betydeligt i praksis. For en 'standard' hostingleverandør uden applikationsansvar vil det typisk være (dele af) de generelle krav fra kapitel 4.1.3 – 4.1.6, der er relevante, mens en Full-service Lokal IdP kan varetage samtlige krav i NSIS på vegne af en brugerorganisation.

Niveau: Betydelig	Krav: 4) Organisationer som leverer ID-tjenester skal være i stand til at dokumentere deres evne til at påtage sig risikoen for at bære erstatningsansvar, og at de har tilstrækkelige finansielle ressourcer til at fortsætte driften og levere tjenester.
Vejledning: Evnen til at kunne bære erstatningsansvar kan fx demonstreres gennem ansvarsforsikring, selvforsikringsordninger for offentlige myndigheder eller tilsvarende sektorregulering som bl.a. findes i den finansielle sektor. Herunder et eksempel på en situation, der kunne medføre erstatningsansvar: "En organisations anmeldte registreringsprocedurer følges ikke i praksis, således at en medarbejder lykkes med at tilknytte en læges CPR-nummer til sin medarbejderidentitet og herefter logger ind og udskriver kostbar medicin. "	

Niveau: Betydelig	Krav: 5) Private organisationer, som leverer ID-tjenester, skal have en beskrevet termineringsplan, som sikrer en hensigtsmæssig nedlukning eller overtagelse af tredjepart, underretning af myndigheder og brugere. Planen skal indeholde detaljer om, hvordan data opbevares, beskyttes og destrueres.
Vejledning: Kravene til termineringsplan skal dække både anmelderorganisationens eget ophør såvel som nedlukning foretaget af myndigheder og bør dække alle forudseelige omstændigheder, der kan føre til terminering og/eller fortsættelse af servicen under en anden leverandør.	

4.1.2 Oplysningspligt

Niveau: Lav	Krav: 1) Der skal offentliggøres en servicebeskrivelse for Identitetsbrokere og Elektroniske Identifikationsordninger, som beskriver alle relevante betingelser, betalinger for og begrænsninger i brugen af ID-tjenesten. Servicebeskrivelsen skal indeholde en privatlivspolitik, som opfylder kravene i [GDPR].

Vejledning:

Bemærk at dele af dette krav kan være opfyldt via 3.1.1, hvor slutbrugeren skal gøres bekendt med betingelser for brugen af elektroniske identifikationsmidler. Kravet i 4.1.2 går videre end at oplyse slutbrugerne – det kan fx være relevant at stille betingelser til Tjenesteudbydere og brokere, der anvender en Lokal IdP til autentifikation.

Hvis en løsning (som fx Lokal IdP) udelukkende benyttes af interne medarbejdere, er det tilstrækkeligt at publicere servicebeskrivelsen på fx et intranet.

Hvis en tillidskæde indeholder flere elementer (fx Lokal IdP => Broker => Sub broker => Tjeneste) er det tilstrækkeligt at informere næste led i kæden, idet der ikke nødvendigvis er kendskab til parterne længere ude i kæden. Kravene til en servicebeskrivelse kan også være givet af vilkår eller en formel aftale – eksempelvis er en Lokale IdP tilsluttet NemLog-in underlagt NemLog-in's vilkår for brugerorganisationer, hvorfor en Lokal IdP ikke skal meddele NemLog-in en servicebeskrivelse. Hvis en Lokal IdP ikke har nogen tjenester koblet direkte til IdP'en men alene brokere, kan kravet fraviges, da de pågældende brokere så vil håndtere det i forhold til deres tilkoblede tjenester.

Det forudsættes generelt, at anmelderen overholder relevant lovgivning. Under privatlivspolitik samt oplysninger om behandling af personoplysninger bør anmelderen iagttage kravene til oplysningspligt i databeskyttelseslov og [GDPR], som stiller eksplicitte krav både til form og indhold.

Som inspiration for relevante emner har NemLog-in brokeren publiceret vilkår for private tjenesteudbydere som kan findes her: https://tu.nemlog-in.dk/tilslutning/vilkar/privat-tjenesteudbyder/. Forholdene i en Lokal IdP kan dog være meget anderledes end i en fællesoffentlig broker.

4.1.3 Informationssikkerhedsledelse

Niveau: Betydelig	Krav: 2) Ledelsessystemet for ID-tjenesten skal være i overensstemmelse med principperne i [ISO 27001] standarden.

Vejledning: Håndtering af risici er særdeles relevant for udstedere af Elektroniske Identifikationsmidler samt Identitetsbrokere. For at være effektivt, må ledelsessystemet for informationssikkerhed (ISMS) håndtere relevante risici for alle dele af en løsning. Afhængigt af den organisatoriske struktur, kan et eksisterende ISMS dække en Elektronisk Identifikationsordning eller Identitetsbroker. Det er dog ikke et krav, at der er etableret et ISMS for hele organisationen, men det er tilstrækkeligt, at ID-tjenesten er dækket af et ISMS. Under kravene til informationssikkerhedsledelse er det relevant at påpege, at man på niveau Betydelig kun er forpligtet til at have et ledelsessystem, som følger principperne i [ISO 27001], og derfor kan benytte alternative rammeværk med tilsvarende indhold. Ved 'principperne' i ISO 27001 skal forstås en ledelsesforankret, systematisk og risikobaseret tilgang til at håndtere fortrolighed, integritet og tilgængelighed for aktiver som data og systemer. Der bør således foreligge en ledelsesgodkendt informationssikkerhedspolitik og sikkerhedshåndbog, et SOA dokument mv.	

Niveau: Høj	Krav: 4) Ledelsessystemet for ID-tjenesten skal være certificeret efter [ISO 27001] standarden eller der skal på tilsvarende måde kunne dokumenteres efterlevelsen af krav til informationssikkerhedsledelse.
Vejledning: Kravet kan opfyldes gennem en ISO 27001-certificering eller en erklæring fra en uafhængig, godkendt revisor med kompetence indenfor området, der har gennemført revision af ISMS'et for den elektronisk Identifikationsordning eller Identitetsbroker efter ISO/IEC 27007. Ved sidstnævnte fremgangsmåde skal revisor dokumentere sin kompetence fx ved henvisning til relevante certificeringer (fx CISA og/eller ISO 27001 Lead Auditor) samt uddannelse og/eller erfaring indenfor ISO/IEC 27001 og 27007. Hvis Anmelder i al væsentlighed blot agerer som indkøber af ydelser fra underleverandører og ikke selv har et operationelt ansvar for sikkerhedskontroller i medfør af NSIS (fx foretager Identitetssikring eller drifter it-systemer), er det tilstrækkeligt, at underleverandørerne opfylder kravet om ISO-certificering eller tilsvarende.	

4.1.4 Logning

Niveau: Lav	Krav:

	1) Relevant information skal logges og beskyttes i henhold til gældende lov samt god praksis inden for databeskyttelse og forvaltning.
Vejledning: Logdata bør udformes, så de indeholder færrest mulige personoplysninger (i henhold til princippet om dataminimering), samtidig med at de opfylder deres forretningsmæssige formål i forhold til sporbarhed, sikkerhed og dokumentation.	

Niveau: Lav	Krav: 3) Informationer (herunder logs) skal opbevares og beskyttes, så længe de er nødvendige af hensyn til revision eller efterforskning af sikkerhedshændelser, under hensyntagen til lovgivningens begrænsninger, hvorefter de skal slettes sikkert.
Vejledning: For centrale logningsdata, som er vigtige for afklaring af hændelser og tvister, kan det som tommelfingerregel anbefales at gemme disse i løbende kalenderår plus frem år – med mindre at lovgivningen eller de forretningsmæssige behov tilsiger noget andet for de konkrete data. Her kan det fx være relevant at skele til bogføringsloven. Det kan i øvrigt anbefales at adskille logninger, som indeholder personoplysninger, fra logninger som indeholder øvrige typer data, da hensyn til persondatabeskyttelse typisk vil tilsige, at disse slettes efter en kortere periode, mens fx administrative handlinger typisk vil blive gemt i en længere periode.	

