

National Standard for
Identiteters Sikringsniveauer (NSIS)
Version 2.0

Udgivet: 05.10.2018

| | | |
|----------|--|-----------|
| 1 | INDLEDNING | 4 |
| 1.1 | FORORD | 4 |
| 1.2 | INTRODUKTION | 4 |
| 1.3 | FORMÅL OG SCOPE | 4 |
| 1.4 | EKSEMPLER PÅ ID-TJENESTER OG SIKRINGSNIVEAUER | 5 |
| 1.5 | TERMINOLOGI | 6 |
| 1.6 | KRAVOPFYLDELSE | 12 |
| 2 | LIVSCYKLUS FOR ELEKTRONISKE IDENTIFIKATIONSMIDLER..... | 13 |
| 3 | KRAV TIL ELEKTRONISKE IDENTIFIKATIONSMIDLER | 15 |
| 3.1 | REGISTRERINGSPROCESSEN | 15 |
| 3.1.1 | Ansøgning..... | 15 |
| 3.1.2 | Verifikation af Identitet (fysiske personer) | 15 |
| 3.1.3 | Verifikation af Identitet (juridiske personer) | 16 |
| 3.2 | UDSTEDELSE OG HÅNDTERING AF ELEKTRONISKE IDENTIFIKATIONSMIDLER | 17 |
| 3.2.1 | Styrke af Elektronisk Identifikationsmiddel | 17 |
| 3.2.2 | Levering og aktivering | 18 |
| 3.2.3 | Suspendering, spærring og genaktivering..... | 18 |
| 3.2.4 | Fornyelse og erstatning..... | 19 |
| 3.3 | ANVENDELSE OG AUTENTIFIKATION..... | 19 |
| 3.3.1 | Autentifikationsmekanismer | 19 |
| 4 | ORGANISATORISKE- OG TVÆRGAÆNDE KRAV..... | 21 |
| 4.1.1 | Generelle krav | 21 |
| 4.1.2 | Oplysningspligt | 21 |
| 4.1.3 | Informationssikkerhedsledelse | 22 |
| 4.1.4 | Dokumentation og registerføring..... | 22 |
| 4.1.5 | Faciliteter og personale | 23 |
| 4.1.6 | Tekniske kontroller | 23 |
| 4.1.7 | Anmeldelse og revision..... | 24 |
| 5 | ELEKTRONISKE IDENTIFIKATIONSMIDLER ASSOCIERET TIL JURIDISKE PERSONER | 26 |
| 5.1 | UDSTEDELSE AF ELEKTRONISKE IDENTIFIKATIONSMIDLER | 26 |
| 5.2 | BINDING (ASSOCIERING) MELLEM ELEKTRONISKE IDENTIFIKATIONSMIDLER FOR FYSISKE OG JURIDISKE PERSONER..... | 26 |
| 6 | KRAV TIL IDENTITETSBROKERE | 28 |
| 7 | GOVERNANCE | 30 |
| 7.1 | EJERSKAB OG VEDLIGEHOLDELSE AF STANDARDEN | 30 |



DIGITALISERINGSSTYRELSEN

| | | |
|-----|-------------------------------------|----|
| 7.2 | OPHØR OG FRATAGELSE | 30 |
| 7.3 | ANSVAR OG FORSIKRING | 30 |
| 7.4 | OMKOSTNINGER | 31 |
| 7.5 | DELING AF SIKKERHEDSHÆNDELSER | 31 |
| 8 | REFERENCER..... | 32 |

1 Indledning

1.1 Forord

Dette dokument indeholder en 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, akkreditering 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 vejledning til standarden [VEJL], som uddyber kravene gennem forklaringer og eksempler, samt revisionsinstrukser, som benyttes ved anmeldelse (se afsnit 4.1.7 for flere detaljer).

1.2 Introduktion

Nærværende standard definerer krav til styrken af en autentifikationsproces, den underliggende Identitetssikring og 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 egen-skab.

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 i denne version, 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 [TU-LoA], 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, idet mange faktorer har indflydelse på tilliden til digitale Identiteter og ID-tjenester.

