DIGITALISERINGSSTYRELSEN

Vejledning til National Standard for Identiteters Sikringsniveauer (NSIS)

Status: Version 2.0

Version: 26.06.2018

1 Indledning

1.1 Forord

Dette dokument indeholder vejledning til 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 åbenhed og fleksibilitet for løsningerne.

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 rammeværk sat op mod hinanden i tabellen nedenfor.

Formålet med sikringsniveauerne i [eIDAS] er således at definere krav til nationale elektroniske identifikationsordninger[3], der anmeldes af det enkelte medlemsland til kommissionen med henblik på gensidig anerkendelse i grænseoverskridende transaktioner. Verifikation af kravene 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*).

---

[1] På engelsk: "outcome based".

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

[3] I [eIDAS] dokumenterne benævnes dette også som eID skema.

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.

Område	eIDAS	NSIS
Anmelder	Medlemsland	Udbyder (fx privat part)
Kustode	EU Kommissionen	Digitaliseringsstyrelsen
Formål	Grænseoverskridende transaktioner[4]	Nationale og lokale transaktioner
Ansvarlig for fejl	Medlemslandet	Anmelderen
Verifikation af krav	Peer-review proces mellem medlemslande	Revisions- og ledelseserklæring
Brugerpopulationer	Store (hele befolkning bør kunne dækkes 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 kravsopfyldelsen. 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.

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.

For læsere, der er bekendt med den amerikanske NIST 800-63 standard er det relevant at bemærke, at begrebet 'Akkreditiv' 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 et eller flere Akkreditiver ('Authenticators').

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

[4] Inden for EU/EØS.

2 Livscyklus for Akkreditiver

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 Akkreditiver, herunder sammenhænge og ansvarsområder.

3 Normative krav

Dette kapitel indeholder vejledning til kravene relateret til udstedelse og anvendelse af Akkreditiver. Da kravene som sagt går på forskellige trin i livscyklussen, vil ikke alle krav være relevante for alle typer tjenester. I forbindelse med anmeldelse er det derfor vigtigt som det første at gøre sig klart, hvilke dele af NSIS, der er relevant at opfylde.

Der forventes to arketypiske anmeldelser, men rammeværket er åbent for andre varianter:

a) Udstedere af Akkreditiver.
b) Identitetsbrokere.

En udsteder af Akkrediver kan typisk benytte sig af eksterne parter eller underleverandører i forbindelse med verifikation af brugernes identitet (*identity proofing*). I den forbindelse må udstederen i forbindelse med sin anmeldelse redegøre for dette underleverandørforhold - herunder hvorledes de samlede krav til udstedelse er overholdt fx ved at inddrage relevant dokumentation fra de eksterne parter, relevante aftaler mellem parterne etc.

Tilsvarende vil en Identitetsbroker, når den påtrykker et NSIS niveau i et udstedt security token, skulle forholde sig til både sit eget sikringsniveau samt niveauet af Autentifikationen, der er sket på baggrund af Akkreditiver. Hvis det pågældende Akkreditiv er anmeldt under NSIS, er dette naturligvis enkelt at fastslå, idet brokeren så blot kan forlade sig på det publicerede sikringsniveau, og ellers må der foretages en fuld vurdering mod NSIS kravene.

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, 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.

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 om afkrydsning af 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 for brugeren. Anmeldere bør endvidere overveje, hvordan man over for en revisor vil dokumentere brugerens accept ved fx at indrette systemet med relevante logninger.	

3.1.2 Verifikation af identitet (fysiske personer)

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 fremlagte beviser kan være blevet tabt, stjålet, suspenderet, tilbagekaldt eller være udløbet. Ansøgeren eksisterer i autoritative registre (fx CPR) og er ikke markeret som død eller forsvundet.

Vejledning:

Kravene på niveau Betydelig er udformet, så det er muligt at foretage verifikationsprocessen on-line (dvs. uden fysisk fremmøde fra ansøgeren). Dette giver mulighed for både kost-effektive og brugervenlige processer, men som det fremgår af kravene, skal man her nedbringe risikoen for anvendelse af tabte eller stjålne beviser. Som eksempel på foranstaltninger kan her nævnes, at pas/kørekort kan tjekkes for spærring i centrale registre, således at risikoen for anvendelse af stjålne/tabte dokumenter mindskes, samt at løsningen fremsender fysiske Akkreditiver (fx nøglekort) til folkeregisteradressen[5] for den påståede identitet for at modvirke indrullering af anden person.