4.1.5 Faciliteter og personale

For områder, hvor der kræves særlige færdigheder af personalet, bør der være etableret træningsprogrammer som sikrer, at de relevante medarbejdere oparbejder og vedligeholder de nødvendige færdigheder.

Niveau: Lav	Krav: 1) Der skal findes procedurer, som sikrer, at personale og underleverandører er tilstrækkeligt uddannede, kvalificerede, erfarne og har de færdigheder, der er behov for, når de skal udfylde deres roller.
Vejledning: Et særligt vigtigt område for udstedere af Elektroniske Identifikationsmidler er identitetssikringsprocessen, hvor personale i nogle sammenhænge udfører en vigtig opgave i identitetssikringen ved fx at kontrollere pas og kørekort. Af øvrige områder kan nævnes administratorer, sikkerhedspersonale, auditorer og andre, som udfører betroede funktioner og har særlige systemadgange.	

For underleverandører kan der etableres aftaler, revision eller andre mekanismer, der sikrer opfyldelse af kravet for deres område. Et eksempel kan være, at medarbejdere hos fx en driftsleverandør skal besidde særlige kompetencer fx i form af certificeringer mv. I ISO 27001 indgår området i Annex A under 'Human Resources Security' og vil derfor normalt være håndteret som en del af organisationens ISMS.

Niveau: Lav	Krav: 3) Driftsfaciliteter skal løbende overvåges for og beskyttes imod skade forvoldt ved miljøkatastrofer, uautoriseret adgang eller andre faktorer, som kan påvirke tjenestens sikkerhed.
Vejledning: Driftsfaciliteter for ID-tjenester bør have et basalt niveau af fysisk sikkerhed i form af adgangskontrol, alarmer, indbrudssikring, nødstrømsanlæg, brandsikringsanlæg mv. Området vil typisk være en del af organisationens ISMS, eksempelvis indgår 'Physical and Environmental Security' i ISO 27001 Annex A. Ved outsourcing af drift vil leverandøren typisk have erklæringer eller certificeringer, der kan lægges til grund som fx 3402 erklæringer, certificeringer fra Uptime Institute etc.	

Niveau: Betydelig	Krav: 5) Det skal kontrolleres, at ledere og medarbejdere, der udfører betroede opgaver, ikke er straffet for en forbrydelse, der gør dem uegnede til at bestride deres hverv, samt at medarbejdere og ledere har tilstrækkelig uddannelse og erfaring. Det samme gælder leverandører og underleverandører.
Vejledning: Med betroede opgaver skal man tænke i NSIS-relevante kontroller. Eksempler kunne være "RA-medarbejdere" som kontrollerer pas etc. for at verificere identiteten af personer / medarbejdere, sikkerhedsadministratorer / AD-administratorer eller andre, som i kraft af deres arbejde har udvidede adgange til brugerkatalog / systemopsætning og ville kunne omgå de almindelige sikkerhedskontroller i relation til identiteter og identifikationsmidler. Det er således personer, der udfører manuel identitetssikring samt superbrugere / privilegerede brugere, der i kraft af deres adgange ville kunne begå svindel med identiteter og identifikationsmidler, som kravet er rettet imod. Eksempelvis vil en personaleleder, som opretter en medarbejder i organisationens HR- eller lønsystemer, og som ikke selv udfører identitetssikring men alene	

opretter forbindelsen (se afsnit 5.2) eller inviterer brugere til et digitalt oprettelsesforløb, ikke være at betragte som en betroet medarbejder i NSIS regi. Hvis personalelederen eller HR-medarbejderen ikke udfører identitetssikring, forudsættes naturligvis at andre personer eller processer håndterer dette (fx login med privat MitID), således at der ikke sker automatisk brugeroprettelse med tilhørende NSIS-niveau uden at kravene i afsnit 3.1.2 er opfyldt. Ej heller vil en person, der administrerer rettigheder, skulle opfattes som 'betroet' i regi af NSIS, idet rettigheder slet ikke er en del af rammeværket, og adgang til at nedlægge en bruger vil heller ikke i sig selv skulle anses som en betroet opgave. Organisationen kan indhente straffeattester årligt, der dokumenter strafforhold for betroede medarbejdere, eller endnu stærkere kan man alternativt indhente sikkerhedsgodkendelser fra PET. Bemærk at NSIS ikke specificerer, hvornår man er egnet / uegnet til at varetage en opgave – dette er således en lokal vurdering. Det vil således være op til en konkret vurdering hos anmelderen, om eventuelle straffeforhold gør ledere og medarbejdere uegnede til at bestride deres hverv. Typisk ligger indhentning og screening af straffeattester i organisationens HR-funktion, der opererer på baggrund af lister over betroede medarbejdere. Det er vigtigt at sikre et revisionsspor for, at denne proces har været udført – fx en log af at straffeattesten har været screenet på en bestemt dato for en bestemt medarbejder, men dette betyder ikke, at selve straffeattesten skal gemmes efterfølgende. For underleverandører gælder samme krav for dennes medarbejdere, hvis de udfører betroede opgaver for anmelderen, og når disse opgaver er underlagt krav i NSIS. Det kan eksempelvis være systemadministratorer hos en driftsleverandør med udvidet adgang til anmelderens system og med mulighed for at omgå etablerede sikkerhedskontroller, så de eksempelvis selv ville kunne oprette brugere. Opfyldelse af krav til baggrundstjek hos en underleverandør kan typisk dokumenteres gennem en revisionserklæring, som anmelderen kan henvise til i sin egen anmeldelse. Driftsleverandører vil ofte have baggrundstjek inkluderet i deres ISMS og egne revisionserklæringer. I ISO 27001 indgår området i Annex A under 'Human Resources Security' og vil derfor normalt være håndteret som en del af organisationens ISMS. Der kan henvises i ISO standarden for yderligere baggrundsinformation.

Niveau: Betydelig	Krav: 7) Betroede adgange (herunder administratoradgange) i produktionssystemer skal sikres og overvåges.
Vejledning: Betroede adgange i form af administratorkonti eller brugere med privilegerede adgange er kritiske at sikre og overvåge, da kompromittering ofte kan udløse store konsekvenser. Betroede adgange bør derfor være beskrevet, risikovurderet og relevante sikkerhedskontroller identificeret og implementeret. Eksempler på ofte anvendte sikkerhedsmekanismer inden for dette område er brug af stærk autentifikation (herunder to-faktor eller tilsvarende), anvendelse af	

jump-servere ved administrativt log-in til infrastrukturen, logning og overvågning af administrative handlinger, *password vaulting*, anvendelse af PIM / PAM -løsninger (Privileged Identity Management / Privileged Access Management), periodisk gennemgang af logs med administratorhandlinger etc. Kravet skal forstås i forhold systemer, der er kritiske i forhold til NSIS processer, og hvor den betroede adgang vil kunne anvendes til at omgå vigtige kontroller i NSIS relateret til fx identitetssikring, autentifikation mv. Det kan eksempelvis være nyttigt at definere en særlig gruppe af systemer og/eller en særlig gruppe af administratorer, der er relevant for NSIS, som overvågningen afgrænses i forhold til, således at kravet isoleres til en mindre del af organisationen eller systemlandskabet.

