DIGITALISERINGSSTYRELSEN

Vejledning til National Standard for Identiteters Sikringsniveauer (NSIS)

Status: Version 2.1

Version: 14.09.2020

1 Indledning

1.1 Forord

Dette dokument indeholder vejledning til version 2.0.1 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 høringsprocessen eller på anden måde har vist behov for uddybning og forklaring.

EU-kommissionen har ligeledes udgivet et vejledningsdokument[2] til gennemførelsesforordningen om Sikringsniveauer, som kan være en hjælp til at forstå [eIDAS]-forordningen, som NSIS bygger på. Hovedfokus i nærværende vejledning er derfor på lokale, danske forhold, og på udvidelserne i forhold til [eIDAS], således at overlap med kommissionens vejledning [LOA-GUID] kan minimeres.

1.2 Forskelle på eIDAS og NSIS

I forbindelse med den offentlige høring af NSIS viste det 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

[1] På engelsk: "outcome based".

[2] "Guidance for the application of the levels of assurance which support the eIDAS Regulation",[LOA-GUID].

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.

Område	eIDAS	NSIS
Anmelder	Medlemsland	Udbyder (fx privat part)
Kustode	EU Kommissionen	Digitaliseringsstyrelsen
Formål	Grænseoverskridende transaktioner[3]	Nationale og lokale transaktioner
Ansvarlig for fejl	Medlemslandet (anmelder)	Anmelderen
Verifikation af krav	Peer-review proces mellem medlemslande (inkl. relevante erklæringer[4])	Selvdeklarering (niveau Lav) Revisions- og 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 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.

1.3 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.

[3] Inden for EU/EØS.

[4] 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, 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.

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 CVR-registrene. 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 [JM-SAM].

3.1.2 Verifikation af Identitet (fysiske personer)

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.	

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. Når dette ikke er muligt, kommer anden del af kravet i spil: "Hvor ansøgeren ikke er i[5] 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).	

[5] "i" mangler i NSIS 2.0.1

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.

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.

Uden brug af pas:

Som nævnt under krav 4) er det vigtigt at være opmærksom på, at alternative legitimationsdokumenter end pas 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[6] med en række eksempler på indhentning og kontrol af identitetsoplysninger, som kan være relevante at overveje.

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.

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.

CPR-opslag:

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

Derudover bør der så vidt muligt foretages kontrolopslag mod CPR, og ved fremsendelse af fysiske Elektroniske Identifikationsmidler (fx nøglekort) bør folkeregisteradressen[7] for den påståede identitet slås op og benyttes for at modvirke identitetstyveri.

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, 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.	

[7] Dette hører strengt taget til under leverings- og aktiveringsprocesser, men bidrager under alle omstændigheder til, at det bliver vanskeligere at få udstedt et Elektronisk Identifikationsmiddel knyttet til en anden persons identitet.

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)

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 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:

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, hvilket kan danne grundlag for en automatiseret verifikation af autorisationen. For virksomhedsformer uden persontilknytning i CVR (fx fonde og 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 generalforsamling 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.

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 dette fremgår af CVR-registret for 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 NemID NøgleApp'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[8], 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.

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

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 indehaverbaseret eller iboende Autentifikationsfaktor.	

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

På niveau Høj kræves en meget stor resistens - selv mod angribere med høj angrebskapacitet. Som et simpelt eksempel kan nævnes, at et papirbaseret NemID nøglekort kan kopieres/fotograferes, uden at dette kan ses (fx hvis indehaveren efterlader kortet i sin jakke/taske), og derfor kræver et angreb kun et mindre '*window of opportunity*' men ingen særlig teknisk viden eller hardware/software. Derimod kan en fysisk chip med en kryptografisk nøgle designes, så den i praksis er særdeles vanskelig at kompromittere, hvorfor et angreb kan kræve specialistviden, speciel hardware og lang tid.

I relation til punkt 6) kan nævnes, at der for kryptografiske enheder findes en række standarder (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 disse anerkendte standarder vil generelt være en 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 af Elektroniske Identifikationsmidler til 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. Ofte kombineres udleveringen på niveau Betydelig og Høj 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).