Et andet eksempel på en kontrol, der kan modvirke anvendelse af tabt/stjålet/forfalsket dokumentation, er kontrolspørgsmål. Mulighederne 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, mens man ved fysisk fremmøde vil få vanskeligere ved at svare korrekt.

Anmeldere bør endvidere overveje, hvordan man over for en revisor vil dokumentere, at de planlagte kontroller faktisk er udført.

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. Sammenligningen kan eksempelvis tage ud-

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

gangspunkt i et billede på et pas eller kørekort og/eller kontrol af en frisk underskrift udført af personen mod et tidligere etableret underskriftseksempel fra fx pas eller kørekort. Hensigten med dette er at etablere høj sikkerhed for, at det er ansøgeren selv og ikke fx en *man-in-the-middle*, som videreformidlere foto eller underskrift fra en anden person. I mange sammenhænge vil kontrol af fysiske kendetegn på et højt sikringsniveau 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 opfanger de biometriske data, og det sted, hvor de biometriske data verificeres.

Endelig kan det nævnes, at NSIS gør det muligt at udstede nye Akkreditiver på baggrund af en autentifikation med et andet, gyldigt Akkreditiv, der opfylder kravene på mindst samme NSIS sikringsniveau. Et eksempel på dette kunne være, at man ved udstedelse af et Akkreditiv til erhvervsbrug lader brugeren autentificere sig med et Akkreditiv udstedt til brugeren i egenskab af borger. Herved behøver man ikke på ny foretage identitetssikring af den fysiske person men kan koncentrere sig om at verificere tilknytningen til den juridiske person samt evt. udstedelse af et nyt Akkreditiv. Dette betyder, at der kan etableres mere smidige løsninger, og brugerne undgår potentielt at skulle stille op til flere, identiske indrulleringsprocesser. Dette princip åbner dog i teorien for, at en fejl eller svaghed hos én Akkreditivudsteder kan udnyttes til at få udstedt andre, falske Akkreditiver - dette vurderes dog som mindre sandsynligt på niveau Betydelig og Høj, hvor kravene til tekniske kontroller, procedurer og revisionserklæringer er høje.

3.1.3 Verifikation af Identitet (juridiske personer)

Niveau: Lav	Krav: 4) Det kan antages, at registreringen gennemføres af en person, der er autoriseret til dette af den juridiske person.
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 person. I den forbindelse skal personen være autentificeret, så vedkommende kan gøres ansvarlig for misbrug.	

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 person, skal ved on-line registrering autentificeres via et Akkreditiv på mindst samme sikringsni-	

veau som den juridiske person registreres på. En person autentificeret på sikringsniveau Lav må eksempelvis ikke gennemføre registreringer af juridiske personer 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 person. 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 person 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 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 person 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 person.

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 person generelt eller som medlem af den øverste ledelse, således at der er eftervist en stærk kobling mellem den autentificerede person og persontilknytningen for den juridiske person registreret i CVR.
b) Fremlagte fuldmagter udstedt af den juridiske person er kontrolleret som værende ægte og gyldige, herunder at de er underskrevet eller digital signeret af en person, der kan repræsentere den juridiske person (tilfælde a).
    - Papirbaserede fuldmagter rummer påtegning af vitterlighedsvidner grundet

den øgede mulighed for forfalskning (ikke nødvendigt for digitale fuldmagter). • 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 Akkreditiver

3.2.1 Styrke af Akkreditiv

Niveau: Lav	Krav: 1) Akkreditivet er udformet således, at udstederen tager rimelige skridt til at kontrollere, at det kun er den Person, som de tilhører, der har kontrol over og er i besiddelse af det.
Vejledning: Kravene til styrken af Akkreditiv går primært på at beskytte indehaveren af et Akkreditiv mod, at uvedkommende får adgang til at benytte dette og dermed udgive sig for indehaveren. Der er i NSIS ikke nogen krav til, at et Akkreditiv 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 andre steder i infrastrukturen, der kunne indikere, at et Akkreditiv 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. Brugerens muligheder for at bevare kontrollen med sit Akkreditiv afhænger af en række faktorer, herunder om Akkreditivet 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 Akkreditivet er blevet udleveret til rette vedkommende - så kravene går med andre ord på anvendelse af Akkreditivet efter udleveringen. Der er i NSIS separate krav til udleveringsprocessen, som adresseres nedenfor.	