4.1.6 Tekniske kontroller

Niveau: Lav	Krav: 1) Der findes rimelige tekniske kontroller, som gør det muligt at afværge trusler mod tjenesternes sikkerhed og sikre de behandlede oplysningers fortrolighed, integritet og tilgængelighed.
Vejledning: De tekniske kontroller har til formål at understøtte fortrolighed, integritet og tilgængelighed. Med begrebet 'rimelige tekniske kontroller' i NSIS refereres til, at kontrollerne skal nedbringe risici for tab af fortrolighed, integritet og tilgængelighed til et acceptabelt niveau ud fra en risikovurdering, hvor det ønskede Sikringsniveau er taget i betragtning. Som eksempel vil det være naturligt at risikoniveauet i risikovurderingen øges i takt med det ønskede Sikringsniveau, således at konsekvenserne ved tab af integritet på Sikringsniveau Høj er langt større end konsekvenserne på Sikringsniveau Lav. En organisation vil typisk sikre et tilstrækkeligt niveau af tekniske kontroller ved at implementere et ISMS, der identificerer aktiver, trusler og sårbarheder, samt iværksætter kontroller der nedbringer sandsynligheden for tab af fortrolighed, integritet og tilgængelighed til et acceptabelt niveau. Som inspiration til konkretisering af et 'rimeligt' niveau for tekniske kontroller kan der henvises til de tekniske minimumskrav for statslige myndigheder[10] eller tilsvarende anbefalinger på det kommunale område[11]. For NSIS er scope dog afgrænset til systemer eller processer, der er relevante for eller anvendes i den anmeldte ID-tjeneste. For udstedere af Elektroniske Identifikationsmidler vil aspektet 'integritet' ofte være vigtigere end fortrolighed og tilgængelighed, idet konsekvenserne ved at en bruger kan udgive sig for en anden ofte er de største - afhængigt af hvilke data i	

[10] https://sikkerdigital.dk/myndighed/tekniske-tiltag/tekniske-minimumskrav/tekniske-minimumskrav-2024

[11] https://www.kl.dk/media/5rpj3xi2/anbefalinger-om-tekniske-minimumskrav-i-kommuner-2023.pdf

forretningstjenester, der kan opnås adgang til. Da Elektroniske Identifikationsordninger sjældent behandler følsomme personoplysninger (i sig selv), er konsekvenserne ved tab af fortrolighed ofte mindre. Endelig er der aspektet tilgængelighed, hvor nedetid af en Elektronisk Identifikationsordning kan føre til manglende adgang til de bagvedliggende forretningstjenester, der anvender Elektroniske Identifikationsmidler. Her vil kritikaliteten skulle ses i forhold til disse tjenester samt brugernes muligheder for at få adgang via alternative kanaler. Ovenstående er ment som generelle tommelfingerregler, og der bør under alle omstændigheder foretages en konkret og detaljeret risikovurdering. For yderligere vejledning i og god skik for håndtering af kryptografisk materiale kan der henvises til ISO 27001 standarden under kontrollerne A.9 'Access control' og A.10 'Cryptography', og for håndtering af medier kan der henvises til kontrollerne under A.8 'Asset Management'.

Niveau: Lav	Krav: 4) Der er indført procedurer, som garanterer, at sikkerheden bevares over tid, og at der er mulighed for at reagere på ændringer i risikoniveau, sikkerhedshændelser og brud på sikkerheden.
Vejledning: Organisationens ISMS bør sikre, at der løbende tages højde for ændringer i løsninger og procedurer, ændrede trusler, nye sårbarheder mv. og at læring fra hændelser løbende indarbejdes. ISO 27001 følger eksempelvis en PDCA (Plan-Do-Check-Act) cyklus kendt fra Deming's cyklus for kontinuerlige procesforbedringer. Konkret kan man indføre procedurer for at risikovurdere alle større ændringer til ID-tjenesten, og man kan planlægge aktiviteter som risikovurderinger, sikkerhedstest og beredskabsøvelser som faste, årlige begivenheder i et årshjul for at sikre kontinuitet og løbende forbedringer.	

Niveau: Betydelig	Krav: 5) Alle medier, som indeholder personlige, kryptografiske eller andre fortrolige eller følsomme oplysninger, lagres, transporteres og bortskaffes på en sikker måde.
Vejledning: Kravet dækker basal informationssikkerhed vedr. håndtering af lagringsmedier med følsomt indhold vedr. brugere og identifikationsmidler, som typisk kan befinde sig på servere, SAN etc. Der kan henvises til ISO 27001 "Annex A.8.3 Media Handling" for yderligere beskrivelser.	

Niveau: Betydelig	Krav:

	7) Der må ikke benyttes kryptografiske algoritmer eller protokoller med kendte sårbarheder eller med utilstrækkelige nøglelængder.
Vejledning: Implementering af kryptografisk beskyttelse er typisk en opgave for specialister med særlige forudsætninger på området, og ofte vil implementeringen for en Lokal IdP blive varetaget gennem underleverandører eller standardprogrammel. Der kan dog være en opgave med at konfigurere programmel eller løsninger, herunder de ønskede algoritmer og nøglelængder. Der er konstant udvikling i computerkraften samt forskningen inden for kryptografi, og derfor giver NSIS ikke en fast liste af algoritmer eller nøglelængder. For identitetsbrokere kan man i OIOSAML 3 profilen[12] afsnit 3.3 læse konkrete forslag til algoritmer og nøglelængder, der er vurderet tilstrækkelige til den offentlige sektor. Som en simpel tommelfingerregel vil symmetrisk kryptering baseret på AES-algoritmen med en nøglelængde på minimum 128 bit være tilstrækkelig til de fleste formål, og for RSA nøgler til asymmetrisk kryptering og signaturer anbefales som minimum 3072 bit nøgler. Kryptografi er dog et komplekst område med mange aspekter, der skal tages højde for. Mere generelle og omfattende kilder til 'best practice' anbefalinger indenfor kryptografiske algoritmer er "Agreed Cryptographic Mechanisms v1.2" https://www.sogis.eu/documents/cc/crypto/SOGIS-Agreed-Cryptographic-Mechanisms-1.2.pdf samt ENISA rapporten ' Algorithms, Key Sizes and Parameters Report - 2013' https://www.enisa.europa.eu/publications/algorithms-key-sizes-and-parameters-report?v2=1	

[12] https://digst.dk/it-loesninger/standarder/oiosaml-profiler/

4.1.7 Anmeldelse og revision

Elektroniske Identifikationsordninger og Identitetsbrokere skal underlægges periodevis intern eller ekstern revision. Ved anmeldelse af løsninger på Sikringsniveau Betydelig og Høj, skal der indgå en revisonserklæring udarbejdet efter vejledningen til anmeldelses- og revisionsprocessen [REV], som Digitaliseringsstyrelsen har udgivet til formålet. Desuden er der udarbejdet et kontrolskema (Excel og Word), som kan anvendes til at dokumentere kravopfyldelse, revisionshandlinger og konklusion. Ved udfyldelse af skemaet skal der krav-for-krav redegøres for, hvordan kravet er opfyldt, hvordan revisionen er foretaget, og hvilken konklusion revisor er kommet frem til.

Revisionsvejledning, anmeldelsesskema og andet materiale vedr. NSIS er tilgængeligt på Digitaliseringsstyrelsens hjemmeside: https://digst.dk/it-loesninger/standarder/nsis/

Det anbefales udbydere af Elektroniske Identifikationsordninger og Identitetsbrokere at opbygge dokumentationen til anmeldelsen i form af en **praksis**, der specifikt adresserer alle krav fra NSIS i forhold til det relevante understøttede sikringsniveau med udgangspunkt i revisionsinstruksen.

Denne model kendes allerede fra håndtering af fx Public Key Infrastruktur, hvor der benyttes certifikatpolitikker (Certificate Policy, CP) og certificeringspraksis (Certification Practice Statement, CPS).

For at lette anmeldelsesprocessen er der udarbejdet en anmeldelsesskabelon, som oplister og strukturerer den supplerende dokumentation, der skal indsendes udover de nævnte regneark. Dette omfatter fx en beskrivelse af det organisatoriske setup, beskrivelse af ISMS, ledelseserklæringer osv. Kontrolskemaet skal altid udfyldes uanset hvilket sikringsniveau, der anmeldes på. Det er tilladt at overføre indholdet af kontrolskemaet til andre dokumenttyper, hvis dette vurderes mere praktisk, så længe indholdet bevares for de krav, der er relevante. Hvis en tjeneste understøtter flere funktionaliteter (fx hvis den både kan agere elektronisk identifikationsordning og identitetsbroker), kan der indsendes én samlet anmeldelse.

