Digitaliserings-
styrelsen

National Standard for Identiteters Sikringsniveauer (NSIS) Version 2.1

Udgivet: 03.05.2024 (Høringsversion)

1 Indledning

1.1 Ændringshistorik

Dato	Version	Ændringer
08.11.2022	2.0.2	Referencer til hjemmesider og øvrige dokumenter er opdateret og udbygget. Enkelte slåfejl er rettet. Indledningen til afsnit 3.1.3 er udbygget med henblik på at præcisere, hvornår verifikation af juridiske enheder er relevant. Afsnit 4.1.1 punkt 2 vedr. overholdelse af lovgivning er justeret sprogligt. Afsnit 4.1.7 om anmeldelse og revision er opdateret: • I krav 3 om intern revision er det præciseret, at kravet alene gælder niveau Lav, og der er indført krav om årlig genbekræftelse af anmeldelser på niveau Lav. • I krav 5 og 6 er det præciseret, at man kan anvende alternativer til kontrolskemaet med samme indhold (se også den opdaterede vejledning til dette punkt). Indledningen til kapitel 6 er udbygget med henblik på tydeligere at beskrive identitetsbrokernes rolle.
02.02.2023	2.0.2a	Der er fjernet et overskydende "eller" fra krav 3.2.3 punkt 4. Opdateringen er mao. kun sproglig.

Dato	Version	Ændringer
18.04.2024	2.1	Opdateret på baggrund af survey samt feedback fra revisorer og erfaringer med implementering af standard. • Terminologiafsnittet er udbygget med forklaring af centrale begreber (Lokal IdP og Full-Service IdP) og der indført en ny illustration af begreberne Entitet, Digital Identitet og Identifikationsmiddel. • Der er indført et afsnit om 'tillidskæden for digitale identiteter' med henblik på at forklare roller og ansvar for de forskellige parter, der håndterer digitale identiteter. • Der er indført en præcisering af, hvornår et eksisterende identifikationsmiddel kan anvendes til at udstede et nyt identifikationsmiddel. • Krav 4.1.1 punkt 2) om overholdelse af lovgivning er undtaget af revisionspligten. • Forhold omkring oplysningspligten er præciseret. • Revisionserklæringer kan udformes af registrerede revisorer og ikke kun statsautoriserede revisorer (4.1.7) og der er indført formulering om relevante kompetencer. • I afsnit 7.2 er det præciseret i forhold til bl.a. ophør. • I afsnit 7.3 er formuleringen omkring ansvar bragt i overensstemmelse med standardens krav, herunder at erhvervsansvarsforsikringer i visse sammenhængende kan erstattes af andre ordninger. • Henvisninger til NemID er fjernet.

1.2 Forord

Dette dokument beskriver National Standard for Identiteters Sikringsniveauer (NSIS), hvis formål er at skabe rammer for tillid til digitale Identiteter samt digitale ID-tjenester. Standarden er udarbejdet og administreres af Digitaliseringsstyrelsen og stilles til rådighed som referenceramme for arbejdet med brugerstyring i den offentlige sektor.

Dokumentet tager afsæt i internationale standarder og rammeværk med henblik på at sikre interoperabilitet, videndeling, certificering og understøttelse af det indre

marked, herunder væsentligst [eIDAS] forordningen, den tilhørende gennemførselsforordning 2015/1502 om "Levels of Assurance" [LOA]), referencearkitektur for brugerstyring [REF-ARK] og [ISO 29115].

Udover dette dokument med normative krav findes også en særskilt og omfattende vejledning til standarden [VEJL], som uddyber kravene gennem forklaringer og eksempler, samt i vejledningen til anmeldelses og revisionsprocessen [REV] og kontrolskemaet, som benyttes ved anmeldelse (se afsnit 4.1.7 for flere detaljer).

Det anbefales meget kraftigt at læse vejledningen sammen med standarden, da vejledningen bibringer konteksten for at forstå kravene i standarden.

På Digitaliseringsstyrelsens hjemmeside (https://digst.dk/it-loesninger/standarder/nsis/) kan man finde alt relevant materiale, læse svar på ofte stillede spørgsmål (FAQ), se positivlisten og tilmelde sig nyhedsbrevet om NSIS.

1.3 Introduktion

Nærværende standard definerer krav til styrken af en autentifikationsproces, den underliggende Identitetssikring samt det anvendte Elektronisk Identifikationsmiddel - udtrykt som et samlet 'Sikringsniveau'. Dette kan også udtrykkes som graden af tillid en tjenesteudbyder kan have til en autentificeret Identitet – eller på engelsk '*Level of Assurance*' (LoA). Begreberne 'Sikringsniveau' og 'LoA' anvendes nedenfor som udtryk for den samme egenskab.

Standarden indeholder en række krav til ID-tjenester på tre forskellige Sikringsniveauer benævnt 'Lav', 'Betydelig' og 'Høj'. Tidligere versioner af NSIS opererede desuden med niveauet 'Begrænset', men dette Sikringsniveau er udgået, da det i praksis ikke har nogen reel anvendelse. De tre niveauer i NSIS modsvarer direkte de tre niveauer i [eIDAS]-forordningen.

Hensigten med NSIS er, at en tjenesteudbyder kan definere kravene til ønsket Sikringsniveau for brugerne baseret på en risikovurdering som beskrevet i vejledningen [LOA-VEJL], og at ID-tjenester som leverer identiteter måles mod disse niveauer. Herved afpasses risici i forretningstjenesten ("risikoniveauer") med styrken af kontroller ("Sikringsniveauer").

Kravene til de tre Sikringsniveauer omfatter både tekniske, organisatoriske og økonomiske forhold og revision, idet mange faktorer har indflydelse på tilliden til digitale Identiteter og ID-tjenester.

1.4 Formål og scope

Denne standard er gældende for nationale, fællesoffentlige Elektroniske Identifikationsordninger og Identitetsbrokere, der håndterer identiteter for fysiske personer, juridiske enheder og fysiske personer associeret med en juridisk enhed (herunder medarbejdere). Standarden stilles til rådighed for anvendelse i såvel stat, kommuner som regioner og på tværs af domæner (fx sundhed og uddannelse) og omfatter både private og offentlige udbydere af Elektroniske Identifikationsordninger samt Identitetsbrokere. Ud fra en modenhedsbetragtning er identitetshåndtering for enheder/devices og Internet of Things på nuværende tidspunkt ikke omfattet af stan-

darden. I takt med at disse områder modnes, og der evt. fremkommer internationale rammeværk herfor, kan områderne blive indlemmet i NSIS, hvis det vurderes hensigtsmæssigt. Sikringsniveauerne i NSIS udtaler sig alene om Identitet, og derfor er der ikke medtaget håndtering af kvalitet for andre typer attributter som fx rettigheder, fuldmagter, lokale autorisationer mv. På disse områder findes der endnu ikke nogen nationale standarder, som fastlægger kvalitetskrav.

NSIS behandler alene forhold vedrørende udstedelse og brug af Elektroniske Identifikationsmidler og Identitetsbrokere, men der findes naturligt en lang række øvrige aspekter, man bør tage stilling til, når det samlede niveau af informationssikkerhed for en forretningstjeneste skal fastlægges som fx autorisation, fortrolighed og tilgængelighed.

Kravene i NSIS tager udgangspunkt i og er i tråd med [eIDAS] reguleringen, således at en dansk Elektronisk Identifikationsordning, som opfylder et givet Sikringsniveau i denne standard, også må forventes at kunne opfylde kravene til samme niveau i forhold til [eIDAS]-forordningen. I den forbindelse skal det dog bemærkes, at NSIS vil være tilpasset nationale forhold og være mere detaljeret end den gennemførelsesretsakt [LOA], som definerer de tilsvarende niveauer under [eIDAS]-forordningen, som på en række punkter vil have en mere overordnet karakter. Det kan endvidere bemærkes, at Lov om MitID og NemLog-in [LOV] fastlægger, at NSIS ligger til grund for den offentlige infrastruktur.

Det ligger ikke inden for rammerne af denne standard at beskrive yderligere forhold omkring tjenesteudbyderes ansvar i forbindelse med informationssikkerhed og valg af Sikringsniveau for autentificerede brugere, der tilgår deres forretningstjeneste:

NSIS stiller ikke normative krav til tjenesteudbydere.
Ansvaret for vurdering af det krævede Sikringsniveau og risikoniveau for den enkelte forretningstjeneste (dvs. i rollen som ***modtager*** af identitet) ligger hos den enkelte myndighed/udbyder, som er dataansvarlig for de data, som udstilles og kan tilgås via tjenesten på det krævede Sikringsniveau. Der kan i denne forbindelse henvises til publikationen [LOA-VEJL], der giver eksempler og vejledning til tjenesteudbydere om, hvordan fastlæggelse af behov for Sikringsniveau kan gribes an ud fra en risikobaseret tilgang. Denne vejledning er dog ikke normativ og tjener alene til inspiration.

For organisationer, som behandler personoplysninger, vil afdækning af risici og kontroller ofte ligge i naturlig forlængelse af forpligtelserne i henhold til den til enhver tid gældende regulering af behandling af personoplysninger. Datatilsynet fører tilsyn med overholdelse af den gældende regulering af personoplysninger.

1.5 Eksempler på ID-tjenester og Sikringsniveauer

MitID og *NemLog-in 3*	NemLog-in og MitID løsningerne arbejder med differentiering mellem forskellige typer Elektroniske Identifikationsmidler og identitetssikringsprocesser, og benytter NSIS som referenceramme til at beskrive Sikringsniveauerne for disse. Lov om MitID og NemLog-in [LOV] benytter ligeledes NSIS som referenceramme for sikringsniveauer.
Private ID-tjenester	Standarden definerer betingelserne for et kendt Sikringsniveau, således at private ID-tjenester vil kunne vurderes i forhold til anvendelse i offentligt regi. Ved at benytte en fælles standard muliggøres samarbejde på tværs af sektorer.