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).
- 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.
- 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 NemID / 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 også 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: Vedr. punkt 4) skal man på niveau Høj kunne modstå insiderangreb, så en enkeltstående, ondsindet administrator hos udstederen ikke på egen hånd kan få udstedt eller tiltage sig et fungerende Elektronisk Identifikationsmiddel i en andens navn – fx implementeret gennem funktionsadskillelse etc.	

3.2.3 Suspendering, spærring og genaktivering

Niveau: Lav	Krav: 1) Det skal være muligt for 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[9] 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	

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

udgive en spærreliste for PKI-baserede Elektroniske Identifikationsmidler eller ved at markere en central brugerkonto 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.	

Niveau: Lav	Krav: 4) Udstederen af et Elektronisk Identifikationsmiddel, skal på eget initiativ spærre et Elektronisk Identifikationsmiddel: o hvis der er mistanke om kompromittering eller tab af kontrol over dette, o hvis der konstateres fejl i det Elektroniske Identifikationsmiddel (fx forkerte data), o hvis der ikke længere foreligger en gyldig aftale[10] mellem udsteder og ansøger, eller
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. 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, men disse aspekter bør indtænkes i udformningen af Elektroniske Identifikationsordninger.	

3.2.4 Fornyelse og erstatning

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

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 under 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 skal blot kende den fysiske Identitet bag et Elektronisk Identifikationsmiddel i forbindelse med udstedelsen samt have en separat log af denne.	

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 Angrebskapaci-

	tet at gætte, lytte sig til, gengive eller manipulere kommunikationen og på den måde omgå autentifikationsmekanismen.
Vejledning: 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. 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.	

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 skal for så vidt angår ID-tjenesten til enhver tid kunne dokumentere overholdelse af 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.	

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.	

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 forsikringsordninger. Dokumentation for disse skal vedlægges anmeldelsen.	

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, som beskriver alle relevante betingelser, betalinger for og begrænsninger i brugen af servicen. Servicebeskrivelsen skal indeholde en privatlivspolitik, som opfylder kravene i [GDPR].
Vejledning: 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.	

4.1.3 Informationssikkerhedsledelse

Niveau: Betydelig	Krav: 2) Ledelsessystemet 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.

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, statsautoriseret 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.	

4.1.4 Dokumentation og registerføring

Niveau: Lav	Krav: 1) Relevant information skal arkiveres 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. Af øvrige områder kan nævnes administratorer, sikkerhedspersonale, auditorer og andre, som udfører betroede funktioner. For underleverandører kan der etableres aftaler, revision eller andre mekanismer, der sikrer opfyldelse af kravet for deres område.	

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), peridisk gennemgang af logs med administratorhandlinger etc.	

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 konfidentialitet, integritet og tilgængelighed. Med begrebet 'rimelige tekniske kontroller' i NSIS refereres til, at kontrollerne skal nedbringe risici for tab af konfidentialitet, 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. 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 forretningstjenester, der kan opnås adgang til. Da Elektroniske Identifikationsordninger sjældent behandler følsomme personoplysninger (i sig selv), er konsekvenserne ved tab af konfidentialitet 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 mulighedere 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'.	

4.1.7 Anmeldelse og revision

Elektroniske Identifikationsordninger og Identitetsbrokere skal underlægges periodevis intern og/eller ekstern revision. Ved anmeldelse af løsninger på Sikringsniveau Betydelig og Høj, skal der indgå en revisorerklæring udarbejdet efter den revisionsvejledning med tilhørende Excel-skema, som Digitaliseringsstyrelsen har udarbejdet (se link i NSIS standarden). 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.

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.

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) Der skal etableres periodevis intern revision, som omfatter alle nødvendige områder af de tilbudte tjenester med henblik på at sikre overholdelse af relevante krav og politikker.
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. Det er obligatorisk at anvende de udarbejdede skabeloner for anmeldelse og revision.	