Niveau: Betydelig	Krav: 2) Akkreditivet er udformet således, at det med betydelig sikkerhed kan antages, at det kun kan bruges, når det er den Person, som det tilhører, der har kontrol over eller er i besiddelse af det.
Vejledning: NSIS definerer ikke eksplicitte krav til kvaliteten af de enkelte Akkreditiver som fx længden eller entropien af kodeord eller engangskoder, perioder for udskiftning etc. Her må	

udstederen af et Akkreditiv foretage en konkret risikovurdering, der tager afsæt i den specifikke implementering inkl. mitigerende kontroller (fx muligheden for at spærre Akkreditiv 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. Til gengæld må man så overveje risikoen *for denial of service* angreb, hvor en legitim brugers kodeord/konto spærres.

Niveau: Høj	Krav: 3) Akkreditivet skal være beskyttet mod kopiering og manipulering af angribere med høj Angrebskapacitet. 4) Akkreditivet er udformet således, at den Person, som det tilhører, kan beskytte det sikkert mod, at andre bruger det.

Vejledning:

Terminologi omkring angrebskapacitet er hentet fra ISO 15408 "Information technology – Security techniques – Evaluation criteria for IT security" og ISO/IEC 18045 "Information technology – Security techniques – Methodology for IT security evaluation". Standarden er frit tilgængelig på www.commoncriteriaportal.org/cc.

På niveau Høj kræves en meget stor resistens - selv mod angribere med høj angrebskapacitet. Som 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 lever løsningen ikke op til kravene på dette niveau. Derimod kan en fysisk chip med en kryptografisk nøgle designes, så den i praksis er særdeles vanskelig at kopiere, hvorfor indehaveren kan være langt mere sikker på, om Akkreditivet kan være kompromitteret.

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 mobile enheder som smart phones etc. Her kan man på niveau Høj skele til nedenstående krav som alternativ til certificeringer:

1. Kryptografiske nøgler skal 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 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 Akkreditiver til rette vedkommende er en kritisk del af en Akkreditiv ordnings sikkerhed. Udleveringen kan afhængig af Akkreditivets 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 Akkreditiv ikke kan benyttes, før det er aktiveret. Dette nedbringer risikoen for, at uvedkommende kan benytte et opsnappet Akkreditiv (fx fra en postforsendelse).

Niveau: Betydelig	Krav: 2) Akkreditivet leveres efter udstedelse via en mekanisme, som gør det muligt med betydelig sikkerhed 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:

- Udleveringskanalen bør beskyttes bedst muligt – fx bør udlevering online ske over krypterede 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.
- Aktiveringskode og Akkreditiv kan fremsendes ad forskellige kanaler (fx den ene med post og den anden elektronisk).
- 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.
- Det kan være god skik at spærre et Akkreditiv automatisk, hvis det ikke aktiveres inden for et bestemt tidsrum fra afsendelsen/udleveringen.

Niveau: Høj	Krav:

	3) Aktiveringsprocessen kontrollerer, at Akkreditivet kun bliver udleveret til den Person, som det tilhører. 4) Udleveringen skal beskyttes mod angreb, hvor Akkreditivet stjæles under transport samt insider-angreb i udleveringsfunktionen hos udstederen ved fx at benytte to uafhængige forsendelseskanaler eller funktionsadskillelse.
Vejledning: Forskellen på niveau Betydelig og Høj består i, at niveau Høj forudsætter en personlig aktiveringsfunktion, hvor indehaveren tager ejerskab over sit Akkreditiv - og ikke alene en sikker forsendelse. Desuden skal man på niveau Høj mitigere insider angreb, så en enkeltstående, ondsindet person hos udstederen ikke på egen hånd kan få udstedt eller tiltage sig et fungerende Akkreditiv 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 Akkreditiv at suspendere (midlertidigt forhindre anvendelse) og/eller spærre (permanent forhindre anvendelse) hurtigt og effektivt.
Vejledning: Et vigtigt element i sikkerheden for Akkreditiver er brugernes aktive medvirken, der bl.a. kan opnås gennem oplysningskampagner, awareness, brugsvilkår mv. Særligt centralt er brugernes[6] mulighed for at spærre eller evt. suspendere deres Akkreditiv 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). Akkreditivudstederen har en særlig pligt til at sikre, at et Akkreditiv ikke kan anvendes efter spærring fx ved at udgive en spærreliste for PKI-baserede Akkreditiver – 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 Akkreditiver 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 deni-	

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

al-of-service angreb, hvor uvedkommende forsøger at spærre andres Akkreditiv – fx ved at etablere mekanismer, der gør det vanskeligt at massespærre Akkreditiver samt kontroller der sikrer, at det er rette vedkommende (eller anden autoriseret part), der spærrer sit Akkreditiv.