1.3 Formål og scope

Denne standard er gældende for nationale, fællesoffentlige Elektroniske Identifikationsordninger og Identitetsbrokere, der håndterer identiteter for fysiske personer, juridiske personer og fysiske personer associeret med en juridisk person (herunder medarbejdere). Den er gældende for 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 identitetshåndte-

ring for enheder/devices og Internet of Things på nuværende tidspunkt ikke omfattet af standarden. 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, konfidentialitet 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 ligger ikke inden for rammerne af denne standard at beskrive yderligere forhold omkring tjenestudbyderes ansvar i forbindelse med informationssikkerhed og valg af Sikringsniveau for autentificerede brugere, der tilgår deres forretningstjeneste:

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. Dette reguleres derfor ikke i NSIS. Der kan i denne forbindelse henvises til publikationen [TU-LoA], der giver eksempler og vejledning til tjenestudbydere 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.

1.4 Eksempler på ID-tjenester og Sikringsniveauer

| | |
|------------------------------------|--|
| <i>MitID og NemLog-in 3</i> | NemLog-in og MitID løsninger vil arbejde med en større differentiering mellem forskellige typer Elektroniske Identifikationsmidler og identitetssikringsprocesser, og benytter NSIS som referenceramme til at beskrive Sikringsniveauerne for disse. |
| <i>Private ID-tjenester</i> | Standarden definerer betingelserne for et kendt Sikringsniveau, således at private ID-tjenester vil kunne vurderes i forhold til anvendelse i offentligt regi. |

| | |
|--|---|
| <i>Kommunal Identity Provider</i> | I den fælleskommunale rammearkitektur agerer den enkelte kommune som Identity Provider (Identitetsbroker) og udsteder af Elektroniske Identifikationsmidler for egne medarbejdere. På den baggrund vil en medarbejders lokale log-in til et lokalt domæne kunne blive fødereret til eksterne, fælleskommunale systemer. Kommunerne har forskellige "identity proofing" processer og forskellige Elektroniske Identifikationsmidler. Her giver NSIS en ramme med standardiserede krav at måle den enkelte kommune op imod. |
| <i>Sundhedsområdet (Security Token Services)</i> | 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. |
| <i>Uddannelsesområdet</i> | 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 vil kunne danne en fælles ramme for tillid til disse. |
| <i>Udenlandske Elektroniske Identifikationsmidler</i> | 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 tillidsrammewærk, der definerer et antal kendte Sikringsniveauer. |

1.5 Terminologi

Nedenfor er de vigtigste begreber beskrevet. I dokumentet 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 sikker- |
|-----------------------|--|

¹ Billetudstedere som giver adgang til sundhedstjenester.



DIGITALISERINGSSTYRELSEN

| | |
|---------------------------------|---|
| | hedspolitik. |
| 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 | <p>En egenskab ved et Elektronisk Identifikationsmiddel, der binder det til Entiteten, og som kan være i kategorierne:</p> <p>a) »indehaverbaseret autentifikationsfaktor«: en autentifikationsfaktor, som Entiteten skal bevise at være i besiddelse af (fx en fysisk enhed)</p> <p>b) »vidensbaseret autentifikationsfaktor«: en autentifikationsfaktor, som Entiteten skal bevise at have kendskab til (fx et kodeord)</p> <p>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)</p> <p>Et Elektronisk Identifikationsmiddel kan have en eller flere faktorer.</p> |
| 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 | <p>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.</p> <p>I dette dokument anvendes begreberne <i>basalt</i>, <i>moderat</i> og <i>højt</i> om forskellige angrebsstyrker. Terminologien er taget fra [ISO15408] som kan konsulteres for yderligere beskrivelser.</p> |
| 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 be- |