Lokal Identity Provider (IdP)	Mange organisationer ønsker at agere som Identity Provider (Identitetsbroker) og udsteder af Elektroniske Identifikationsmidler for egne medarbejdere. Dette gælder eksempelvis på det kommunale område, hvor næsten alle kommuner har en Lokal IdP. I en sådan model kan en medarbejders lokale log-in blive fødereret til eksterne, fælleskommunale systemer eller tjenester i andre føderationer (fx på sundhedsområdet eller NemLog-in føderationen), hvorved medarbejderen opnår fordele ved at kunne anvende det samme identifikationsmiddel på tværs af alle tjenester, og organisationen opnår fordele ved kun at skulle administrere deres brugere ét sted. Organisationer med Lokal IdP har forskellige processer til identitetssikring, forskellige HR-processer, forskellige it-systemer, forskellig organisering af sikkerhed og anvender forskellige Elektroniske Identifikationsmidler. Her giver NSIS en standardiseret ramme at måle den enkelte Lokale IdP op imod, så tjenesteudbydere ikke behøver at forholde sig til de konkrete forhold hos den enkelte Lokale IdP men blot kan efterspørge et bestemt sikringsniveau fastlagt i standarden. I de fleste tilfælde vil en organisation med Lokal IdP både udstede lokale identifikationsmidler til deres brugere samt udstille en autentifikationsservice, hvor tjenesteudbydere kan anmode om at få en bruger autentificeret. Dermed vil en typisk Lokal IdP således skulle opfylde kravene i kapitel 3, 4, 5 og 6 (evt. fraregnet 3.1.3), hvis den skal kunne udtale sig om et NSIS sikringsniveau.

FullService IdP	En FullService IdP er en variant af en Lokal IdP beskrevet ovenfor, der leveres som en service til en brugerorganisation. Modellen er defineret ved, at leverandøren af FullService IdP'en varetager samtlige krav i NSIS-standarden på vegne af brugerorganisationen og herunder tager ansvaret for identitetssikring og udstedelse af identifikationsmidler, hvorved det ikke er nødvendigt for brugerorganisationen selv at foretage en NSIS anmeldelse forud for anvendelse af FullService IdP'en til autentifikation af egne medarbejdere. Bemærk at modellen forudsætter, at brugerorganisationen ikke er ansvarlig for nogen af processerne, der er underlagt krav i NSIS (fx identitetssikring, udstedelse af identifikationsmidler osv.) eller driver nogen af de systemer, der medvirker til kravsopfyldelsen. Der kræves således 'vandtætte skodder' til brugerorganisationen, hvis denne skal undgå at skulle NSIS anmeldelses. Hvis der er et delt ansvar, hvor en serviceleverandør er ansvarlig for nogle (men ikke alle) krav til en lokal IdP, skal brugerorganisationen selv NSIS-anmelde den lokale IdP, men kan så i anmeldelsen evt. henvise til erklæringer fra serviceleverandøren. Yderligere detaljer om revision ved brug af serviceleverandører er beskrevet i NSIS i vejledningen til anmeldelses og revisionsprocessen [REV]. En FullService IdP vil som udgangspunkt skulle håndtere kravene i afsnit 3.1.3 vedr. verifikation af identitet for juriske enheder. Disse krav sikrer, at FullService IdP'en har verificeret identiteten af den brugerorganisation, som den leverer en service til og autentificerer brugere på vegne af.
Sundhedsområdet (Security Token Services)	Sundhedsområdet har etableret Security Token Services[1] både nationalt og på regionernes serviceplatforme (NSP'er), som udsteder såkaldte ID-kort for sundhedsfaglige Identiteter (se [NSI]). Disse ID-kort forudsætter et bestemt niveau af tillid til den digitale Identitet i forbindelse med adgang til tjenester, og en fælles standard vil muliggøre anvendelse på tværs af sektorer med fælles forståelse af Sikringsniveau.
Uddannelsesområdet	Der er en række ID-tjenester og føderationer etableret på uddannelsesområdet, og uddannelsesinstitutioner står ofte som garanter for Identiteter i egne organisationer gennem deltagelse i en føderation. Tjenester som Uni-Login og WAYF agerer hhv. som Identity Provider og Proxy, som fødererer disse Identiteter, og NSIS kan anvendes som en fælles ramme for tillid til disse.

[1] Billetudstedere som giver adgang til sundhedstjenester.

Udenlandske Elektroniske Identifikationsmidler	Som følge af [eIDAS] forordningen skal EU-landene gensidigt anerkende nationale Elektroniske Identifikationsordninger, som er anmeldt til Kommissionen. Medlemslandenes nationale Elektroniske Identifikationsordninger er vidt forskellige, men gensidig tillid opnås gennem et fælles tillidsrammeværk, der definerer et antal kendte Sikringsniveauer. I Danmark er der etableret en såkaldt eID-gateway, som bl.a. kan facilitere autentifikation af personer fra øvrige EU-lande med deres lokale eID til danske tjenester med et veldefineret sikringsniveau.

1.6 Terminologi

Nedenfor er de vigtigste begreber i standarden beskrevet. Der anvendes den konvention, at definerede begreber skrives med stort begyndelsesbogstav. Terminologien er for en stor dels vedkommende kompatibel med referencearkitekturen for brugerstyring [REF-ARK] for at sikre konsistens med andet arbejde inden for fællesoffentlig brugerstyring. På en række områder har NSIS dog behov for at gå i større detaljer, og det skal endvidere bemærkes, at referencearkitekturen anvender begrebet 'Akkreditiv' for det begreb, der i NSIS og eIDAS kaldes for 'Elektronisk Identifikationsmiddel'.

Adgangskontrol	Proces i en tjeneste, der afgør hvilke funktioner og data en bruger får adgang til på baggrund af brugerens Identitet, Attributter, roller/rettigheder og tjenestens sikkerhedspolitik.
Attribut	Karakteristika eller egenskaber ved en Entitet eller Identitet. Dette kan fx være et navn, brugernavn, et pseudonym, et CPR-nummer, en UUID, bopæl, rolle etc.
Autentifikation	En proces som genkender og verificerer en Identitet (tilknyttet en Entitet) gennem anvendelse af et Elektronisk Identifikationsmiddel, der er koblet til Identiteten. Ved **multi-faktor** autentifikation forstås en autentifikationsproces, hvor det anvendte Elektroniske Identifikationsmiddel tilvejebringer flere Autentifikationsfaktorer fra forskellige kategorier (se nedenfor).

Autentifikationsfaktor	En egenskab ved et Elektronisk Identifikationsmiddel, der binder det til Entiteten, og som kan være i **kategorierne:** a) »indehaverbaseret autentifikationsfaktor«: en autentifikationsfaktor, som Entiteten skal bevise at være i besiddelse af (fx en fysisk enhed) b) »vidensbaseret autentifikationsfaktor«: en autentifikationsfaktor, som Entiteten skal bevise at have kendskab til (fx et kodeord) c) »iboende autentifikationsfaktor«: en autentifikationsfaktor, der er baseret på et fysisk træk hos en fysisk person, og som Entiteten skal bevise at have (fx biometri) Et Elektronisk Identifikationsmiddel kan have en flere faktorer.
Autoritativ kilde	Enhver kilde der uanset dens form kan anvendes til at opnå nøjagtige data, oplysninger og/eller beviser, der kan bruges til at fastslå en Identitet. Autoritative kilder kan antage mange former som f.eks. registre, dokumenter eller organer, afhængig af hvilken kontekst et identitetsbevis skal kontrolleres i.
Angrebskapacitet	En autentifikationsmekanisme kan ikke modstå alle angreb men kun angreb til vist niveau. En standardiseret måde at kvantificere modstandskraften mod forskellige mekanismer er at rangordne dem mod angreb med en bestemt angrebsstyrke. I dette dokument anvendes begreberne *basalt*, *moderat* og *højt* om forskellige angrebsstyrker. Terminologien er taget fra [ISO15408] som kan konsulteres for yderligere beskrivelser.
Dynamisk Autentifikation	En elektronisk proces, som anvender kryptografi eller andre teknikker til på forlangende at skabe et elektronisk bevis for, at en Entitet har adgang til eller er i besiddelse af et Elektronisk Identifikationsmiddel, og hvor beviset ændres ved hver Autentifikation mellem Entiteten og det system, der kontrollerer beviset. Dynamisk Autentifikation beskytter bl.a. mod såkaldte *replay*-angreb.