Man kan endvidere foretage en 'fælles' NSIS-anmeldelse for en flerhed af CVR-numre. Dette forudsætter dog, at både anmeldelsen (forsiden) og revisionserklæringen (omfangsbeskrivelsen) indeholder beskrivelser af det samlede system (inkl. de pågældende CVR-numre). Der må således ikke forekomme lokale varianter i processer eller systemer, som ikke er dækket af den fælles anmeldelse og den tilhørende revisionserklæring. Ved 'fællesanmeldelser' skal én af organisationerne fremgå som kontaktperson for den samlede anmeldelse.

Niveau: Lav	Krav: 1) Ved anmeldelse af en Elektronisk Identifikationsordning og/eller Identitetsbroker til Digitaliseringsstyrelsen skal der redegøres for den tekniske og sikkerhedsmæssige udformning samt Sikringsniveau og navn.

	2) Ved anmeldelse af en Elektronisk Identifikationsordning og/eller Identitetsbroker til Digitaliseringsstyrelsen skal der anvendes selvdeklarering. Anmelderen indestår herved selv for, at kravene til det angivne Sikringsniveau (Lav) er opfyldt. 3) Ved anmeldelse på niveau Lav skal der være udført intern revision, som omfatter alle nødvendige områder af de tilbudte tjenester med henblik på at sikre overholdelse af relevante krav og politikker. Anmelderen skal på sikringsniveau Lav endvidere årligt indsende en ledelseserklæring som bekræfter, at den oprindelige anmeldelse fortsat er retvisende og løsningen er aktiv – eller alternativt opdatere sin anmeldelse eller bede om afnotering fra listen over anmeldte løsninger. Såfremt der gennemføres ekstern revision ift. sikringsniveau Betydelig eller Høj, bortfalder kravet til intern revision.
Vejledning: Digitaliseringsstyrelsen forventer i forbindelse med en anmeldelse at modtage fyldestgørende dokumentation for den anmeldte Elektroniske Identifikationsordning eller Identitetsbroker, herunder dokumentation for den gennemførte revision. På sikringsniveau Lav er dette den interne revision og på øvrige sikringsniveauer er der tale om ekstern revision, der træder i stedet for intern revision. Revisor skal dokumentere sin samlede konklusion af den foretagne revision samt med sin underskrift bekræfte denne. Anmelderen skal på sikringsniveau Lav årligt indsende en ledelseserklæring på, at anmeldelsen fortsat er retvisende og løsningen er aktiv – eller alternativt opdatere sin anmeldelse eller bede om afnotering fra listen over anmeldte løsninger. Endvidere skal anmelderen på sikringsniveau Lav indsende dokumentation for den gennemførte, interne revision. Hvis en anmeldt ID-tjeneste ophører, skal der indsendes en afsluttende ledelseserklæring, som dækker perioden frem til ophørsdatoen.	

Niveau: Betydelig	Krav: 4) Ved anmeldelse på niveau Betydelig anvendes selvdeklarering suppleret med en revisionserklæring fra en uafhængig, godkendt revisor med relevante kompetencer indenfor it-revision eller et akkrediteret overensstemmelsesvurderingsorgan (jf. [eIDAS] artikel 3, stk. 1, nr. 18). Denne skal bekræfte, at løsningens tekniske og sikkerhedsmæssige udformning er

	gennemgået, at kravene i denne standard er overholdt af løsningen på det angivne Sikringsniveau, og at der er implementeret processer for løbende at sikre, at det angivne Sikringsniveau opretholdes. Anmeldelsen suppleres med en ledelseserklæring underskrevet af en tegningsberettiget, hvoraf det fremgår, at alle relevante krav er opfyldt og fornødne processer for opretholdelse er implementeret. Der skal årligt indsendes en ny revisionserklæring, som bekræfter, at kravene til stadighed opfyldes.

Vejledning:

Såfremt ID-tjenesten på et tilsvarende Sikringsniveau er underlagt formaliseret tilsyn og/eller audit i henhold til lov eller kontrakt med en offentlig myndighed, kan revisions- og ledelseserklæring herfra genanvendes. Dette er nærmere beskrevet i NSIS revisionsvejledningen, ligesom der i denne er redegjort for håndtering af underleverandører.

Digitaliseringsstyrelsen forpligter sig ikke til at kontrollere rigtigheden af dokumentationen men vil lægge revisors/overensstemmelsesorganets erklæring til grund, medmindre dokumentationen giver anledning til tvivl herom.

Revisionserklæringen spiller således en vigtig rolle for tilliden i NSIS, da denne er den primære garant for, at kravene i NSIS er overholdt. Revisionserklæringen modsvarer peer-review processen ved anmeldelse af nationale eID ordninger under [eIDAS], hvor medlemslandene i en proces styret af Kommissionen gennemgår eID ordninger i forbindelse med anmeldelse. Bemærk at det ikke længere er et krav, at der skal udføres intern revision, hvis der anmeldes på sikringsniveau Betydelig eller Høj. Man kan finde yderligere information om typer, frister og perioder for erklæringer i NSIS revisionsvejledningens afsnit 1.3.1.

Revisor skal være uafhængig og godkendt, hvilket samlet betegnelse for både en statsautoriseret og en registreret revisor[13]. Revisor bør desuden have relevante kompetencer inden for it-revision i form af en CISA-certificering eller tilsvarende.

Det er vigtigt at designe løsninger og kontrolprocesser, så der dannes et revisionsspor (skriftligt bevis), der kan dokumentere overholdelse af NSIS-kravene over for en revisor – særligt på niveau Betydelig og Høj. Det er således ikke tilstrækkeligt, at kravene i sig selv overholdes – dette skal også være dokumenterbart. Bemærk at kravet om type 2 erklæringer i vejledningen til anmeldelses- og revisionsprocessen [REV] indebærer, at organisationen skal kunne dokumentere, at kontrollerne udføres løbende i løbet af perioden, herunder eksempelvis at der er dokumentation for oprettelser / nedlæggelser af brugere. Til brug for type 2 erklæringerne kan det være relevant at sikre en eksplicit ændringshåndtering ('change proces'), hændelseslogs og andet, da en væsentlig del af kravene typisk går på konfigurationer, hvor det kan være vanskeligt for revisor at teste bagud i tid, hvorfor kontrol over en periode derfor indebærer, at der er effektive kontroller og sporbarhed omkring ændringshåndtering af ID-tjenesten.

[13] https://www.fsr.dk/politik-analyse/om-revisor-og-aarsregnskaber/hvorfor-vaelge-en-godkendt-revisor

For nye løsninger, der ønskes anmeldt under NSIS, anbefales det at tage kontakt til Digitaliseringsstyrelsen i god tid inden anmeldelsen foretages med henblik på at aftale den nærmere proces samt åbne mulighed for at afklare evt. tvivlsspørgsmål, inden revisionserklæringer udarbejdes og anmeldelsen fremsendes. Derudover henvises til revisionserklæringen for yderligere detaljer og krav til erklæringens omfang, den anvendte revisionstandard mv.

Ved indsendelse af den årlige revisionserklæring, skal anmelder kontrollere, om der er ændringer i forhold til den oprindelige anmeldelse. Hvis dette er tilfældet, skal der indsender en opdateret anmeldelsesblanket baseret på den gældende anmeldelsesskabelon med tydelig angivelse af ændringerne i forhold til den oprindelige anmeldelse.

Hvis en anmeldt ID-tjeneste ophører, skal der udføres en afsluttende revision. Detaljerne er beskrevet i vejledningen til anmeldelses- og revisionsprocessen [REV].