DIGITALISERINGSSTYRELSEN

| | |
|---|--|
| | siddelse 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 <i>replay</i> -angreb. |
| Elektronisk Identifikationsmiddel | <p>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.</p> <p>Et <i>samlet</i> Elektronisk Identifikationsmiddel består af ét eller flere elementer, der hver især er et <i>enkelt</i> 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.</p> <p>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 <i>bindingen</i> mellem en Identitet og en eller flere 'Authenticators'.</p> <p>Sikringsniveauet for et samlet Elektronisk Identifikationsmiddel betegnes AAL (<i>Authenticator Assurance Level</i>) - se begrebet Sikringsniveau for flere detaljer om AAL samt forklaring og eksempler under tabellen med begreber.</p> |
| Elektronisk Identifikationsordning | <p>Et samlet system til elektronisk identifikation under hvilket der udstedes Elektroniske Identifikationsmidler til fysiske eller juridiske personer, og/eller fysiske personer, der repræsenterer juridiske personer. 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.</p> <p>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.</p> |
| Entitet | En fysisk eller juridisk person, 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. |



DIGITALISERINGSSTYRELSEN

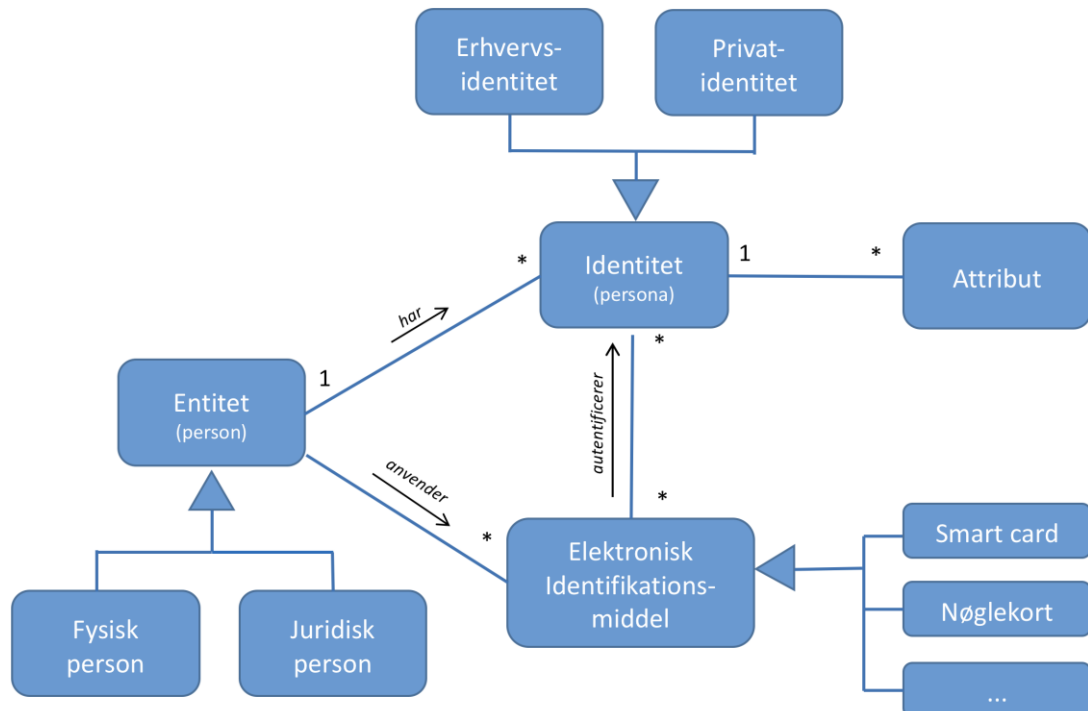
| | |
|----------------------------------|--|
| Identitet (Elektronisk) | En digital persona repræsenteret ved et sæt af attributter, som fx kan repræsentere en fysisk person (privatidentitet), en juridisk person (virksomhedsidentitet), eller en fysisk person, der er associeret med en juridisk person (fx erhvervsidentitet). En Identitet <i>kan</i> 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 broderen 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 <i>trusted third party</i>) fra forretnings-tjenester, 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 person) efterprøves. Processen benævnes ' <i>identity proofing</i> ' på engelsk. |
| ID-tjeneste | <p>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.</p> <p>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.</p> <p>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).</p> |
| Person | En fysisk eller juridisk person. |
| Personidentifikationsdata | Et sæt af data, der gør det muligt at fastslå Identiteten af en fysisk eller juridisk person (dvs. som identificerer en Entitet entydigt). |
| Sikringsniveau (LoA) | Graden af tillid til en autentificeret Identitet (på engelsk " <i>Level of Assurance</i> ") og ofte benævnt <i>autenticitetsSikrings-</i> |