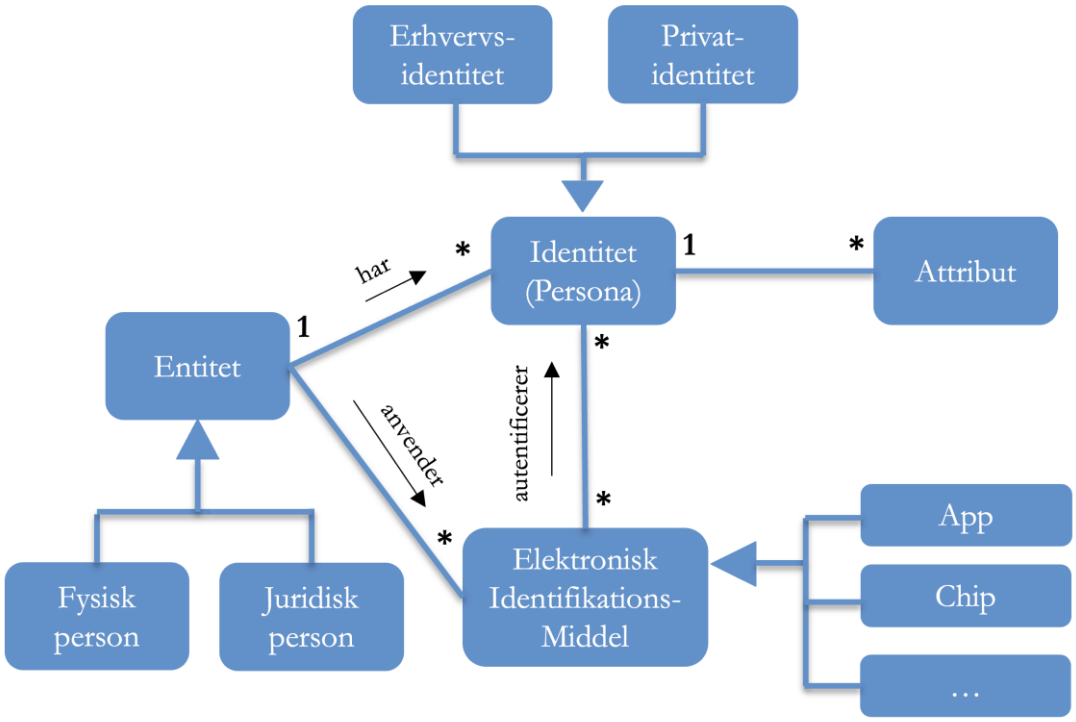
Elektronisk Identifikations-middel	Et middel som en Entitet får udstedt til brug for on-line Autentifikation. Midlet kan både være fysisk og virtuelt, og skal være under Entitetens kontrol. Et s*amlet* Elektronisk Identifikationsmiddel består af ét eller flere elementer, der hver især er et *enkelt* elektronisk Identifikationsmiddel, som anvendes i kombination med henblik på at tilfredsstille kravene på et højere Sikringsniveau, end der kan opnås isoleret med et enkelt Elektronisk Identifikationsmiddel. Bemærk at begrebet (enkelt) Elektronisk Identifikationsmiddel anvendes tilsvarende begrebet 'Authenticator' i den amerikanske [NIST] standard - og altså ikke begrebet 'Credential', som i [NIST] anvendes som betegnelse for *bindingen* mellem en Identitet og en eller flere 'Authenticators'.
Elektronisk Identifikations-ordning	Et samlet system til elektronisk identifikation under hvilket der udstedes Elektroniske Identifikationsmidler til fysiske personer eller juridiske enheder, og/eller fysiske personer, der er associeret til juridiske enheder. En Elektronisk Identifikationsordning dækker alle processer i livscyklus for Elektroniske Identifikationsmidler, herunder registrering, udstedelse, anvendelse, udløb, spærring og arkivering. En Elektronisk Identifikationsordning anmeldes samlet til Digitaliseringsstyrelsen, og kan underliggende anvende en eller flere ID-tjenester til at håndtere de enkelte processer i Elektroniske Identifikationsmidlers livscyklus. Kravene til en Elektronisk Identifikationsordning fremgår i kapitel 3-5 og stilles separat fra kravene til Identitetsbrokere, der fremgår i kapitel 4 og 6. Der er således ingen forpligtelse til at implementere begge sæt af krav, idet der kun skal opfyldes krav til den rolle, man vælger at anmelde.
Entitet	En fysisk person eller juridisk enhed, som ønsker adgang til en on-line tjeneste gennem Autentifikation med Elektroniske Identifikationsmidler. En Entitet kan have flere Elektroniske Identiteter – fx kan en fysisk person både have en privatidentitet og flere erhvervsidentiteter.

Identitet (Elektronisk)	En digital persona (brugeridentitet) repræsenteret ved et sæt af attributter, som fx kan repræsentere en fysisk person (privatidentitet), en juridisk enhed (virksomhedsidentitet), eller en fysisk person, der er associeret med en juridisk enhed (fx erhvervsidentitet eller erhvervsbruger). En Identitet *kan* rumme Personidentifikationsdata men kan også være pseudonym.
Identitetsbroker	En ID-tjeneste som formidler en autentificeret Identitet til tredjeparter på baggrund af en Autentifikation verificeret af brokeren selv eller evt. af en anden tredjepart (brokere i flere led). En Identitetsbroker foretager ikke nødvendigvis selv Identitetssikring eller udstedelse af Elektroniske Identifikationsmidler, og kan derfor være separat fra en Elektronisk Identifikationsordning. En Identitetsbroker er en tjeneste, som kræver tillid (optræder som en såkaldt *trusted third party*) fra forretningstjenester, og er derfor underlagt krav i denne standard.
Identitetsregister	En funktion/register, der registrerer information om Entiteter (fx borgere) og betragtes som en Autoritativ Kilde. Dette kan fx være CPR-registret og CVR-registret som eksempler blandt flere registre.
Identitetssikring	En proces hvor Identiteten af en Entitet fastlægges, og hvor Personidentifikationsdata (fx navn og CPR-nummer eller tilknytning til juridisk enhed) efterprøves. Processen benævnes '*identity proofing*' på engelsk.
ID-tjeneste	En betroet tjeneste, som udfører en eller flere af de processer, som er underlagt krav i denne standard. Dette kan fx være Identitetssikring, udstedelse af Elektroniske Identifikationsmidler eller en Identitetsbroker. Bemærk at [eIDAS] reguleringen bruger begrebet "tillidstjeneste" om tjenester involveret i udstedelse af digitale signaturer/certifikater, validering af certifikaters gyldighed og tidsstempling, hvilket ligger uden for NSIS område. NSIS vedrører således områderne i [eIDAS] kapitel 2 (særligt Artikel 8), mens tillidstjenester vedrører [eIDAS] kapitel 3. En NSIS ID-tjeneste skal mao. ikke opfattes som en [eIDAS] tillidstjeneste (med mindre den også udsteder certifikater, foretager tidsstempling eller nogle af de andre funktioner, der beskrives i [eIDAS] kapitel 3).
Person	En fysisk person eller juridisk enhed.

Personidentifikationsdata	Et sæt af data (attributter), der gør det muligt at fastslå Identiteten af en fysisk person eller juridisk enhed (dvs. som identificerer en Entitet entydigt). Typiske eksempler er navn, fødselsdato, CPR-nummer, CVR nummer, PID, RID, UUID etc. Typisk vil en IdP udstede et token (billet) indeholdende Personidentifikationsdata samt evt. andre attributter (fx rettigheder) som resultat af en succesfuld autentifikation. Det tilhørende NSIS sikringsniveau i tokenet angår alene Personidentifikationsdata og ikke øvrige attributter.
Sikringsniveau (LoA)	Graden af tillid til en autentificeret Identitet (på engelsk *"Level of Assurance"*) og ofte benævnt *autenticitetsSikringsniveau*. Sikringsniveauer beskrives i dette dokument som tre niveauer benævnt hhv. Lav, Betydelig og Høj, og der stilles krav til de forskellige delprocesser i forbindelse med identitetssikring, registrering, udstedelse og anvendelse af Elektroniske Identifikationsmidler mv. Ved vurderingen af LoA gælder alle krav i NSIS (dog ikke kravene til Identitetsbrokere, hvis en sådan ikke har været en del af Autentifikationen). Det overordnede Sikringsniveau (LoA) kan dekomponeres i flere underbegreber: **IAL** (*Identity Assurance Level*) beskriver styrken af Identitetssikringsprocessen. Ved vurderingen gælder kravene i afsnit 3.1, kapitel 5 samt de generelle krav i kapitel 4. **AAL** (*Authenticator Assurance Level*) beskriver Sikringsniveauet for et samlet Elektronisk Identifikationsmiddel som anvendes i en Autentifikation. Ved vurdering af AAL gælder kravene i afsnit 3.2 og 3.3 samt de generelle krav i kapitel 4. **FAL** (*Federation Assurance Level*) beskriver Sikringsniveauet for en Identitetsbroker, der videreformidler en Identitet til tredjepart. Ved vurderingen gælder kravene i afsnit 6.1 samt de generelle krav i kapitel 4.

Tjenesteudbyder	En organisation med et it-system, som brugere logger ind på med et Elektronisk Identifikationsmiddel - typisk via en Identitetsbroker. Benævnes også som *relying party* på engelsk. Tjenesteudbyderen aftager den elektroniske identitet og stiller typisk krav om et bestemt sikringsniveau, før der kan opnås adgang til tjenesten. Eksempler tjenester kan være Borger.dk, Virk.dk eller kommunale sagsbehandlingssystemer. NSIS stiller ikke krav til Tjenesteudbydere.