5 Elektroniske identifikationsmidler associeret til juridiske enheder

Kapitlet omhandler identifikationsmidler for 'erhvervsbrugere', der i eIDAS-terminologi beskrives som elektroniske identifikationsmidler for fysiske personer associeret med en juridisk enhed. Begrebet 'erhvervsbrugere' dækker både medarbejdere ansat i en virksomhed, men også andre relationer, hvor der ikke foreligger et ansættelsesforhold. En associering mellem en person og en juridisk enhed kan typisk udmøntes på to forskellige måder:

a) Ved udstedelse af et nyt selvstændigt, Elektronisk Identifikationsmiddel som det fx kendes fra MitID Erhverv, hvor en Brugeradministrator i virksomheden kan foranledige, at der udstedes et nyt, særskilt MitID til erhvervsbrugeren.
b) Ved etablering af en *logisk forbindelse* gennem en registrering, der knytter en fysisk person til en juridisk enhed uden udstedelse af nye Elektroniske Identifikationsmidler (fx ved CVR- opmærkning af den fysiske person, hvor den fysiske person benytter sit personlige Elektronisk Identifikationsmiddel i erhvervsmæssig sammenhæng). Herved kan der skabes en ny, logisk erhvervsidentitet uden udstedelse af et nyt, fysisk Elektronisk Identifikationsmiddel. Dette princip anvendes fx i MitID-privat-til-Erhverv løsningen, hvor forbindelsen mellem CPR-nummer og CVR-nummer udspringer af CVR-registret.

5.1 Udstedelse af elektroniske identifikationsmidler

Der er ingen krav i dette afsnit og dermed heller ingen specifik vejledning.

5.2 Binding (associering) mellem Elektroniske Identifikationsmidler for fysiske og juridiske enheder

Niveau: Lav	Krav: 1) Det skal være muligt at suspendere og/eller ophæve en forbindelse for begge parter.
Vejledning: Kravet indebærer, at både den fysiske person og den juridiske enhed skal kunne suspendere og/eller nedlægge en erhvervsbruger fx via en selvbetjeningsløsning eller en service desk. For den juridiske enhed vil det typisk være en udpeget administrator, der kan suspendere eller nedlægge organisationens erhvervsbrugere, eller det kan ske ved synkronisering med et autoritativt kildesystem, der sikrer fjernelse af ophørte medarbejdere.	

Niveau: Lav	Krav:

	2) Den juridiske enhed har (typisk via en administrator) ret til at udføre suspendering eller ophævning, hvilket evt. kan indbefatte suspendering / spærring af et tilhørende Elektroniske Identifikationsmiddel, hvis forbindelsen er etableret herigennem.
Vejledning: En udpeget administrator skal udover at kunne suspendere og/eller nedlægge brugeridentiteter (punkt 1) kunne gøre det samme for Elektroniske Identifikationsmidler for en erhvervsbruger. Bemærk at dette ikke gælder for et personligt identifikationsmiddel (fx personligt MitID) koblet til en erhvervsbruger men alene identifikationsmidler udstedt i regi af en juridiske enhed (fx dedikeret/særskilt MitID udstedt til erhvervsbrugeren eller et medarbejdercertifikat som benyttes til autentifikation). Hvis et identifikationsmiddel er koblet til erhvervsbrugere i flere organisationer (for samme fysiske person), vil det være den organisation, som har foranlediget udstedelsen af identifikationsmidlet, som bør have adgang til at spærre og/eller suspendere dette.	

Niveau: Lav	Krav: 3) Det skal sikres, at forbindelsen fjernes, når associationen mellem den juridiske enhed og fysiske person ophører. Et eksempel kan være, at medarbejdere ikke længere er ansat eller ikke længere har et arbejdsbetinget behov for at være associeret, eller i tilfælde af den juridiske enheds konkurs eller likvidering.
Vejledning: Kravet går på vedligehold af erhvervsbrugere, specifikt at de nedlægges, når brugeren ikke længere har en relation til organisationen (fx ved afskedigelser og opsigelser), eller når en organisation ophører. I sidstnævnte tilfælde kan statusskift i CVR-registret anvendes som autoritativ kilde. Erhvervsbrugere bør først nedlægges, når en organisation endeligt ophører, mens 'mellem-tilstande' i CVR-registret som fx 'under konkurs', 'under likvidation', 'under tvangsopløsning', 'under reassumering' mv. ikke behøver resultere i at brugere nedlægges; her kan midlertidig suspension i stedet overvejes.	

Niveau: Lav	Krav: 5) Forbindelsen kan oprettes på grundlag af opslag i CVR-registret eller anden Autoritativ Kilde, herunder den juridiske enhed selv.
Vejledning: En organisation er naturligt autoritativ kilde for sine erhvervsbrugere og kan oprette og vedligeholde sine brugere enten manuelt (fx via en brugerflade) eller ved	

synkronisering med autoritative kildesystemer (fx HR-systemer, AD, IdM, brugerkataloger mv.). Desuden kan CVR-registret for visse virksomhedstyper indeholde registreringer af personer med tilknytning til en virksomhed som fx direktion, bestyrelse, fuldt ansvarlige deltagere mv. Det er tilladt at anvende flere autoritative kilder som grundlag for oprettelse af erhvervsbrugere, så længe der sikres konsistens. MitID Erhverv løsningen anvender begge modeller, hvor en brugerorganisation via brugerflade eller API kan oprette erhvervsbrugere, og hvor personer registreret i CVR til at kunne tegne en organisation fuldt ud har mulighed for at agere som erhvervsbrugere via MitID-privat-til-Erhverv løsningen.

Niveau: Lav, Betydelig, Høj	Krav: 4) Godtgørelse af identiteten af den fysiske person, der handler på vegne af den juridiske enhed, kontrolleres på Sikringsniveau »Lav« eller derover. 7) Sikringen af identiteten af den fysiske person, der handler på vegne af den juridiske enhed, foretages på Sikringsniveau »Betydelig« eller »Høj«. 12) Sikringen af identiteten af den fysiske person, der handler på vegne af den juridiske enhed, kontrolleres på Sikringsniveau »Høj«.
Vejledning: Kravene handler om at sikre identiteten af den fysiske person, der (senere) kobles til den juridiske enhed – med andre ord skal man vide, hvem personen er bag en medarbejderidentitet. Når der etableres en association mellem en juridisk enhed og en fysisk person, der er underlagt NSIS rammeværket, kan man bygge på den identitetssikring og udstedelsesproces, som gør sig gældende for den fysiske person og det tilhørende Elektronisk Identifikationsmiddel. Hvis man allerede har etableret, hvem den fysiske person er, og udstedt et Elektronisk Identifikationsmiddel til denne, kan man koncentrere sig om at sikre koblingen til den juridiske enhed – eksempelvis ved at sikre relationen mellem et CVR-nummer og CPR-nummer.	

Niveau: Lav	Krav: 6) Den fysiske person er ikke registreret af en Autoritativ Kilde med en status, der afholder den fysiske person fra at handle på vegne af den juridiske enhed.
Vejledning:	

Eksempler på relevante hændelser kan være, at en person er registreret som død eller med fuld fratagelse af den retlige handleevne i CPR-registret (under værgemål), og derfor ikke må have en aktiv erhvervsbruger.

Niveau: Betydelig	Krav: 8) Forbindelsen er etableret under kontrol af den juridiske enhed fx via en udpeget administrator eller via oplysninger fra en Autoritativ kilde.
Vejledning: Ofte vil der være administrative kontroller fra ID-tjenestens side, som forpligter den juridiske enhed (brugerorganisationen) gennem aftale til at vedligeholde sin erhvervsbrugere. Herved vil virksomhederne selv håndtere (og dermed kontrollere) associeringerne mellem virksomheden og fysiske personer, herunder om og hvornår der evt. skal udstedes Elektroniske Identifikationsmidler til disse. Typisk vil dette ske ved, at brugerorganisationens ledelse udpeger en administrator (fx en administrator i MitID Erhverv eller lignende), der på organisationens vegne vedligeholder erhvervsbrugere og deres Elektroniske Identifikationsmidler, eller ved at der skabes en integration mellem et autoritativt system hos virksomheden (fx HR-system, IdM-system eller tilsvarende) ligeledes udpeget af ledelsen, så erhvervsbrugere og Elektroniske Identifikationsmidler automatisk vedligeholdes. For visse virksomhedstyper kan der endvidere vedligeholdes erhvervsbrugere på baggrund af autoritative relationer mellem personer og virksomheder oplistet i CVR-registret som eksempelvis fuldt ansvarlige deltagere eller personer, der kan tegne et selskab alene.	