DIGITALISERINGSSTYRELSEN

| | |
|--|--|
| | <p><i>niveau</i>. 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).</p> <p>Det overordnede Sikringsniveau (LoA) kan dekomponeres i flere underbegreber:</p> <p>IAL (<i>Identity Assurance Level</i>) beskriver styrken af Identitetssikringsprocessen. Ved vurderingen gælder kravene i afsnit 3.1, kapitel 5 samt de generelle krav i kapitel 4.</p> <p>AAL (<i>Authenticator Assurance Level</i>) 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.</p> <p>FAL (<i>Federation Assurance Level</i>) 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.</p> |
|--|--|

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 nøglekort i NemID 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.

Eksempler:

- **NemID Elektronisk Identifikationsmiddel:** Kombinationen af brugernavn/kodeord og enten et nøglekort, nøgleviser eller nøgleapp udgør et samlet Elektronisk Identifikationsmiddel, mens brugernavn/kodeord, nøglekort, nøgleviser eller nøgleapp hver især er et enkelt Elektronisk Identifikationsmiddel.
- **MitID Elektronisk Identifikationsmiddel:** Kombinationen af det enkelte Elektroniske Identifikationsmiddel "password" og det enkelte Elektroniske Identifikationsmiddel "fysisk device" kan opfattes som et samlet Elektronisk Identifikationsmiddel, som lever op til kravene på Sikringsniveau Betydelig, hvis de enkelte midler hver især indplaceres som et enkelt elektronisk Identifikationsmiddel på Sikringsniveau Lav. Herved kan to enkelte Elektroniske Identifikationsmidler på et lavere Sikringsniveau kombineres til et samlet Elektronisk Identifikationsmiddel på et højere Sikringsniveau.

1.6 Kravopfyldelse

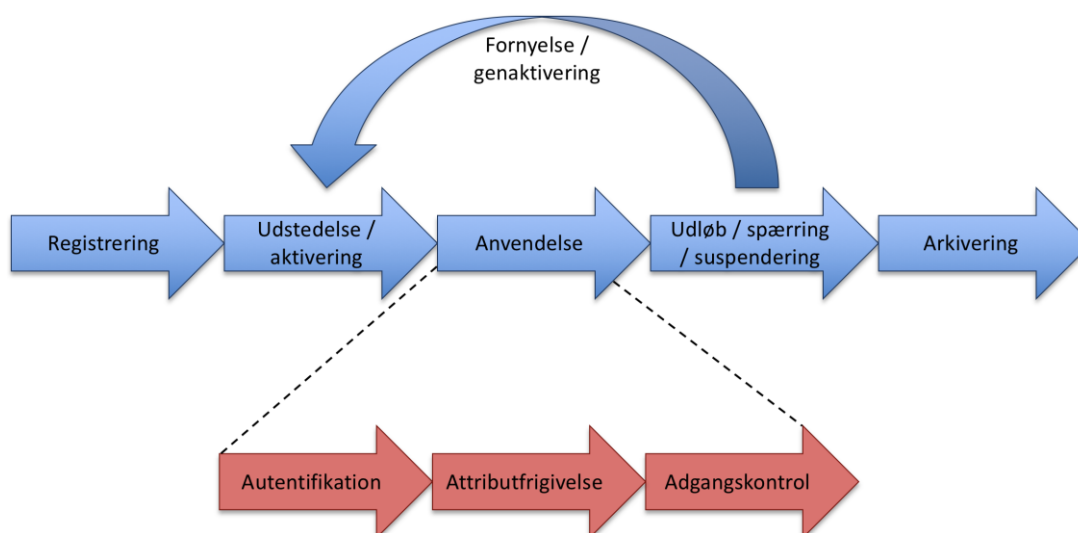
Når der til et givet Sikringsniveau er angivet flere krav, skal samtlige krav til Sikringsniveauet opfyldes, med mindre andet eksplicit er anført. Herudover skal krav på lavere Sikringsniveauer altid opfyldes, så der herved etableres et hierarki og en progression over de tre Sikringsniveauer. Det samlede 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 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 Identifikationsmidler

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/NemID-løsningerne ske i samarbejde mellem Borgerservice, CPR-registret og MitID/NemID leverandøren, udstedelsen foretages af MitID/NemID 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 2: Livscyklus for et Elektronisk Identifikationsmiddel²

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.