Nedenstående figur illustrerer relationerne mellem de vigtige begreber Entitet, Identitet og Elektronisk Identifikationsmiddel:

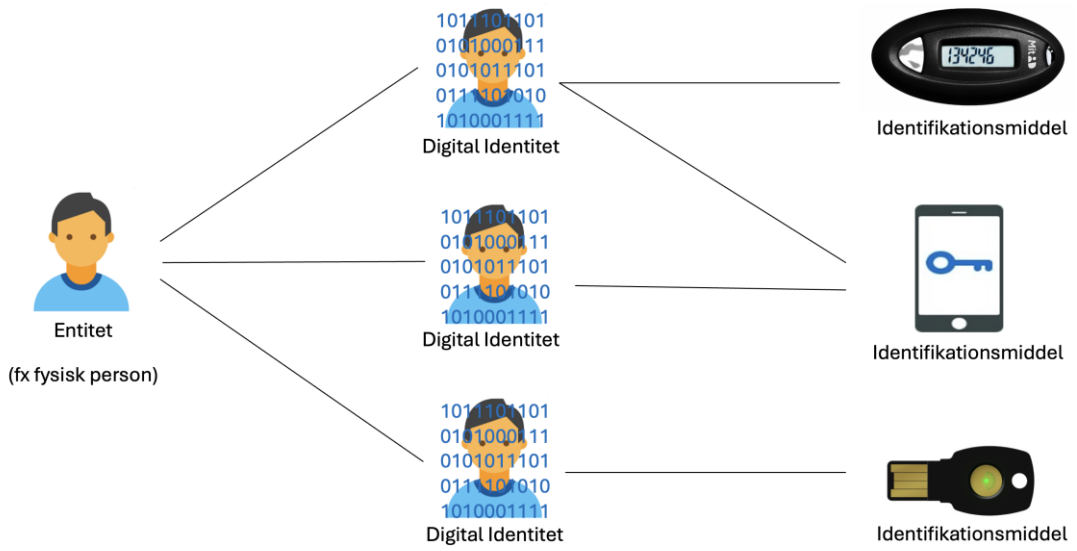


Figur 1: Relation mellem begreberne Entitet, Identitet og Elektronisk Identifikationsmiddel

Et samlet Elektronisk Identifikationsmiddel benyttes af en Entitet til Autentifikation på et givet Sikringsniveau, mens det er de enkelte Elektronisk Identifikationsmidler, i det samlede Elektronisk Identifikationsmiddel, som bliver udstedt og administreret i Elektroniske Identifikationsmidlers livscyklus. Eksempelvis kan kodeord og nøgleviser i MitID administreres separat fra hinanden med deres egen livscyklus.

Den overordnede term "Elektronisk Identifikationsmiddel" refererer således både til det samlede Elektroniske Identifikationsmiddel og de enkelte Elektronisk Identifikationsmidler - afhængig af om konteksten er anvendelse (Autentifikation) eller udstedelse / administration.

Nedenstående figur illustrerer relationen mellem begreberne Entitet, Identitet og Identifikationsmiddel:



Figur 2: Grundbegreber

1.7 Kravopfyldelse

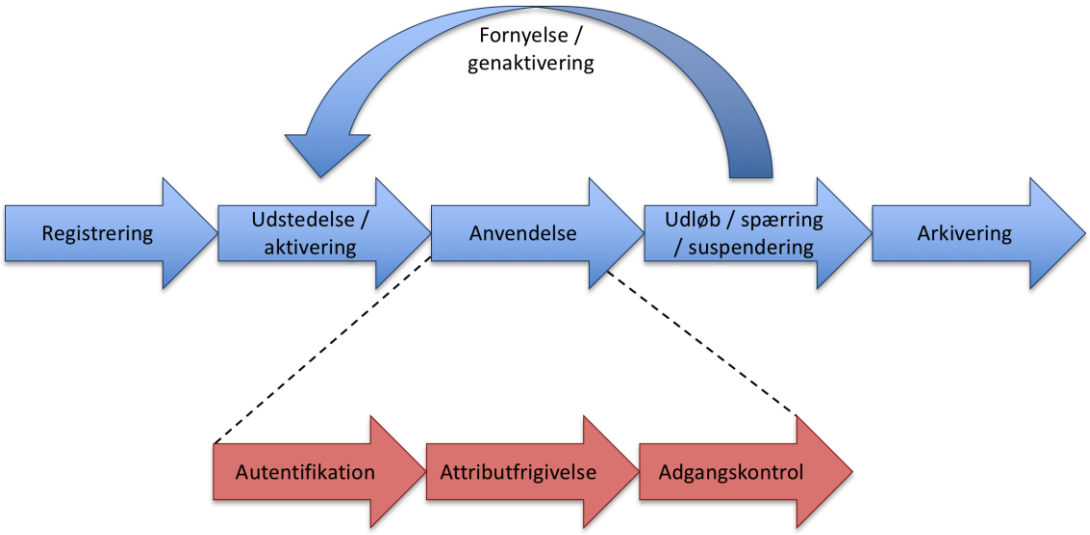
Når der til et givet Sikringsniveau er angivet flere krav, skal samtlige krav til Sikringsniveauet opfyldes med mindre andet eksplicit er anført. Herudover skal krav på lavere Sikringsniveauer altid opfyldes, så der herved etableres et hierarki og en progression over de tre Sikringsniveauer. Det samlede Sikringsniveau (LoA) dikteres af det mindste Sikringsniveau opnået på de specifikke områder nedenfor. Med andre ord, skal samtlige krav til fx niveau 'Betydelig' opfyldes, før en Elektronisk Identifikationsordning kan siges at leve op til NSIS på niveau 'Betydelig'.

Kravene er i udgangspunktet formuleret resultatbaserede (*outcome-based*), således at de primært sigter på **resultatet** af bestemte kontroller og processer (det ønskede, kvalitative niveau), frem for at diktere **metoden** til at opnå niveauet. Dette er valgt af hensyn til at muliggøre forskellige teknologier, processer, organisering og løsninger, og da dette også er tilgangen i [LOA]. Der er dog afvigelser fra denne tilgang, så reelt er kravene en blanding af flere tilgange.

2 Livscyklus for Elektroniske Identifikations-midler

Kravene i de efterfølgende kapitler retter sig mod forskellige faser af livscyklus for Elektroniske Identifikationsmidler – både i forbindelse med deres registrering, udstedelse og anvendelse. Med henblik på at skabe en forståelsesramme, som disse krav kan indgå i, er det derfor relevant at indlede med et overblik over den samlede livscyklus.

Bemærk, at de enkelte faser i livscyklus kan håndteres af forskellige aktører / tjenester. Som et tænkt, konkret eksempel kan registreringen i MitID -løsningerne ske i samarbejde mellem Borgerservice, CPR-registret og MitID-leverandøren, udstedelsen foretages af MitID leverandøren (på vegne af Digitaliseringsstyrelsen og bankerne), Autentifikationen kan videreformidles af NemLog-in løsningen (i rollen som Identitetsbroker), mens sikkerhedskonteksten og autorisationen kan etableres i Borger.dk ved adgang til en borgerrettet tjeneste.



Figur 3: Livscyklus for et Elektronisk Identifikationsmiddel[2]

Nedenfor findes en kort opsummering af livscyklus for et Elektronisk Identifikationsmiddel:

- *Registrering* - en proces, hvor Entiteten (brugeren) ansøger om et Elektronisk Identifikationsmiddel og Identitetssikringen foretages.
- *Udstedelse* – en proces, hvor et Elektronisk Identifikationsmiddel udstedes og overdrages til Entiteten.

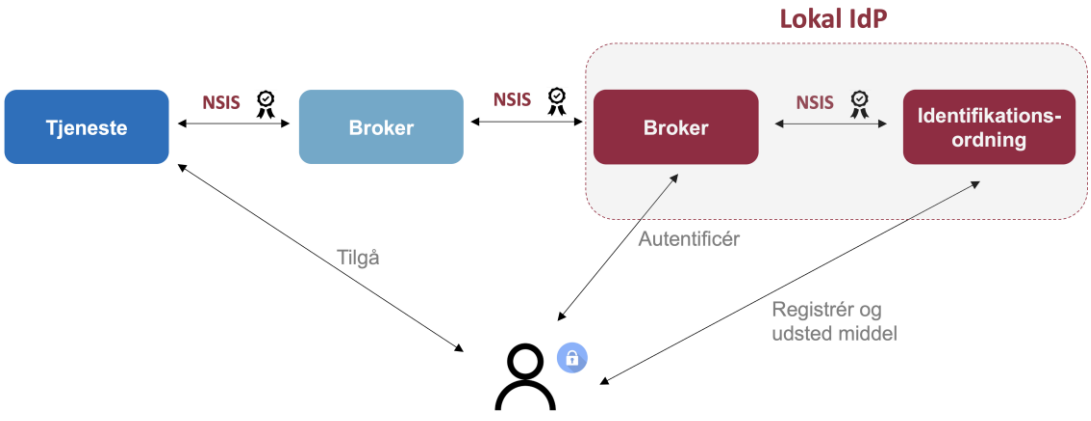
[2] OBS: Hensigten med figuren er at give læseren et overblik over de forskellige stadier - strukturen er afspejlet i kapitlerne med de normative krav, men der er dog ikke en fuldstændig en-til-en relation.

- *Aktivering* - en proces, hvor Entiteten får overdraget sit Elektroniske Identifikationsmiddel og gør det klar til brug.
- *Anvendelse* – de processer, hvor Entiteten anvender sit Elektroniske Identifikationsmiddel til Autentifikation (eller evt. signering) mod online tjenester, som herefter kan danne baggrund for øvrige processer som fx frigivelse af Attributter, adgangskontrol mv.
- *Udløb* – hændelsen hvor et Elektronisk Identifikationsmiddel naturligt udløber og herefter ikke længere kan anvendes. Ikke alle typer Elektroniske Identifikationsmidler har et naturligt udløb.
- *Suspendering* - midlertidig spærring af Elektroniske Identifikationsmiddel (der kan ophæves).
- *Spærring* – en hændelse, hvor et Elektronisk Identifikationsmiddel spærres permanent fx som følge af kompromittering.
- *Arkivering* – en proces, hvor Elektroniske Identifikationsmidler eller relaterede data langtidsarkiveres fx af hensyn til at sikre bevisværdi eller for at kunne dekryptere data mv.

2.1 Tillidskæden for digitale identiteter

Ofte anvendes og formidles digitale identiteter gennem en tillidskæde med flere parter, hvor det er det 'svageste' led i kæden, som afgør det samlede sikringsniveau. Alle led i kæden (pånær tjenesteudbyderen i enden af kæden) skal være omfattet af NSIS, så tjenesten kan stole på kvaliteten af den identitet, der modtages – herunder at den ikke er kompromitteret undervejs.