Niveau: Betydelig	Krav: 9) Procedurer til grund for etableringen af forbindelsen er underlagt revision.
Vejledning: De procedurer, der anvendes til oprettelse af erhvervsbrugere samt øvrig livscyklus for erhvervsbrugere, skal være beskrevne samt være underlagt revision. Dette indebærer, at de er dokumenterede og er underlagt versionering samt ændringskontrol, således at ændringer til procedurerne sker på en kontrolleret måde og med eksplicitte godkendelser. Procedurerne for brugeroprettelser skal naturligvis også efterleves i praksis, hvilket efprøves af revisionen. For en Lokal IdP skal procedurer være beskrevet for, hvorledes organisationens brugere oprettes med et givet NSIS sikringsniveau, herunder hvorledes arbejdsgange er udformet, hvem der har ansvaret for godkendelser i organisationen, hvilke kontroller der sker automatisk hhv. manuelt etc. Hvis der kan ske automatiske brugeroprettelser i en Lokal IdP ved at synkronisere med kildesystemer (fx	

HR-system eller IdM-systemer) er det vigtigt at sikre, at hele kæden er omfattet af relevante NSIS krav samt underlagt revision. En kæde er således ikke stærkere end det svageste led. For FullService IdP'er skal procedurer, der sikrer ansvarsfordelingen mellem FullService IdP og brugerorganisation, være beskrevet, herunder hvordan FullService IdP'en sikrer at brugeroprettelser sker under kontrol af brugerorganisationen, hvorledes administratorer autoriseres til at initiere brugeroprettelser, og hvorledes fysiske personer verificeres.

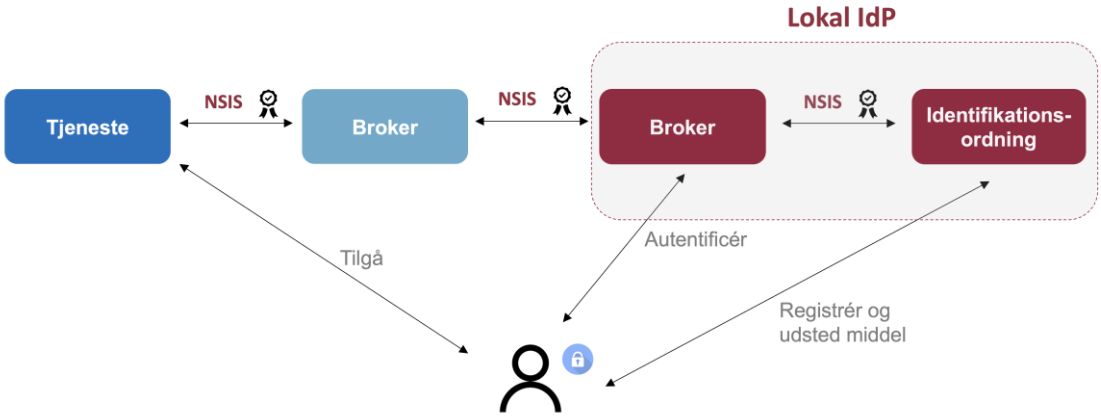
Niveau: Betydelig	Krav: 10) Forbindelsen er blevet kontrolleret på grundlag af et entydigt identifikationsnummer (fx CVR-nummer), der repræsenterer den juridiske enhed, og som bruges i dansk virksomhedsregistrering, og på grundlag af oplysninger, der entydigt repræsenterer den fysiske person, fra en Autoritativ kilde.
Vejledning: Kravet går på at sikre entydig identifikation af en erhvervsbrugers tilknytning til en juridisk enhed fx via et CVR-nummer – eller med andre ord at en erhvervsbruger altid kan henføres til et CVR-nummer. I dansk regi virker dette måske banalt, men ikke alle EU-lande har nødvendigvis en central virksomhedsregistrering med entydige identifikationsnumre.	

Niveau: Betydelig	Krav: 11) Den fysiske person og juridiske enhed notificeres om etablering af forbindelsen.
Vejledning: Kravet har til hensigt at sikre, at det er klart og transparent via en notifikation / kvittering, når en erhvervsbruger oprettes. Notificeringen kan vises som en integreret del af et selvbetjeningsforløb (fx bekræftelsesdialog) og/eller via afsendelse af fx mail, digital post meddelelse eller tilsvarende.	

6 Krav til Identitetsbrokere

Identitetsbrokere udgør en central del af den fællesoffentlige, danske infrastruktur, som i høj grad er opbygget efter en fødereret, løst-koblet model. Dette giver en lang række fordele i form af øget fleksibilitet og agilitet i infrastrukturen, og afkobler konsumenterne af en Identitet fra udstederen af et Elektronisk Identifikationsmiddel. Der henvises til den fællesoffentlige referencearkitektur for brugerstyring [REF-ARK] for yderligere beskrivelser og detaljer.

Indledningsvis er det relevant at præcisere, hvad der menes med en Identitetsbroker. I kontekst af NSIS menes en tjeneste, som *videreformidler en autentifikation til en tredjepart* ved at udstede og signere et såkaldt Security Token (en 'autentifikationsbillet') for en elektronisk Identitet. En broker udstiller med andre ord en autentifikationsservice og indgår dermed i den 'tillidskæde', som (eksterne) tjenester ('relying parties') af en autentifikation skal stole på.



Figur 1: Eksempel på tillidskæde

I nogen sammenhænge går brokere under de tekniske betegnelser 'Identity Providers' eller 'Security Token Services'[14], og der findes en række internationale standarder (visse med tilhørende danske profiler), som regulerer deres snitflader som fx SAML, WS-Trust og OpenID Connect. Et konkret eksempel er NemLog-in løsningen, der udsteder SAML Assertions til offentlige tjenesteudbydere, når borgere eller medarbejdere tilgår tjenesten. Det er med andre ord attributterne i SAML Assertion, der beskriver den elektroniske Identitet, og tjenesten ser herved ikke det bagvedliggende Elektronisk Identifikationsmiddel, der blev anvendt af brugeren, men kun attributter for den resulterende brugeridentitet og et tilhørende Sikringsniveau.

Da Identiteter i en fødereret model i praksis leveres gennem en kæde med flere led, og da de fleste danske tjenester forventes at være koblet til en Identitetsbroker

[14] En Identity Provider er en "aktiv" tjeneste med en brugerflade, som slutbrugerne kan interagere med (autentifikation), mens en Security Token Service er en "passiv" tjeneste, som kun udstiller et API for udstedelse af security tokens.

frem for selv at forestå brugerautentifikation, er det relevant at regulere Sikringsniveauer på tværs af hele tillidskæden frem for kun at se på autentifikationen i første led (som dækket i de første kapitler).

En Identitetsbroker vil, når den påtrykker et NSIS Sikringsniveau i en udstedt autentifikationsbillet (security token), skulle forholde sig til både sit eget Sikringsniveau samt niveauet af Autentifikationen, der er sket på baggrund af Elektroniske Identifikationsmidler. Brokeren skal med andre ord indestå for, at det sikringsniveau, der påtrykkes i en udstedt autentifikationsbillet, også er korrekt og lever op til NSIS. Beregningen af det aktuelle sikringsniveau sker med andre ord dynamisk.