Niveau: Betydelig	Krav: 4) Ved anmeldelse på niveau Betydelig anvendes selvdeklarering suppleret med en revisionserklæring fra en uafhængig statsautoriseret revisor eller et overensstemmelsesvurderingsorgan (jf. [eIDAS] artikel 3, stk. 1, nr. 18), som bekræfter, 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 forudsætter dog, at kravene i denne standard indgår i det gennemførte audit og revision.

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.

Det er vigtigt at designe løsninger og kontrolprocesser, så der dannes et revisionsspor, 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.

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.

5 Elektroniske identifikationsmidler associeret til juridiske enheder

Kapitlet omhandler krav til elektroniske identifikationsmidler for fysiske personer associeret med en juridisk enhed. Associationen dækker både medarbejdere ansat i en virksomhed, men også andre relationer, hvor der ikke foreligger et ansættelsesforhold. En associering kan typisk udmøntes på to forskellige måder:

a) Ved udstedelse af et nyt selvstændigt, Elektronisk Identifikationsmiddel som det fx kendes fra OCES Medarbejdercertifikater, hvor en NemID Administrator i virksomheden kan foranledige, at der udstedes et nyt Elektronisk Identifikationsmiddel.
b) Ved etablering af en *logisk forbindelse*, 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.

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, 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: 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: Betydeligt	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 gennem aftale til at vedligeholde egne forbindelser (fx til medarbejdere). Herved vil virksomhederne selv håndtere (og dermed kontrollere) associeringerne mellem virksomheden og fysiske personer, herunder om og hvornår der evt. skal udstedes Elektroniske Identifikationsmidler, som understøtter forbindelsen. Typisk vil dette ske ved, at virksomhedens ledelse udpeger en administrator (fx en NemID-administrator eller lignende), der på virksomhedens vegne vedligeholder forbindelser og 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 forbindelser og Elektroniske Identifikationsmidler automatisk vedligeholdes. For visse virksomhedstyper kan der endvidere vedligeholdes associeringer 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.	

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 'billet') for en elektronisk Identitet. Disse benævnes i nogen sammenhænge for 'Identity Providers' eller 'Security Token Services'[11], 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 men kun attributter og et formidlet 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 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 et udstedt 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 et udstedt token, også er korrekt og lever op til NSIS. Beregningen af det aktuelle sikringsniveau sker med andre ord dynamisk.

Identitetsbrokere kan omveksle og berige security tokens 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.

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

[11] 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.

	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).	

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, og disse bør derfor fastlægges ud fra en konkret risikovurdering. Generelt anbefales tokens for aktive scenarier (fx en bruger som anvender en Identity Provider) at være begrænset til få minutter (fx 5-10 min). Derudover er der spørgsmålet om levetid af brugersessionen, som oprettes på baggrund af tokenet, og her anbefaler Digitaliseringsstyrelsen pt. en levetid for bruger*sessioner* på 30 minutter hos tjenester og 60 minutter for Identity Provideren. Dertil kommer, at en tjeneste gennem SAML protokollen altid kan anmode en Identity Provider om en frisk brugerautentifikation uden mulighed for Single Sign-On (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 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 session 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 korrelering-sID'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.	

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 opsnappes af uvedkommende, der har kompromitteret brugerens browser eller platform. Endelig er der i senere år 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
[JM-SAM]	”Vejledning om Samtykke”, Datatilsynet og Justitsministeriet, September 2019. https://www.datatilsynet.dk/media/6562/samtykke.pdf
[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".

[LOA-GUID] ”Guidance for the application of the levels of assurance which support the eIDAS Regulation". https://ec.europa.eu/cefdigital/wiki/download/attachments/40044784/Guidance%20on%20Levels%20of%20Assurance.docx

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

[NSI] ”Fællesoffentlige brugerstyringsløsninger - en analyse af sikkerhedsstandarder og -løsninger”, NSI.

[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/media/21945/vejledning-til-valg-af-sikringsniveau-for-tjenesteudbydere-202.pdf