I eksemplet på figuren nedenfor starter tillidskæden i højre side med udstedelse af et lokalt identifikationsmiddel via en Lokal IdP, der er NSIS anmeldt som Elektronisk Identifikationsordning. Den lokale IdP udstiller en autentifikationstjeneste i form af en ID-tjeneste, der kan autentificere de lokale brugere med de lokalt-udstedte midler. I eksemplet videreformidles autentifikationen via endnu en broker (som fx kunne være NemLog-in), inden den rammer forretningstjenesten, der som tidligere nævnt ikke er NSIS-anmeldt, men blot beslutter, hvilket sikringsniveau der kræves for at opnå adgang.



Figur 4: Eksempel på tillidskæde

3 Krav til Elektroniske Identifikationsmidler

Dette kapitel indeholder normative krav til udstedelse af Elektroniske Identifikationsmidler og deres tilhørende anvendelse ifm. Autentifikation med udgangspunkt i [eIDAS] og [LoA]. Da kravene som sagt er rettet mod forskellige trin i livscyklussen, vil ikke alle krav være relevante for alle ID-tjenester – nedenstående skal altså opfattes som den samlede mængde krav.

3.1 Registreringsprocessen

Dette afsnit stiller krav til Identitetssikring af en ansøger (*identity proofing*), herunder validering og verifikation af Identitet inden udstedelse af Elektroniske Identifikationsmidler. Niveauet af Identitetssikring, som opnås jf. nedenstående tabel, betegnes IAL (Identity Assurance Level). Ved termen 'ansøger' forstås den fysiske person eller juridiske enhed (Entitet), som ønsker at få udstedt et Elektronisk Identifikationsmiddel.

3.1.1 Ansøgning

Nedenstående beskriver kravene til ansøgningsprocessen. Det skal bemærkes, at der ved udstedelse af Elektroniske Identifikationsmidler i virksomheder ikke nødvendigvis foreligger en eksplicit ansøgning, som fx hvis et Elektronisk Identifikationsmiddel udstedes automatisk som en del af ansættelsesprocessen. I disse tilfælde skal kravene opfyldes alligevel.

Sikringsniveau	Krav
Lav	1) Ansøgeren (den kommende bruger) skal gøres bekendt med betingelserne for brugen af udstedte Elektroniske Identifikationsmidler. 2) Ansøgeren skal gøres bekendt med de krævede sikkerhedsforanstaltninger, som har at gøre med brugen af Elektroniske Identifikationsmidler. 3) De data, som er relevante for godtgørelse og kontrol af Identitet, skal indsamles på en pålidelig måde.
Betydelig	4) Ansøgeren skal afkræves accept af betingelser og tilkendegive at have læst dem.
Høj	Som Betydelig.

3.1.2 Verifikation af Identitet (fysiske personer)

Dette afsnit stiller krav til Identitetssikring af fysiske personer. Kravene i nedenstående tabel er møntet på ny-udstedelse baseret på ikke-elektronisk dokumentation.

Generelt er det tilladt at basere identitetssikringen på en Autentifikation med gyldigt Elektronisk Identifikationsmiddel på mindst samme eIDAS- eller NSIS Sikringsniveau, som der ansøges på, og i givet fald bortfalder kravene i tabellen nedenfor. Det Elektroniske Identifikationsmiddel behøver ikke være fra den samme udsteder, men det skal verificeres, at det pågældende Elektroniske Identifikationsmiddel er gyldigt og ikke spærret.

Såfremt det anvendte Elektroniske identifikationsmiddel ikke omfatter alle Personidentifikationsdata, der er nødvendige for udstedelsen af det nye identifikationsmiddel, skal de manglende personidentifikationsdata sikres i henhold til nedenstående krav, og det samlede sikringsniveau justeres i henhold til det lavest opnåede sikringsniveau for alle Personidentifikationsdata.

Sikringsniveau	Krav
Lav	1) Der skal gennemføres en verifikation, og der skal foreligge en beskrivelse af verifikationsprocessen, herunder de forudsætninger, der lægges til grund. 2) Ansøgeren (Entiteten) skal med overvejende sandsynlighed vurderes at være i besiddelse af almindeligt anerkendt dokumentation for sin Identitet. 3) Dokumentationen kan antages at være ægte og gyldig.
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 besiddelse af dette, kan anvendes de samme identifikationsprocesser, som benyttes ved udstedelse af dansk pas eller kørekort. 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. 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. 7) Hvis der gennemføres manuelle kontroller, må disse kun udføres af specielt uddannet personale, der har modtaget relevant instruktion i at verificere ægthed af dokumentation og detektere svindel. 8) Hvis registreringen gennemføres af en anden person end ansøgeren, skal denne være autentificeret på Sikringsniveau Betydelig eller Høj.

Sikringsniveau	Krav
Høj	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. 10) Der er med meget høj sandsynlighed et fysisk match mellem ansøgeren og den præsenterede dokumentation (fx match af billede og underskrift). 11) Hvis registreringen gennemføres af en anden person end ansøgeren, skal denne være autentificeret på Sikringsniveau Høj.

3.1.3 Verifikation af Identitet (juridiske enheder)

Dette afsnit stiller krav til Identitetssikring af juridiske enheder. Kravene i nedenstående tabel er møntet på ny-udstedelse baseret på fysisk eller elektronisk dokumentation.

Verifikation af juridiske enheder er relevant, hvis man udsteder identifikationsmidler til andre organisationer eller medarbejdere i fremmede organisationer[3], herunder hvis man fx leverer en FullService IdP. Her er det således relevant at sikre sig, at man udsteder til (erhvervsbrugere i) den rigtige organisation. Et eksempel på dette er MitID Erhverv løsningen, som udsteder identiteter og/eller identifikationsmidler til (potentielt) alle organisationer med et CVR-nummer. Her sikrer MitID Erhverv's tilslutningsprocesser, at identiteten af organisationen er dokumenteret, og at administratorer er udpeget af ledelsen, inden der kan oprettes brugere og udstedes identifikationsmidler tilknyttet organisationen.

Udsteder man kun identifikationsmidler inden for egen organisation eller koncern, er kravene i dette afsnit ikke relevante; se evt. vejledningen vedr. fællesanmeldelser i afsnit 4.1.7 om anmeldelse og revision.

Generelt er det tilladt at basere identitetssikringen på en Autentifikation med gyldigt Elektronisk Identifikationsmiddel på mindst samme eIDAS- eller NSIS Sikringsniveau, som der ansøges på, og i givet fald bortfalder kravene i tabellen nedenfor. Det Elektroniske Identifikationsmiddel behøver ikke være fra den samme udsteder, men det skal verificeres, at det pågældende Elektroniske Identifikationsmiddel er gyldigt og ikke spærret.

Såfremt det anvendte Elektroniske identifikationsmiddel ikke omfatter alle Personidentifikationsdata, der er nødvendige for udstedelsen af det nye identifikationsmiddel, skal de manglende personidentifikationsdata sikres i henhold til nedenstående krav, og det samlede sikringsniveau justeres i henhold til det lavest opnåede sikringsniveau for alle Personidentifikationsdata.

Sikringsniveau	Krav
Lav	1) Den juridiske enheds eksistens er dokumenteret med et anerkendt bevis (fx registreringsbevis eller tilsvarende) eller ved opslag i CVR-registret. 2) Den juridiske enheds navn, retlige form og entydige registreringsnummer (CVR-nummer) er fastlagt entydigt. 3) Den juridiske enhed er ikke registreret med en status, der afholder den juridiske enhed fra at agere som sådan (herunder konkurs etc.). 4) Det kan antages, at registreringen gennemføres af en person, der er autoriseret til dette af den juridiske enhed. 5) Personen, der gennemfører registreringen, er autentificeret på Sikringsniveau Lav eller højere.

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

Sikringsniveau	Krav
Betydelig	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. 7) Personen, der gennemfører registreringen, er autentificeret på Sikringsniveau Betydelig eller Høj.
Høj	8) Der er gennemført en stærk validering af, at registreringen gennemføres af en person, der er autoriseret til dette af den juridiske enhed. 9) Personen, der gennemfører registreringen, er autentificeret på Sikringsniveau Høj.

3.2 Udstedelse og håndtering af Elektroniske Identifikationsmidler

Nedenstående tabel angiver kravene til Elektroniske Identifikationsmidler på de tre Sikringsniveauer.

3.2.1 Styrke af Elektronisk Identifikationsmiddel

Sikringsniveau	Krav
Lav	1) Det Elektroniske Identifikationsmiddel skal gøre brug af mindst en Autentifikationsfaktor. 2) Det Elektroniske 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.
Betydelig	3) Det Elektroniske Identifikationsmiddel skal gøre brug af mindst to Autentifikationsfaktorer fra forskellige kategorier. 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.
Høj	5) Det Elektroniske Identifikationsmiddel skal være beskyttet mod kopiering og manipulering af angribere med stor Angrebskapacitet. 6) Det Elektroniske Identifikationsmiddel er udformet således, at den person, som det tilhører, kan beskytte det sikkert mod, at andre bruger det.

3.2.2 Levering og aktivering

Nedenstående tabel angiver kravene til levering per Sikringsniveau:

Sikringsniveau	Krav
Lav	1) Det Elektroniske Identifikationsmiddel leveres efter udstedelse via en mekanisme, som gør det muligt at antage, at det kun leveres til den tilsigtede Person.

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

3.2.3 Suspendering, spærring og genaktivering

Nedenstående tabel angiver kravene til suspendering og spærring per Sikringsniveau:

Sikringsniveau	Krav
Lav	1) Det skal være muligt for brugeren/ejeren af et Elektronisk Identifikationsmiddel at suspendere (midlertidigt forhindre anvendelse) og/eller spærre (permanent forhindre anvendelse) hurtigt og effektivt. 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. 3) Reaktivering skal kun finde sted, hvis de samme sikringskrav som forud for udstedelsen fortsat er opfyldt. 4) Udstederen af et Elektronisk Identifikationsmiddel, skal på eget initiativ spærre dette: 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[4] mellem udsteder og ansøger 5) Der gives en kvittering for spærring til brugeren/ejeren af det Elektroniske Identifikationsmiddel, hvis det er muligt.
Betydelig	6) Suspenderings- og spærrefunktion skal være til rådighed døgnet rundt og have en høj grad af tilgængelighed. 7) Udstederen skal spærre Elektroniske Identifikationsmidler, hvis det konstateres, at brugeren/ejeren af det Elektroniske Identifikationsmiddel er ophørt med at eksistere (fx dødsfald for fysisk person eller konkurs for juridisk enhed).
Høj	Som Betydelig.