Identitetsbrokere kan omveksle og berige autentifikationsbilletter med yderligere informationer – og sættes sammen i flere led (en kæde). Her dækker NSIS kun selve brugerautentifikationens styrke gennem et defineret Sikringsniveau, mens kvaliteten af øvrige attributter (fx roller, rettigheder, autorisationer eller fuldmagter for brugeren) kan reguleres af andre rammeværk. I definitionen af en Identitetsbroker som en part, der videreformidler Identitet, er det underforstået "til tredjepart" – dvs. en intern omdannelse af en autentifikation til et andet teknisk format (fx etablering af en browser cookie i en session eller dannelse af en nøgle til et API, som kan tilgå en given brugerkontekst) betragtes ikke som videreformidling og dermed ikke underlagt krav til Identitetsbrokere. Endvidere vil system-kald (API-kald), hvor data fx hentes for en bestemt bruger, ikke falde under krav til Identitetsbrokere, når kalderen blot medsender brugeridentiteten som parameter og ikke udsteder et token via en autentifikationsservice, som modtageren stoler på. Dette gælder med andre ord alene, når det kaldende system ikke er en del af tillidskæden men blot agerer som tjenesteudbyder og fx henter data om en identitet via services i Datafordeleren eller et myndighedsregister.

Niveau: Lav	Krav: 1) Security tokens må kun udstedes umiddelbart efter a) forudgående, succesfuld autentifikation, b) på baggrund af en gyldig, autentificeret session (Single Sign-On), eller c) ved omveksling af et gyldigt security token fra en anden Identitetsbroker, der er etableret et tillidsforhold til. 2) Det aktuelle Sikringsniveau skal angives som en oplysning i det udstedte token (LoA), således at modtageren af tokens direkte kan aflæse dette. Sikringsniveauet i et token opgøres som mindsteværdien af Sikringsniveauet for Autentifikationen (jf. afsnit 2-5), brokerens eget Sikringsniveau (FAL) jf. afsnit 4 og 6, samt Sikringsniveauerne for evt. Identitetsbrokere, der er benyttet som underleverandører i den konkrete Autentifikation. Det er dermed det laveste Sikringsniveau i autentifikationskæden, som bliver det resulterende Sikringsniveau.
Vejledning: Krav 1) og 2) til Identitetsbrokere har til hensigt at regulere formidling af Sikringsniveauer på tværs af en kæde. Her er der flere hensyn:	

- Viden om Sikringsniveauet skal formidles eksplicit gennem kæden.
- Det svageste led i kæden afgør Sikringsniveauet. Hvis en Identitetsbroker eksempelvis har et lavere Sikringsniveau end de tidligere Sikringsniveauer i kæden (fx hvis brugeren autentificerede sig på niveau Høj, mens brokeren kun lever op til niveau Lav), da nedgraderes Sikringsniveauet for brokerens udstedte token til det lave niveau (i eksemplet niveau Lav).

Det er tilladt for en identitetsbroker at angive et NSIS sikringsniveau til en tjenesteudbyder på baggrund af en autentifikation på tilsvarende eIDAS sikringsniveau, såfremt identitetsbrokeren har en forudgående accept fra tjenesteudbyderen af denne konvertering. Eksempelvis kan en autentifikation på eIDAS Betydelig konverteres til NSIS sikringsniveau Betydelig med tjenesteudbyderens forudgående accept. Hensynet til dette er, at mange danske tjenesteudbydere i praksis ikke forventes at ville skelne mellem sikringsniveauer for eIDAS hhv. NSIS på samme niveau (og i mange situationer heller ikke vil have lovhjemmel til det jævnfør eIDAS forordningens artikel 6.1.b).

Hvis en identitetsbroker omveksler et token og i processen selv beriger dette token med yderligere Personidentifikationsdata eller andre attributter, skal dette være klart beskrevet for de tjenester, der anvender brokeren, så de kan fortolke tokenet ud fra korrekte forudsætninger. Eksempelvis kunne en identitetsbroker berige et token med et CPR-nummer, hvis der ikke fremgår et CPR-nummer i det indgående token, således at den modtagende tjeneste lettere kan identificere brugeren. Her skal det være klart for tjenesten, om det i tokenet angivne NSIS sikringsniveau angår alle attributter (fx fornavn, efternavn, fødselsdato) herunder det tilføjede CPR-nummer. Dette er særligt vigtigt, hvis de tilføjede attributter er Personidentifikationsdata, som tjenesten lægger til grund for entydig identifikation af brugeren. I det beskrevne tilfælde kan det evt. være relevant at angive en separat 'koblingsstyrke' for CPR-nummeret, hvis sikkerheden for dette afviger fra eller har en anden oprindelse end de øvrige attributter i tokenet. Alternativt kan brokeren evt. nedklassificere det oplyste NSIS sikringsniveau i tokenet til minimumsværdien, der gælder på tværs af alle Personidentifikationsdata i tokenet, således at den modtagende tjeneste ikke skal forholde sig til kompleksiteten forbundet med multiple sikringsniveauer.

Niveau: Lav	Krav: 4) Brokerens private nøgle, der underskriver security tokens, skal beskyttes mod uautoriseret adgang.
Vejledning Den private nøgle, der kan underskrive security tokens, er afgørende at beskytte mod uautoriseret adgang. Ved uautoriseret adgang kan en angriber potentielt underskrive sine egne adgangsbilletter og dermed kunne impersonere alle brugere over for tjenesteudbydere tilsluttet brokeren. På sikringsniveau lav er det tilstrækkeligt at beskytte nøglen med kryptering (fx krypterede nøglefiler) og almindelig	

fysisk og logisk adgangskontrol, så kun autoriserede processer kan anvende nøglen, mens der på højere sikringsniveauer kan være skærpede krav eksempelvis i form af dedikeret hardware.

Niveau: Lav	Krav: 5) Sessioner med Identitetsbrokere skal have en begrænset levetid (automatisk udløb), og det skal være muligt for brugeren at logge ud af alle sessioner på én gang (single logout).
Vejledning NSIS stiller ikke detailkrav til levetid af tokens og sessioner (sessionscookies) der etableres med brugeres browser, og disse bør derfor fastlægges ud fra en konkret risikovurdering. Generelt anbefales security tokens (SAML eller JWT), der sendes fra en Identitetsbroker (IdP) til en tjeneste som svar på en autentifikationsforespørgsel, at have en levetid, der er begrænset til få minutter (fx 5-10 min). Dette minimerer vinduet, hvor tokens kan opsnappes og bruges uretmæssigt til fx at impersonere brugeren. Derudover er der spørgsmålet om levetid af brugersessionen i brugerens browser, som evt. oprettes af Identitetsbrokeren som grundlag for Single Sign-On med samme browser til andre tjenester. Her anbefales en levetid for brugersessioner på maksimalt 60 minutter. Dertil kommer, at en tjeneste gennem SAML- og OIDC-protokollerne altid kan anmode en Identity Provider om en frisk brugerautentifikation uden mulighed for Single Sign-On (i SAML ved at sætte ForceAuth flaget på sit request) i tilfælde af, at brugeren tilgår en særlig følsom ressource eller handling, som efter tjenestens opfattelse forudsætter genvalidering af brugeren, eller såfremt tjenesten af andre grunde ønsker at få genbekræftet, at der stadig er samme bruger, der sidder ved tasterne i den anden ende.	

Niveau: Lav	Krav: 6) Sessioner med Identitetsbrokere skal beskyttes mod overtagelse.
Vejledning Ofte vil en Identitetsbroker implementere sessioner med brugerne som grundlag for Single Sign-On (SSO), og herefter knytte et sikringsniveau til sessionen, som evt. senere kan hæves med en såkaldt step-up autentifikation. En udbredt teknik kendt fra implementeringer af SAML Identity Providere er at anvende *session cookies* i brugeres browser, og hvis disse kan overtages, kan angriberen herved impersonere brugeren. Det er derfor relevant at beskytte disse cookies eksempelvis ved at sætte egenskaber på dem som sikrer, at de ikke sendes over ukrypterede forbindelser, at de ikke kan tilgås fra JavaScript (med mindre dette er nødvendigt for løsningens virkemåde), at de naturligt udløber efter en given periode og ikke kan tilgås af uvedkommende. Det er med andre ord relevant at se på cookie-egenskaberne *Secure*, *HttpOnly* og *SameSite*. Endvidere kan man overveje at	

binde en cookie til en bestemt IP-adresse på serveren, så en stjålen cookie ikke kan anvendes fra en anden enhed end den, hvor sessionen blev initieret fra.