Niveau: Lav	Krav: 4) Udstederen af et Akkreditiv, skal på eget initiativ spærre et Akkreditiv: o hvis der er mistanke om kompromittering eller tab af kontrol over dette, o hvis der konstateres fejl i Akkreditiv (fx forkerte data), o hvis der ikke længere foreligger en gyldig aftale[7] mellem udsteder og ansøger, eller o hvis der er tale om et Akkreditiv tilknyttet en juridisk person og virksomheden ophører eller går konkurs.
Vejledning: En Akkreditivudsteder skal selvstændigt spærre et Akkreditiv 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 Akkreditivudstederens side afhænger naturligvis af de konkrete forhold – herunder adgang til viden og logfiler om brugen af et Akkreditiv, efterretninger etc. En Akkreditivudsteder er naturligvis ikke forpligtet til at agere på viden, som denne ikke har, men disse aspekter bør i indtænkes i udformningen af elektroniske identifikationsordninger.	

3.2.4 Fornyelse og erstatning

Niveau: Lav	Krav: 1) Processer til fornyelse og udskiftning skal enten honorere de samme krav som den initiale Identitetssikring (og indregne risikoen for ændrede identifikationsdata) eller baseres på en gyldig elektronisk identifikation på samme eller højere Sikringsniveau.
Vejledning: Kravene omhandler fornyelse i forbindelse med udløb af et Akkreditiv. Sker fornyelsen inden for Akkreditivets udløbsperiode (fx fordi brugeren har mistet det oprindelige Ak-	

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

kreditiv, eller dette er kompromitteret), kan re-identifikation evt. udelades op til niveau Betydelig, hvis der er stærke kontroller, som sikrer, at Akkreditivet udstedes til samme bruger. Et eksempel kunne være, at man ikke behøver at starte identitetssikringsprocessen helt forfra, hvis en bruger har mistet sit password og blot skal have et nyt. Hvis man under identitetssikring har etableret data, som giver mulighed for at udlevere et nyt password (fx over mail eller telefon), er det i visse tilfælde muligt at forlade sig på tidligere etablerede identitetsdata.

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 Akkreditivet.	

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 Akkreditiver 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 Akkreditiver og deres 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 Akkreditiv 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 Akkreditivet i forbindelse med udstedelsen samt have en separat log af dette.	

Niveau: Lav	Krav: 3) Autentifikationsmekanismen implementerer sikkerhedskontroller til at efterprøve Akkreditiver, 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: Autentifikationsmekanismer kan normalt ikke fuldstændigt forhindre alle typer angreb – men kan kun modstå angreb til et givet niveau. En måde at udtrykke dette på 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 Akkreditiv, phishing, aflytning, replay attack, session hijacking, man-in-the-middle, tyveri af Akkreditiv, spoofing og masquerading.	

Niveau: Betydelig	Krav: 5) Akkreditiverne, der er anvendt i Autentifikationen, skal tilsammen tilvejebringe mindst to Autentifikationsfaktorer fra forskellige kategorier af Autentifikationsfaktorer (dvs. der er tale om multi-faktor Autentifikation).
Vejledning: Niveau Betydelig forudsætter multi-faktor autentifikation. Det spiller her ingen rolle, om man kombinerer flere forskellige Akkreditiver eller benytter ét Akkreditiv, der i sig selv rummer flere faktorer. Kravet om forskellige kategorier af autentifikationsfaktorer henviser til de forskellige kategorier: a) "noget kun brugeren er" (fx biometri) b) "noget kun brugeren ved" c) "noget kun brugeren er i besiddelse af" 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. 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. Her skal oplåsningen være en specifik handling, der er knyttet til selve autentifikationen (fx startet fra den pågældende App). For en nøglefil vil gælde, at den ikke kan regnes som en faktor, med mindre det kan sikres, at kun brugeren har adgang til den. Dvs. filer på fællesdrev, roaming løsninger etc. hvor	

adgang til nøglefilen reduceres til et password[8], regnes ikke som en selvstændig løsning.