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

3.2.4 Fornyelse og erstatning

Nedenstående tabel angiver kravene til fornyelse og erstatning pr. Sikringsniveau:

Sikringsniveau	Krav
Lav	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.
Betydelig	Som Lav.
Høj	2) Hvor fornyelsen baseres på en gyldig elektronisk identifikation, skal personidentifikationsdata og eksistens af Entiteten verificeres på ny mod en Autoritativ kilde.

Ovenstående krav sigter mod fornyelse i forbindelse med udløb af et Elektronisk Identifikationsmiddel. Sker fornyelsen inden for det Elektroniske Identifikationsmiddels udløb (fx fordi ejeren har mistet det oprindelige Elektroniske Identifikationsmiddel, eller dette er kompromitteret), kan re-identifikation evt. udelades op til niveau Betydelig, hvis der er stærke kontroller, som sikrer, at det Elektroniske Identifikationsmiddel udstedes til samme Person. Et eksempel kunne være, at man ikke skal starte processen helt forfra, hvis en Person har mistet sit password.

3.3 Anvendelse og Autentifikation

3.3.1 Autentifikationsmekanismer

Nedenstående tabel angiver kravene til autentifikationsmekanismer pr. Sikringsniveau, hvor en Entitet anvender et eller flere Elektroniske Identifikationsmidler i en Autentifikation.

Sikringsniveau	Krav
Lav	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. 3) Autentifikationsmekanismen implementerer sikkerhedskontroller til at efterprøve Elektroniske Identifikationsmidler, således at det er højst usandsynligt, at det er muligt for en angriber med en **øget basal** Angrebskapacitet at gætte, lytte sig til, gengive eller manipulere kommunikationen og på den måde omgå autentifikationsmekanismen.

Sikringsniveau	Krav
Betydelig	4) Frigivelsen af personidentifikationsdata finder sted efter en pålidelig kontrol af Elektroniske Identifikationsmidler og deres gyldighed via en Dynamisk Autentifikationsmekanisme. 5) Autentifikationsmekanismen implementerer sikkerheds-kontroller til at efterprøve Elektroniske Identifikationsmidler, således at det er højst usandsynligt, at det er muligt for en angriber med en **moderat** Angrebskapacitet at gætte, lytte sig til, gengive eller manipulere kommunikationen og på den måde omgå autentifikationsmekanismen.
Høj	6) Autentifikationsmekanismen implementerer sikkerheds-kontroller til at efterprøve Elektroniske Identifikationsmidler, således at det er højst usandsynligt, at det er muligt for en angriber med en **høj** Angrebskapacitet at gætte, lytte sig til, gengive eller manipulere kommunikationen og på den måde omgå autentifikationsmekanismen.

4 Organisatoriske- og tværgående krav

4.1.1 Generelle krav

Nedenstående tabel angiver de generelle krav til organisationer, der leverer ID-tjenester inkl. Identitetsbrokere (se kapitel 6):

Sikringsniveau	Krav
Lav	1) Organisationer, som leverer ID-tjenester beskrevet i dette dokument, skal være en registreret juridisk enhed i EU med en etableret organisation. Organisationen skal leve op til alle krav for de tilbudte tjenester, svarende til de beskrevne processer i Elektroniske Identifikationsmidlers livscyklus (registrering, udstedelse, anvendelse, broker etc.). 2) Dette krav udgår fra revision, se dog afsnit 7.2. 3) Organisationer, som leverer ID-tjenester, er ansvarlige for opfyldelse af forpligtelser, som er overdraget til tredjepart.
Betydelig	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. 5) Private organisationer, som leverer ID-tjenester, skal have en beskrevet termineringsplan, som sikrer en hensigtsmæssig nedlukning eller overtagelse af tredjepart, samt underretning af myndigheder og brugere. Planen skal indeholde detaljer om, hvordan data opbevares, beskyttes og destrueres.
Høj	Som Betydelig.

4.1.2 Oplysningspligt

Nedenstående tabel angiver krav til oplysning:

Sikringsniveau	Krav
Lav	1) Der skal offentliggøres en servicebeskrivelse for Identitetsbrokere og Elektroniske Identifikationsordninger, som beskriver alle relevante betingelser, betalinger for og begrænsninger i brugen af ID-tjenesten. Servicebeskrivelsen skal indeholde en privatlivspolitik, som opfylder kravene i [GDPR]. 2) For Elektroniske Identifikationsordninger skal oplyses om ansvar og forudsætninger for brugere samt Tjenesteudbydere, der forlader sig på et Elektronisk Identifikationsmiddel, i forhold til at opnå et givet Sikringsniveau. Dette omfatter fx sikkerhedsvejledning til brugere. 3) For Elektroniske Identifikationsordninger skal det eksplicit kræves i betingelserne, at brugeren: o alene anvender det Elektroniske Identifikationsmiddel i overensstemmelse med udstederens politikker (herunder politikker for brug og evt. længde af kodeord) samt o ikke overdrager sine Elektroniske Identifikationsmidler til andre samt o giver fyldestgørende og korrekte svar på alle anmodninger om information i ansøgningsprocessen samt o tager rimelige forholdsregler for at beskytte sine Elektroniske Identifikationsmidler (herunder ved evt. sikkerhedskopiering) samt o omgående anmoder om spærring af sine Elektroniske Identifikationsmidler i tilfælde af kompromittering eller mistanke om kompromittering af disse, samt o omgående anmoder om fornyelse af sine Elektroniske Identifikationsmidler, hvis tilhørende Personidentifikationsdata ikke længere er i overensstemmelse med de faktiske forhold (herunder oplysninger afgivet under registreringsprocessen, som indgår i Elektroniske Identifikationsmidler).
Betydelig	Som Lav.
Høj	Som Lav.

4.1.3 Informationssikkerhedsledelse

Nedenstående tabel angiver krav til informationssikkerhedsledelse for Organisationer, der leverer ID-tjenester:

Sikringsniveau	Krav
Lav	1) Organisationer, som leverer ID-tjenester, skal etablere et effektivt ledelsessystem for informationssikkerhed (ISMS) som dækker ID-tjenesten med henblik på at håndtere risici knyttet til informationssikkerhed.
Betydelig	2) Ledelsessystemet for ID-tjenesten skal være i overensstemmelse med principperne i [ISO 27001] standarden. 3) Der skal foreligge en beredskabsplan, som dækker alle væsentlige områder.
Høj	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.

4.1.4 Logning

Nedenstående tabel angiver krav til logning:

Sikringsniveau	Krav
Lav	1) Relevant information skal logges og beskyttes i henhold til gældende lov samt god praksis inden for databeskyttelse og forvaltning. 2) Relevante oplysninger registreres og ajourføres ved hjælp af et effektivt registreringssystem, der tager hensyn til gældende lovgivning og god praksis inden for beskyttelse og opbevaring af data. 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.
Betydelig	Som Lav.
Høj	Som Lav.

4.1.5 Faciliteter og personale

Nedenstående tabel angiver krav til faciliteter og personale:

Sikringsniveau	Krav
Lav	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. 2) Der skal være tilstrækkeligt med personale (evt. via underleverandører) til at drive og vedligeholde tjenesten i henhold til de relevante politikker og procedurer. 3) Driftsfaciliteter skal løbende overvåges for og beskyttes imod skade forvoldt ved miljøkatastrofer, uautoriseret adgang eller andre faktorer, som kan påvirke tjenestens sikkerhed. 4) Områder i driftsfaciliteter indeholdende personlige, kryptografiske eller andre fortrolige oplysninger skal begrænses til autoriseret personale.
Betydelig	5) Det skal kontrolleres, at ledere og medarbejdere, der udfører betroede opgaver, ikke er straffet for en forbrydelse, der gør dem uegnede til at bestride deres hverv, samt at medarbejdere og ledere har tilstrækkelig uddannelse og erfaring. Det samme gælder leverandører og underleverandører. 6) Det skal kunne dokumenteres, hvem der har haft adgang til centrale driftslokaler. 7) Betroede adgange (herunder administratoradgange) i produktionssystemer skal sikres og overvåges.
Høj	8) Det skal sikres, at adgang til og ophold i de centrale driftslokaler videoovervåges. 9) Driftsfaciliteter skal have en perimeterbeskyttelse svarende til [DS 471] eller tilsvarende.

4.1.6 Tekniske kontroller

Nedenstående tabel angiver krav til tekniske kontroller:

Sikringsniveau	Krav
Lav	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. 2) Elektroniske kommunikationskanaler, som benyttes til udveksling af persondata, skal beskyttes mod aflytning, manipulation og genspilning (replay). 3) Adgang til kryptografisk materiale brugt til udstedelse af et Elektronisk Identifikationsmiddel eller Autentifikation skal være begrænset til de roller og applikationer, der har et strengt nødvendigt behov for adgang, og kryptografisk materiale må aldrig gemmes i klar tekst i vedvarende lagringsmedier. 4) Der er indført procedurer, som garanterer, at sikkerheden bevares over tid, og at der er mulighed for at reagere på ændringer i risikoniveau, sikkerhedshændelser og brud på sikkerheden. 5) Alle medier, som indeholder personlige, kryptografiske eller andre fortrolige eller følsomme oplysninger, lagres, transporteres og bortskaffes på en sikker måde.
Betydelig	6) Følsomt kryptografisk materiale anvendt til udstedelse af et Elektronisk Identifikationsmiddel og Autentifikation, som lagres vedvarende, skal beskyttes mod manipulation. 7) Der må ikke benyttes kryptografiske algoritmer eller protokoller med kendte sårbarheder eller med utilstrækkelige nøglelængder.
Høj	Som Betydelig.