Niveau: Lav	Krav: 7) Alle forespørgsler til Identitetsbrokeren og alle svar på disse skal skrives til en integritetsbeskyttet log.
Vejledning Med henblik på at kunne spore hændelsesforløb gennem kæder med flere Identitetsbrokere, skal en broker etablere logs med tilstrækkelig korreleringsinformation. I NSIS formuleres i krav 7, at alle forespørgsler og svar skal skrives til en integritetsbeskyttet log, og disse forespørgsler og svarmeddelelser bør forsynes med en unik identifier (som fx i request ID i SAML). Det kan også være god praksis at videresende egne korreleringsID'er ved kald videre i kæden. Såfremt en Identitetsbroker logger sammenhængen mellem en indgående forespørgsel og en relateret udgående forespørgsel for samme transaktion, vil den ønskede sporbarhed på tværs være etableret. Det kan ligeledes være en god praksis at sikre, at Identitetsbrokere anvender præcise tidsstempler i deres logs gennem synkronisering med en pålidelig tidskilde. Loggens troværdighed (integritet) skal beskyttes mod uautoriserede tilføjelser, sletninger eller modifikationer, hvilket i praksis kan ske både med kryptografiske mekanismer og/eller fysisk- samt logisk adgangskontrol samt overvågning. Almindeligt driftspersonale bør således ikke have adgang til at kunne manipulere loggen, og det bør være en betroet rolle (sikkerhedsadministrator eller tilsvarende) at konfigurere og administrere log-systemet. Administrative handlinger ift. loggen bør efterlade sig et audit-trail, som kan inspiceres for at afdække forsøg på manipulation. Der er ikke krav om 24/7 pro-aktiv overvågning af loggen.	

Niveau: Betydelig	Krav: 10) Tokens, som indeholder fortrolige eller følsomme personoplysninger, og transporteres via brugerens browser, skal end-to-end krypteres eller krypteres på attributniveau, således at indholdet kun er læsbart for modtageren.
Vejledning I mange føderationsprotokoller findes der såkaldte '*front channel bindings*', hvor security tokens transporteres via brugerens browser mellem udsteder (fx SAML Identity Provider / Identity Broker) og forretningstjeneste (fx SAML Service Provider). Dette gælder eksempelvis SAML HTTP Redirect Binding og SAML HTTP POST binding samt OAuth ved brug af *Implicit Grant*. Selv om transportkanalen er beskyttet med TLS, kan der her være en risiko for, at indholdet af tokens kan op-	

snappes af uvedkommende, der har kompromitteret brugerens browser eller platform. Endelig er der tidligere set en del sårbarheder og angreb på transportprotokoller (fx POODLE angrebet), og her giver kryptering på meddelelsesniveau et ekstra lag af beskyttelse.

Det skal her bemærkes, at security tokens normalt er digitalt signerede, hvorfor risikoen for manipulering (integritet) må betragtes som særdeles lille, hvis der anvendes anerkendte algoritmer og nøglelængder.

I mange situationer vil security tokens i sig selv ikke indeholde fortrolige eller følsomme oplysninger, og derfor kan transportbeskyttelse være acceptabel ud fra en konkret risikovurdering. Hvis brugerens browser er kompromitteret, vil der alligevel være sandsynlighed for datalæk, når forretningstjenesten præsenterer data lige efter autentifikationen.

Hvis security tokens omvendt indeholder fortrolige eller følsomme oplysninger (herunder følsomme personoplysninger jævnfør [GDPR] artikel 9), og der samtidig kommunikeres via brugerens browser, stiller NSIS krav til kryptering på meddelelseslaget af security tokens eller attributter, hvilket dækker hele vejen fra Identitetsbroker til forretningstjeneste. Et eksempel på dette er anvendelse af XML-kryptering i SAML-standarden til at kryptere hele Assertion (EncryptedAssertion) eller udvalgte attributter (EncryptedAttribute).

Niveau: Høj	Krav: 13) Brokerens private nøgle, der underskriver security tokens, placeres i "tamper-resistent" kryptografisk hardware, der opfylder kravene til FIPS 140-2 level 3 eller tilsvarende.
Vejledning På niveau Høj henvises til anerkendte standarder for kryptografiske enheder (fx FIPS 140-2, Common Criteria eller lignende), der beskriver en række specifikke sikkerhedskrav, og som producenter kan få certificeret deres enheder efter. Det samme gælder på niveau Betydelig for nationale tjenester som fx NemLog-in, hvilket skal forstås som tjenester, som udsteder Elektroniske Identifikationsmidler til private borgere eller personer associeret til vilkårlige virksomheder. I kravet til HSM på niveau Høj er det således underforstået, at der benyttes en kryptografisk enhed, der er certificeret efter en anerkendt standard for kryptografiske enheder. Hensynet bag dette er, at kompromittering af den private nøgle for en broker ofte kan få fatale konsekvenser for samtlige brugere og tjenesteudbydere.	

7 Governance

Der er ikke pt. vejledning til dette kapitel.

8 Referencer

[DBL] ”Databeskyttelsesloven”, Justitsministeriet. https://www.retsinformation.dk/Forms/R0710.aspx?id=201319

[DS-471] "DS 471:1993 - Teknisk forebyggelse af indbrudskriminalitet".

[eIDAS] "EU's forordning nr. 910/2014 om elektronisk identifikation og tillidstjenester til brug for elektroniske transaktioner på det indre marked og om ophævelse af direktiv 1999/93/EF".

[ENISA] "Technical guideline for Incident Reporting" https://www.enisa.europa.eu/publications/technical-guideline-for-incident-reporting

[FIPS 140-2] “FIPS PUB 140-2, Security Requirements for Cryptographic Modules”, NIST. https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.140-2.pdf

[GDPR] "Europa-Parlamentets og Rådets forordning (EU) 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger og om ophævelse af direktiv 95/46/EF (generel forordning om databeskyttelse)".

[ISO15408] “ISO/IEC 15408-1:2009 “Information technology – Security techniques – Evaluation criteria for IT security” og ISO/IEC 18045 “Information technology – Security techniques – Methodology for IT security evaluation”.

[ISO 27001] “ISO/IEC 27001:2013 - Information technology -- Security techniques -- Information security management systems -- Requirements”.

[ISO29115] "ISO/IEC 29115:2013 Information technology -- Security techniques -- Entity authentication assurance framework”. https://www.iso.org/standard/45138.html

[LOA] ”KOMMISSIONENS GENNEMFØRELSESFORORDNING (EU) 2015/1502 af 8. september 2015 om fastlæggelse af tekniske minimumsspecifikationer og procedurer for fastsættelse af Sikringsniveauer for elektroniske identifikationsmidler i henhold til artikel 8, stk. 3, i Europa- Parlamentets og Rådets forordning (EU) nr. 910/2014 om elektronisk identifikation og tillidstjenester til brug for elektroniske transaktioner på det indre marked".

[NIST] “NIST Special Publication 800-63 Revision 3”, NIST. https://pages.nist.gov/800-63-3/sp800-63-3.html

[REF-ARK] "Referencearkitektur for brugerstyring", Digitaliseringsstyrelsen.

https://arkitektur.digst.dk/rammearkitektur/referencearkitekturer/referencearkitektur-brugerstyring

[TU-LoA] ”Vejledning til valg af NSIS Sikringsniveau for tjenesteudbydere - version 2.0.2", Digitaliseringsstyrelsen. https://digst.dk/it-loesninger/standarder/nsis/

[REV] ”Anmeldelses- og revisionsproces, National Standard for Identiteters Sikringsniveauer, version 1.0”, Digitaliseringsstyrelsen. https://digst.dk/it-loesninger/standarder/nsis/ (tidligere titel var ’revisionsvejledning’)