DIGITALISERINGSSTYRELSEN

- *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.

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. Niveaue af Identitetssikring, som opnås jf. nedenstående tabel, betegnes IAL (Identity Assurance Level). Ved termen 'ansøger' forstås den fysiske eller juridiske person (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 | <ol style="list-style-type: none">1) Ansøgeren 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. |
| Betydelig | <ol style="list-style-type: none">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 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.

| Sikringsniveau | Krav |
|------------------|---|
| Lav | <ol style="list-style-type: none"> Der skal gennemføres en verifikation, og der skal foreligge en beskrivelse af verifikationsprocessen, herunder de forudsætninger, der lægges til grund. Ansøgeren (Entiteten) skal med overvejende sandsynlighed vurderes at være i besiddelse af almindeligt anerkendt dokumentation for sin Identitet. Dette kan fx være sygesikringskort, pas, kørekort, dåbsattest eller forskudsopgørelse. Dokumentationen kan antages at være ægte og gyldig. |
| Betydelig | <ol style="list-style-type: none"> 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. Dokumentation kontrolleres med henblik på at fastslå, at den er gyldig i henhold til en Autoritativ kilde. 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. Hvis der gennemføres manuelle kontroller, må disse kun udføres af specielt uddannet personale, der har modtaget relevant instruktion i at verificere ægthed af beviser og detektere svindel. Hvis registreringen gennemføres af en anden person end ansøgeren, skal denne være autentificeret på Sikringsniveau Betydelig eller Høj. |
| Høj | <ol style="list-style-type: none"> 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. Der er med meget høj sandsynlighed et fysisk match mellem ansøgeren og den præsenterede dokumentation (fx match af billede og underskrift). Hvis registreringen gennemføres af en anden person end ansøgeren, skal denne være autentificeret på Sikringsniveau Høj. |

3.1.3 Verifikation af Identitet (juridiske personer)

Dette afsnit stiller krav til Identitetssikring af juridiske 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 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.

| Sikringsniveau | Krav |
|------------------|--|
| Lav | <ol style="list-style-type: none"> 1) Den juridiske persons eksistens er dokumenteret med et anerkendt bevis (fx registreringsbevis eller tilsvarende) eller ved opslag i CVR-registret. 2) Den juridiske persons navn, retlige form og entydige registreringsnummer (CVR-nummer) er fastlagt entydigt. 3) Den juridiske person er ikke registreret med en status, der afholder den juridiske person 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 person. 5) Personen, der gennemfører registreringen, er autentificeret på Sikringsniveau Lav eller højere. |
| Betydelig | <ol style="list-style-type: none"> 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. 7) Personen, der gennemfører registreringen, er autentificeret på Sikringsniveau Betydelig eller Høj. |
| Høj | <ol style="list-style-type: none"> 8) Der er gennemført en stærk validering af, at registreringen gennemføres af en person, der er autoriseret til dette af den juridiske person. 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 | <ol style="list-style-type: none"> 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 | <ol style="list-style-type: none"> 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 | <ol style="list-style-type: none"> 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 | <ol style="list-style-type: none"> 1) Det Elektroniske Identifikationsmiddel leveres efter udstedelse via en mekanisme, som gør det muligt at antage, at det kun leveres til den tilsigtede Person. |
| Betydelig | <ol style="list-style-type: none"> 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 | <ol style="list-style-type: none"> 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 forsendelseskkanaler eller funktionsadskillelse. |