4.1.7 Anmeldelse og revision

Elektroniske Identifikationsordninger samt Identitetsbrokere, som ønsker at blive anerkendt på et givet Sikringsniveau under denne standard, anmeldes til Digitaliseringsstyrelsen. Anmelderen er forpligtet til at levere fyldestgørende materiale samt besvare evt. supplerende spørgsmål.

Såfremt den anmeldte løsning opfylder kravene til anmeldelse, optages løsningen på NSIS positivlisten på Digitaliseringsstyrelsens hjemmeside[5]. Først herefter må en løsning påkalde sig overholdelse af NSIS samt påstemple NSIS sikringsniveauer i en autentifikation, der udstedes til tredjepart.

Digitaliseringsstyrelsen påtager sig alene ansvar for at sikre, at formalia omkring opfyldelse af anmeldelse er overholdt, herunder at der foreligger den krævede dokumentation (fx revisionsrapport). Styrelsen påtager sig intet ansvar for, hvorvidt anmeldte løsninger til stadighed opfylder kravene til det angivne Sikringsniveau.

Nedenstående tabel angiver krav til anmeldelse og revision:

[5] https://digst.dk/it-loesninger/standarder/nsis/

Sikringsniveau	Krav
Lav	1) Ved anmeldelse af en Elektronisk Identifikationsordning og/eller Identitetsbroker til Digitaliseringsstyrelsen skal der redegøres for den tekniske og sikkerhedsmæssige udformning samt Sikringsniveau og navn. 2) Ved anmeldelse af en Elektronisk Identifikationsordning og/eller Identitetsbroker til Digitaliseringsstyrelsen skal der anvendes selvdeklarering. Anmelderen indestår herved selv for, at kravene til det angivne Sikringsniveau (Lav) er opfyldt. 3) Ved anmeldelse på niveau Lav skal der være udført intern revision, som omfatter alle nødvendige områder af de tilbudte tjenester med henblik på at sikre overholdelse af relevante krav og politikker. Anmelderen skal på sikringsniveau Lav endvidere årligt indsende en ledelseserklæring som bekræfter, at den oprindelige anmeldelse fortsat er retvisende og løsningen er aktiv – eller alternativt opdatere sin anmeldelse eller bede om afnotering fra listen over anmeldte løsninger. Såfremt der gennemføres ekstern revision ift. sikringsniveau Betydelig eller Høj, bortfalder kravet til intern revision.
Betydelig	4) Ved anmeldelse på niveau Betydelig anvendes en revisionserklæring fra en uafhængig, godkendt[6] revisor med relevante kompetencer indenfor it-revision eller et akkrediteret overensstemmelsesvurderingsorgan (jf. eIDAS artikel 3, stk. 1, nr. 18). Denne skal bekræfte, at løsningens tekniske og sikkerhedsmæssige udformning er gennemgået, at kravene i denne standard er overholdt af løsningen på det angivne Sikringsniveau, og at der er implementeret processer for løbende at sikre, at det angivne Sikringsniveau opretholdes. Anmeldelsen suppleres med en ledelseserklæring underskrevet af en tegningsberettiget, hvoraf det fremgår, at alle relevante krav er opfyldt og fornødne processer for opretholdelse er implementeret. Der skal årligt indsendes en ny revisionserklæring, som bekræfter, at kravene til stadighed opfyldes. 5) Revisionserklæringen skal udarbejdes i henhold til seneste vejledningen til anmeldelses og revisionsprocessen [REV]. Anmelder og revisor udfylder det tilhørende kontrolskema (eller tilsvarende[7]) for niveau Betydelig.
Høj	6) Revisionserklæringen skal udarbejdes i henhold til seneste vejledningen til anmeldelses og revisionsprocessen [REV]. Anmelder og revisor udfylder det tilhørende kontrolskema (eller tilsvarende) for niveau Høj.

[6] Godkendt revisor anvendes som en samlet betegnelse for både en statsautoriseret og en registreret revisor. Revisor skal have relevante faglige kompetencer, se vejledningen for yderligere detaljer.

[7] Hvis revisor i sin erklæring i særskilt afsnit indarbejder kontroller, revisionshandlinger som fremgår af Kontrolskemaet, er dette således tilstrækkeligt.

Bemærk at kravet om type 2 erklæringer indebærer, at organisationen skal kunne dokumentere, at kontrollerne udføres løbende i løbet af perioden, herunder eksempelvis at der er sporbarhed for oprettelser / nedlæggelser af brugere.

5 Elektroniske Identifikationsmidler associeret til juridiske enheder

Dette kapitel omhandler krav til Elektroniske Identifikationsmidler for 'fysiske personer associeret med en juridisk enhed' – dvs. i daglig tale *erhvervsbrugere*. Begrebet dækker bl.a. medarbejdere ansat i en virksomhed, men også andre relationer, hvor der ikke foreligger et ansættelsesforhold. En associering kan udmøntes ved udstedelse af et nyt, selvstændigt Elektronisk Identifikationsmiddel (fx særskilt MitID Identifikationsmiddel i MitID Erhverv), men kan også bestå af en logisk tilknytning mellem en fysisk person og en juridisk enhed uden udstedelse af nye Elektroniske Identifikationsmidler (fx ved opmærkning af den fysiske person, hvor den fysiske person benytter sit personlige Elektroniske Identifikationsmiddel i en erhvervsmæssig kontekst). Nedenfor angives specifikke krav til håndtering af livscyklus for associeringer.

5.1 Udstedelse af Elektroniske Identifikationsmidler

Når der udstedes et Elektronisk Identifikationsmiddel til fysiske personer associeret med en juridisk enhed anvendes de samme krav som beskrevet i kapitel 3 for fysiske personer. Med andre ord gælder alle krav fra kapitel 3, medmindre andet eksplicit fremgår nedenfor.

Ved en genudstedelse kan man ud fra en risikovurdering genbruge data fra en tidligere Identitetssikringsproces, såfremt der etableres kontroller, der minimerer risici i den forbindelse - fx ved at nærmeste leder siger god for medarbejderens Identitet.

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

Følgende vilkår gælder for forbindelser mellem fysiske personer og juridiske enheders Elektroniske Identifikationsmidler (»forbindelse«):

Sikringsniveau	Krav
Lav	1) Det skal være muligt at suspendere og/eller ophæve en forbindelse for begge parter. 2) Den juridiske enhed har (via en administrator) ret til at udføre suspendering eller ophævning, hvilket evt. kan indbefatte suspendering / spærring af et tilhørende Elektroniske Identifikationsmiddel, hvis forbindelsen er etableret herigennem. 3) Det skal sikres, at forbindelsen fjernes, når associationen mellem den juridiske enhed og fysiske person ophører. Et eksempel kan være, at medarbejdere ikke længere er ansat eller ikke længere har et arbejdsbetinget behov for at være associeret, eller i tilfælde af den juridiske enheds konkurs eller likvidering. 4) Godtgørelse af Identiteten af den fysiske person, der handler på vegne af den juridiske enhed, kontrolleres på Sikringsniveau »lav« eller derover. 5) Forbindelsen kan oprettes på grundlag af opslag i CVR-registret eller anden Autoritativ Kilde, herunder den juridiske enhed selv. 6) Den fysiske person er ikke registreret af en Autoritativ Kilde med en status, der afholder den fysiske person fra at handle på vegne af den juridiske enhed.
Betydelig	7) Sikringen af Identiteten af den fysiske person, der handler på vegne af den juridiske enhed, foretages på Sikringsniveau »Betydelig« eller »Høj«. 8) Forbindelsen er etableret under kontrol af den juridiske enhed fx via en udpeget administrator eller via oplysninger fra en Autoritativ kilde. 9) Procedurer til grund for etableringen af forbindelsen er underlagt revision. 10) Forbindelsen er blevet kontrolleret på grundlag af et entydigt identifikationsnummer (fx CVR-nummer), der repræsenterer den juridiske enhed, og som bruges i dansk virksomhedsregistrering, og på grundlag af oplysninger, der entydigt repræsenterer den fysiske person, fra en Autoritativ kilde. 11) Den fysiske person og juridiske enhed notificeres om etablering af forbindelsen.
Høj	12) Sikringen af Identiteten af den fysiske person, der er knyttet til en juridisk enhed, kontrolleres på Sikringsniveau »Høj«.

6 Krav til Identitetsbrokere

Dette kapitel opstiller en række krav til såkaldte "Identitetsbrokere", som er en speciel slags ID-tjeneste, der videreformidler en Autentifikation til en tredjepart ved at udstede og signere et såkaldt Security Token for en Elektronisk Identitet. En broker udstiller med andre ord en autentifikationsservice og indgår dermed i den 'tillidskæde', som (eksterne) modtagere af en autentifikation ('relying parties') skal stole på. I tekniske sammenhænge anvendes ofte betegnelserne '*Identity Providers*' eller '*Security Token Services*'. Som eksempler kan nævnes den fællesoffentlige NemLog-in løsning, der udsteder SAML Assertions til offentlige tjenesteudbydere på baggrund af eksempelvis en MitID autentifikation. Et andet eksempel er lokale 'Identity Providere' (Lokal IdP), der tilbyder autentifikation og føderation af fx medarbejdere i en kommune på baggrund af en autentifikation med et lokalt udstedt Elektronisk Identifikationsmiddel.