Niveau: Høj	Krav: 7) Mindst ét af de anvendte Akkreditiver skal opfylde kravene til niveau 'Høj' angivet i afsnit 3.2.1. 8) Hvis flere Autentifikationsfaktorer stammer fra samme enhed, så skal faktorerne være udformet, så kompromittering af én faktor ikke bevirker, at andre faktorer på enheden kompromitteres.
Vejledning: Kravet under punkt 7) betyder, at man fx ikke kan kombinere to Akkreditiver på niveau Lav for at opnå niveau Høj i en Autentifikation. Mindst et af Akkreditiverne anvendt i Autentifikationen skal til således opfylde kravene på niveau Høj som bl.a. indebærer, at Akkreditivet er beskyttet mod kopiering og manipulering. I praksis vil dette betyde, at den ene faktor skal være noget 'kun brugeren er i besiddelse af'. Kravet under punkt 8) indebærer, at faktorerne indbyrdes skal udvise en vis uafhængighed, således at kompromittering af den ene faktor ikke direkte kan føre til kompromittering af den anden faktor. Et eksempel kunne være en nøglefil beskyttet med password. Her vil adgang til nøglefilen gøre det muligt at foretage et brute force angreb, hvor mange forskellige passwords afprøves, indtil det rigtige findes. Derfor vil adgang til nøglefilen føre til kompromittering af den anden faktor (password), og derfor er kravet ikke opfyldt. Et andet eksempel kunne være en autentifikation bestående en kombination af en App på en telefon (uden password) kombineret med en engangskode sendt via SMS. Her vil adgang til telefonen (den ene faktor) betyde, at den anden faktor (SMS) kompromitteres.	

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

4 Organisatoriske- og tværgående krav

4.1.1 Generelle krav

Kravene i kapitel 4 skal opfyldes både af udstedere af Akkreditiver 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 ordninger, der anmeldes af Danmark til EU-kommissionen i regi af [eIDAS]-forordningen. Dette vil kun ske for nationale, elektroniske identifikationsordninger efter aftale med Digitaliseringsstyrelsen.	

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.	

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 leverandørens 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 leverandøren overholder relevant lovgivning. Under privatlivspolitik samt oplysninger om behandling af personoplysninger bør leverandøren 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 kravene i [ISO 27001] standarden.
Vejledning: Håndtering af risici er relevant for alle dele for udstedere af Akkreditiver samt Identitetsbrokere. For at være effektivt, må ledelsessystemet for informationssikkerhed (ISMS) håndtere relevante risici for alle dele af en løsning. Afhængig af den organisatoriske struktur, kan det være relevant at have flere ISMS'er til operatørerne af de forskellige dele af en Akkreditiv-ordning eller Identitetsbroker. 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) Organisationen skal være certificeret efter [ISO 27001] standarden eller på tilsvarende måde kunne dokumentere efterlevelsen af krav til informationssikkerhedsledelse.
Vejledning: På niveau Høj skal der foreligge uafhængig dokumentation for, at organisationen efterlever sit valgte ledelsessystem for informationssikkerhed. Dette kan enten være gennem relevant certificering eller gennem alternative mekanismer, der tilvejebringer en tilsvarende betryggelse i efterlevelsen via en uafhængig tredjepart.	

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 fem år – med mindre lovgivning tilsiger noget andet for de konkrete data. Her kan det fx være relevant at skele til bogføringsloven. Det kan i øvrigt anbefales at opdele 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 Akkreditiver er identitetssikringsprocessen, hvor personale i nogle sammenhænge udfører en vigtig opgave i identitetssikringen. Af øvrige områder kan nævnes administratorer, sikkerhedspersonale og andre, som udfører betroede funktioner.	

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 konsekvenserne ved tab af konfidentialitet, integritet og tilgængelighed til et acceptabelt niveau ud fra en risikovurdering, hvor det ønskede sikringsniveau er taget i betragtning. Et eksempel på en måde at operationalisere dette på kan være at sætte konsekvensniveauet i risikovurderingen (typisk defineret på en tretrinsskala fra 1=Mindre alvorlig, 2=Alvorlig og 3=Meget Alvorlig) til samme niveau som det ønskede sikringsniveau (der også benytter en tretrinsskala gående fra niveau 1=Lav til niveau 3=Høj).

For Akkreditivudstedelse vil aspektet 'integritet' ofte være det vigtigste af de tre, 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 kan føre til manglende adgang til de bagvedliggende forretningstjenester, der anvender Akkreditiverne. Her vil kritikaliteten skulle ses i forhold til disse tjenester samt brugernes mulighederne for at få adgang via andre kanaler. Ovenstående er ment som generelle tommelfingerregler, og der bør under alle omstændigheder foretages en konkret 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

Niveau: Lav	Krav: 1) Organisationen skal ved anmeldelse af sin Elektroniske Identifikationsordning og/eller Identitetsbroker til Digitaliseringsstyrelsen redegøre for den tekniske og sikkerhedsmæssige udformning samt Sikringsniveau og navn. 2) Organisationen skal ved anmeldelse af sin Elektroniske Identifikationsordning og/eller Identitetsbroker til Digitaliseringsstyrelsen anvende selvdeklarering. Anmelderen indestår selv for, at kravene til det angivne Sikringsniveau 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.	

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: Dokumentationen skal på niveau Betydelig og Høj som minimum omfatte: • Service- og formålsbeskrivelse. • Beskrivelse af det organisatoriske setup, parter, underleverandører etc. • Præcis og dækkende teknisk dokumentation for løsningen. • Beskrivelse af processer og procedurer. • Dokumentation for ISMS. • Dokumentation for gennemførte risikovurderinger, herunder identificerede konsekvenser, trusler, sårbarheder og kontroller. • Revisionserklæringer samt evt. baggrundsmateriale udarbejdet i forbindelse med disse. • Ledelseserklæringer. • Dokumentation for tegnede forsikringer mv. • Kontaktinformation for videnspersoner, hvor yderligere oplysninger kan søges, og kontaktinformation på driftsansvarlige og ledelsesansvarlige. Digitaliseringsstyrelsen forpligter sig ikke til at gennemgå dokumentationen men vil opbevare denne i tilfælde af fremtidige hændelser eller sager. Dokumentationen holdes fortrolig og vil ikke blive offentliggjort – dog forbeholdes ret til at dele denne med rådgivere, der arbejder for styrelsen under fortrolighedserklæring, samt relevante andre myndigheder, der kan have en interesse i evt. sikkerhedshændelser (fx Politiet, Datatilsynet, Efterretningstje-	

nester o.lign.).

Revisionserklæringen spiller 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 hinandens 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 dokumenteret.

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 personer

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

a) Ved udstedelse af et nyt selvstændigt, Akkreditiv som det fx kendes fra OCES Medarbejdercertifikater, hvor en NemID Administrator i virksomheden kan foranledige, at der udstedes et nyt Akkreditiv.
b) Ved etablering af en logisk forbindelse, der knytter en fysisk person til en juridisk person uden udstedelse af nye Akkreditiver (fx ved CVR- opmærkning af den fysiske person, hvor den fysiske person benytter sit personlige Akkreditiv i erhvervssammenhæng). Herved skabes en ny, logisk erhvervsidentitet uden udstedelse af et nyt, fysisk Akkreditiv.

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 personer

Niveau: Lav, Betydelig, Høj	Krav: 4) Godtgørelse af Identiteten af den fysiske person, der handler på vegne af den juridiske person, kontrolleres på Sikringsniveau »lav« eller derover. 7) Sikringen af Identiteten af den fysiske person, der handler på vegne af den juridiske person, foretages på sikringsniveau »Betydelig« eller »Høj«. 11) Sikringen af Identiteten af den fysiske person, der er tilknyttet en juridisk person, kontrolleres på Sikringsniveau »Høj«.
Vejledning: Når der etableres en association mellem en juridisk person og et Akkreditiv udstedt til 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 Akkreditivet. Med andre ord har man allerede etableret hvem den fysiske person er og udstedt et Akkreditiv til denne, og kan så koncentrere sig om at sikre koblingen til den juridiske person.	