Organisationer, som leverer Identitetsbrokere, skal generelt overholde organisatoriske krav angivet i kapitel 4 på det Sikringsniveau, som Identitetsbrokeren klassificeres til. Sikringsniveauet for en Identitetsbroker betegnes *FAL (Federation Assurance Level).*

Ud over de organisatoriske krav i kapitel 4 gælder flg. specifikke krav for Identitetsbrokere:

Sikringsniveau	Krav
Lav	1) Security tokens må kun udstedes umiddelbart efter a) forudgående, succesfuld Autentifikation, b) på baggrund af en gyldig, autentificeret session (Single Sign-On), eller c) ved omveksling af et gyldigt security token fra en anden Identitetsbroker, der er etableret et tillidsforhold til. 2) Det aktuelle Sikringsniveau skal angives som en oplysning i det udstedte token (LoA), således at modtageren af tokens direkte kan aflæse dette. Sikringsniveauet i et token opgøres som mindsteværdien af Sikringsniveauet for Autentifikationen (jf. afsnit 2-5), brokerens eget Sikringsniveau (FAL) jf. afsnit 4 og 6, samt Sikringsniveauerne for evt. Identitetsbrokere, der er benyttet som underleverandører i den konkrete Autentifikation. Det er dermed det laveste Sikringsniveau i autentifikationskæden, som bliver det resulterende Sikringsniveau. 3) Tokens skal signeres med brokerens private nøgle og må kun udveksles over krypterede kanaler. 4) Brokerens private nøgle, der underskriver security tokens, skal beskyttes mod uautoriseret adgang. 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). 6) Sessioner med Identitetsbrokere skal beskyttes mod overtagelse. 7) Alle forespørgsler til Identitetsbrokeren og alle svar på disse skal skrives til en integritetsbeskyttet log.

Sikringsniveau	Krav
Betydelig	8) Anvendere af Identitetsbrokere, der aftager Autentifikation, skal i deres forespørgsel kunne fravælge Single Sign-On, hvis der fra tjenestens side er ønske om at gennemtvinge en Autentifikation med aktiv brugerinvolvering (dvs. fravælge SSO). 9) Tokenet skal være begrænset til en eller flere specifikke tjenester, og disse skal fremgå eksplicit i tokenet (fx som *Audience Restriction*). 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. 11) Brokerens private nøgle, der underskriver security tokens, skal beskyttes mod uautoriseret adgang både fra interne og eksterne, og der skal etableres eksplicitte procedurer for nøglehåndtering, som dækker den fulde livscyklus. 12) For nationale tjenester[8] skal brokerens private nøgle, der underskriver security tokens, placeres i 'tamper-resistent' kryptografisk hardware der opfylder kravene til [FIPS 140-2] level 3 eller tilsvarende.
Høj	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. 14) Den private nøgle skal genereres i hardware og må ikke kunne eksporteres i klar tekst.

[8] Tjenester som agerer som brokere for vilkårlige private borgere eller personer associeret til vilkårlige virksomheder (fx FullService IdP'er). En broker som kun håndterer en/få virksomheders eller myndigheders egne lokale brugere anses ikke som national, og derfor gælder kravet ikke for disse.

7 Governance

I dette kapitel beskrives regler for Elektroniske Identifikationsordninger samt Identitetsbrokere, der ønsker at gøre brug af NSIS.

7.1 Ejerskab og vedligeholdelse af standarden

I lighed med OCES-certifikatpolitikkerne er denne standard udarbejdet af Digitaliseringsstyrelsen ligesom den administreres og vedligeholdes af Digitaliseringsstyrelsen som en fællesoffentlig standard.

Større ændringer i standarden gennemføres med inddragelse af stat, kommuner og regioner og på baggrund af en bred offentlig høring. Digitaliseringsstyrelsen kan dog umiddelbart foretage nødvendige sikkerhedsmæssige tilpasninger.

Dokumentet versioneres, og nye udgaver publiceres på https://digst.dk/it-loesninger/standarder/nsis/

Ved hver udgivelse af opdatering af dette dokument, vil det samtidig blive offentliggjort, hvor lang en frist anvenderne har til at overholde nye / ændrede krav. Udgangspunktet er, at der normalt er mindst 6 måneders frist, medmindre sikkerhedsmæssige forhold kræver kortere implementeringsfrist.

7.2 Ophør og opfølgning

En organisation, der har anmeldt en Elektronisk Identifikationsordning eller Identitetsbroker til Digitaliseringsstyrelsen, er forpligtet til af egen drift straks at meddele Digitaliseringsstyrelsen, hvis et eller flere krav i denne standard ikke længere opfyldes, hvis en ID-tjeneste planlægges at ophøre, eller hvis Sikringsniveauet ønskes ændret. Ved ophør er anmelder forpligtet til en afsluttende revision – de nærmere detaljer er beskrevet i vejledningen til anmeldelses- og revisionsprocessen [REV].

Digitaliseringsstyrelsen kan til enhver tid fratage en organisation retten til at henvise til denne standard samt fjerne den Elektroniske Identifikationsordning eller Identitetsbroker fra positivlisten over anmeldte løsninger, såfremt denne ikke efterlever kravene i standarden. Hvis en organisation enten fratages muligheden for anvendelse af NSIS eller af egen drift ophører med anvendelsen, skal organisationen så vidt muligt notificere sine tjenesteudbydere og brugere om dette.

Digitaliseringsstyrelsen er endvidere berettiget til at rette henvendelse til en anmelder med henblik på afklaringer eller supplerende redegørelser, såfremt tilsynet bliver opmærksom på forhold af væsentlig betydning for NSIS-anmeldelsen. En anmelder skal loyalt og effektivt medvirke til besvare sådanne henvendelser, og manglende samarbejde kan i yderste konsekvens resultere i afnotering fra positivlisten.

7.3 Ansvar og forsikring

Anmelderen af en Elektronisk Identifikationsordning eller Identitetsbroker bærer det fulde ansvar for at kravene beskrevet i denne standard er opfyldt. Derudover forventes de at overholde relevant lovgivning.

Elektroniske Identifikationsordninger eller Identitetsbrokere på Sikringsniveau Betydelig eller Høj skal påtage sig erstatningsansvar efter dansk rets almindelige regler overfor indehavere af Elektroniske Identifikationsmidler samt tjenester, der forlader sig på et Elektronisk Identifikationsmiddel (*relying parties*), såfremt tabet skyldes:

- at oplysninger i udstedte Elektroniske Identifikationsmidler eller Security Tokens er forkerte på tidspunktet for udstedelsen eller manglende spærring på baggrund af gyldig anmodning
- at security tokens udstedes i strid med kravene til Identitetsbrokere i denne standard,
- manglende umiddelbar spærring eller suspension af et Elektronisk Identifikationsmiddel efter anmodning om spærring/suspension,
- alvorlige sikkerhedsbrud som følge af, at sikkerhedskrav ikke er opfyldt,

medmindre det kan godtgøres, at der ikke er handlet uagtsomt eller forsætligt.

Anmelderen udformer selv sine aftaler m.v. med sine medkontrahenter og er berettiget til at søge at begrænse sit ansvar i forholdet mellem sig og sine medkontrahenter i det omfang, at disse medkontrahenter er erhvervsdrivende eller offentlige myndigheder. Anmelderen er ikke berettiget til at søge at begrænse sit ansvar i forhold til private borgere, som medkontrahenter, udover hvad der fremgår af denne standard.

Digitaliseringsstyrelsen påtager sig intet erstatningsansvar for anmeldte løsninger og deres udformning i forbindelse med publicering.

Anmeldere af Elektroniske Identifikationsordninger eller Identitetsbrokere på niveau Betydelig og Høj skal have evne til at bære erstatningsansvar, hvilket fx opnås gennem forsikringsordninger (evt. selvforsikringsordninger for offentlige myndigheder).

7.4 Omkostninger

Alle omkostninger til overholdelse af kravene i standarden afholdes af anmelderen.

7.5 Deling af sikkerhedshændelser

Anmeldte Elektroniske Identifikationsordninger samt Identitetsbrokere på niveau Betydelig eller Høj skal af egen drift dele alvorlige sikkerhedshændelser med Digitaliseringsstyrelsen samt andre relevante myndigheder som fx Center for Cybersikkerhed. Dette sker ved indrapportering til NSIS-tilsynet hos Digitaliseringsstyrelsen, når der optræder alvorlige sikkerhedshændelser – herunder ved begrundet mistanke om, at et eller flere krav i standarden ikke længere overholdes, og/eller at en kontrol er kompromitteret. ID-tjenesteyderen skal ligeledes være til rådighed for en opfølgende dialog samt afklaring af evt. spørgsmål fra Digitaliseringsstyrelsen. I fald en sikkerhedshændelse påvirker brugere eller andre tjenester (*relying parties*), skal disse informeres, og relevante modforanstaltninger skal træffes som fx spærring af et Elektronisk Identifikationsmiddel mv.

Den Europæiske Unions Agentur for Net- og Informationssikkerhed (ENISA) har udarbejdet retningslinjer for incident rapportering (se [ENISA]), som der skal tages udgangspunkt i.

8 Referencer

[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 27001:2022 - Information technology -- Security techniques -- Information security management systems -- Requirements".

[ISO29115] "ISO/IEC 29115:2022 Information technology -- Security techniques -- Entity authentication assurance framework". https://www.iso.org/standard/45138.html

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

elektronisk identifikation og tillidstjenester til brug for elektroniske transaktioner på det indre marked".

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

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

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

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

[LOA-VEJL] "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

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

[VEJL] "Vejledning til NSIS – version 2.5", Digitaliseringsstyrelsen https://digst.dk/it-loesninger/standarder/nsis/

[LOV] "Lov om MitID og NemLog-in" https://www.retsinformation.dk/eli/lta/2021/783