Niveau: Betydeligt	Krav: 8) Forbindelsen er etableret under kontrol af den juridiske person fx via en udpeget administrator eller via oplysninger fra en Autoritativ kilde.
Vejledning: I mange tilfælde vil virksomhederne selv håndtere (og dermed kontrollere) associeringerne mellem virksomheden og fysiske personer, herunder om og hvornår der evt. skal udstedes Akkreditiver, som understøtter forbindelsen. Typisk vil dette ske ved, at virksomhedens ledelse udpeger en administrator, der på virksomhedens vegne vedligeholder forbindelser og Akkreditiver, 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 Akkreditiver automatisk vedligeholdes. I visse tilfælde kan man endvidere vedligeholde associeringer på baggrund af 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 Akkreditivet. Der henvises til den fællesoffentlige referencearkitektur for brugerstyring [REF-ARK] for yderligere beskrivelser og detaljer.

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 kæden frem for kun at se på autentifikationen i første led (som dækket i de første kapitler).

Først og fremmest er det relevant at præcisere, hvad der menes med en Identitetsbroker. I kontekst af NSIS menes her en tjeneste, som videreformidler en autentifikation til en tredjepart ved at udstede og signere et såkaldt Security Token for en elektronisk identitet. Disse benævnes i nogen sammenhænge for 'Identity Providers' eller 'Security Token Services'[9], 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 Akkreditiv men kun attributter og et formidlet sikringsniveau.

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 videreformidler er 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) er ikke videreformidling og dermed 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 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 (Level of Assurance), således at modtageren af tokens direkte kan aflæse dette. Sikringsniveauet i et token opgøres som mindsteværdien af Sikringsniveauet for Autentifikationen, brokerens eget Sik-

[9] 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.

	ringsniveau (FAL) samt Sikringsniveauerne for evt. Identitetsbrokere, der er benyttet som underleverandører i den konkrete Autentifikation (dvs. LoA i token er minimum af IAL, AAL og FAL).
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. • Hvis en Identitetsbroker har et lavere sikringsniveau end de tidligere sikringsniveauer i kæden (fx hvis brugeren autentificerede sig på niveau Høj mens brokeren kun opretholder niveau Lav, da nedgraderes sikringsniveauet for brokerens udstedte token til det lave niveau (i eksemplet niveau Lav). I modsat fald ville en broker på et lavere niveau kunne give en bagdør til at forfalske autentifikationer på højere sikringsniveauer.	

Niveau: Lav	Krav: 5) Single Sign-On sessioner 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 (bruger anvender Identity Provider) at være begrænset til få minutter (fx 5-10 min), og i NemLog-in føderationen anvendes 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: 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 hver 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 SAML). 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 Iden-	

titetsbrokere anvender præcise tidsstempler i deres logs.

Niveau: Betydelig	Krav:
	10) Tokens, som indeholder følsomme personoplysninger eller transporteres via brugerens browser, skal end-to-end krypteres, 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 (Identity Provider / Identity Broker) og forretningstjeneste. Dette gælder eksempelvis SAML HTTP Redirect Binding og SAML HTTP POST binding. 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. 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 ovennævnte trussel mod fortroligheden være acceptabel. Hvis brugerens browser er kompromitteret, vil der alligevel være sandsynlighed for datalæk, når forretningstjenesten præsenterer data lige efter autentifikationen. Hvis security tokens omvendt indeholder følsomme oplysninger (herunder følsomme personoplysninger jævnfør [GDPR] artikel 9), og der samtidig kommunikeres via brugerens browser, stiller NSIS krav til end-to-end kryptering af security tokens, hvilket dækker hele vejen fra Identitetsbroker til forretningstjeneste.	

Niveau: Høj	Krav:
	14) Brokerens private nøgle, der underskriver security tokens, placeres i "tamper-resistent" kryptografisk hardware (HSM), 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 Akkreditiver 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.

Kravene om certificering for brokere er derfor skærpet i forhold til kravene til beskyttelse af den enkelte brugers Akkreditiv, som findes i afsnit 3.3.1.

7 Governance

Der er ikke pt. vejledning til dette kapitel.

8 Referencer

[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".

[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 "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".

[ISO 29115] "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".

[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 [CIR] "Cirkulære vedrørende sikkerhedsbeskyttelse af informationer af fælles interesse for landene i NATO, EU eller WEU, andre klassificerede informationer samt informationer af sikkerhedsmæssig beskyttelsesinteresse i øvrigt", CIR nr. 204 af 07/12/ 2001."

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

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

[TU-LoA] "Valg af sikringsniveau for identiteter - vejledning i brug af NSIS for tjenesteudbydere - version 1.1", Digitaliseringsstyrelsen. https://www.digitaliser.dk/resource/3651469