3.2.3 Suspendering, spærring og genaktivering

Nedenstående tabel angiver kravene til suspendering og spærring per Sikringsniveau:

| Sikringsniveau | Krav |
|----------------|---|
| Lav | <ol style="list-style-type: none"> 1) Det skal være muligt for ejeren af et Elektronisk Identifikationsmiddel at suspendere (midlertidigt forhindre anvendelse) og/eller spærre (permanent forhindre anvendelse) hurtigt og effektivt. 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: <ul style="list-style-type: none"> ○ hvis der er mistanke om kompromittering eller tab af kontrol over dette, |

| | |
|------------------|--|
| | <ul style="list-style-type: none"> ○ hvis der konstateres fejl i det Elektroniske Identifikationsmiddel (fx forkerte data), ○ hvis der ikke længere foreligger en gyldig aftale³ mellem udsteder og ansøger, eller <p>5) Der gives en kvittering for spærring til ejeren af det Elektroniske Identifikationsmiddel, hvis det er muligt.</p> |
| Betydelig | <p>6) Suspenderings- og spærrefunktion skal være til rådighed døgnet rundt og have en høj grad af tilgængelighed.</p> <p>7) Udstederen skal spærre Elektroniske Identifikationsmidler, hvis det konstateres, at ejeren af det Elektroniske Identifikationsmiddel er ophørt med at eksistere (fx dødsfald for fysisk person eller konkurs for juridisk person).</p> |
| Høj | Som Betydelig. |

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 |
|----------------|------|
|----------------|------|

³ Lovgivning kan træde i stedet for en aftale.



DIGITALISERINGSSTYRELSEN

| | |
|------------------|---|
| Lav | <ol style="list-style-type: none">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. |
| Betydelig | <ol style="list-style-type: none">4) Frigivelsen af personidentifikationsdata finder sted efter en pålidelig kontrol af Elektroniske Identifikationsmidler og deres gyldighed via en Dynamisk Autentifikationsmekanisme.5) Autentifikationsmekanismen implementerer sikkerhedskontroller 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 | <ol style="list-style-type: none">6) Autentifikationsmekanismen implementerer sikkerhedskontroller 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 | <ol style="list-style-type: none"> 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) 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. 3) Organisationer, som leverer ID-tjenester, er ansvarlige for opfyldelse af forpligtelser, som er overdraget til tredjepart. |
| Betydelig | <ol style="list-style-type: none"> 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 | <ol style="list-style-type: none"> 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]. 2) Der skal oplyses om ansvar og forudsætninger for brugere samt 'relying parties', der forlader sig på et Elektronisk Identifikationsmiddel, i forhold til at opnå et givet Sikringsniveau. Dette omfatter fx sikkerhedsvejledning til brugere. 3) Det skal eksplicit kræves i betingelserne, at ejeren: <ul style="list-style-type: none"> o alene anvender det Elektroniske Identifikationsmiddel i overensstemmelse med udstederens politikker (herunder politikker for brug og evt. længde af kodeord) samt |



DIGITALISERINGSSTYRELSEN

| | |
|------------------|---|
| | <ul style="list-style-type: none">○ ikke overdrager sine Elektroniske Identifikationsmidler til andre samt○ giver fyldestgørende og korrekte svar på alle anmodninger om information i ansøgningsprocessen samt○ tager rimelige forholdsregler for at beskytte sine Elektroniske Identifikationsmidler (herunder ved evt. sikkerhedskopiering) samt○ omgående anmoder om spærring af sine Elektroniske Identifikationsmidler i tilfælde af kompromittering eller mistanke om kompromittering af disse, samt○ omgående anmoder om fornyelse af sine Elektroniske Identifikationsmidler, hvis indholdet af disse 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 skal være i overensstemmelse med principperne i [ISO 27001] standarden. 3) Der skal foreligge en beredskabsplan, som dækker alle væsentlige områder. |
| Høj | 4) Organisationen skal være certificeret efter [ISO 27001] standarden eller på tilsvarende måde kunne dokumentere efterlevelsen af krav til informationssikkerhedsledelse. |

4.1.4 Dokumentation og registerføring

Nedenstående tabel angiver krav til dokumentation:

| Sikringsniveau | Krav |
|----------------|---|
| Lav | 1) Relevant information skal arkiveres 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 | <ol style="list-style-type: none"> 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 | <ol style="list-style-type: none"> 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 | <ol style="list-style-type: none"> 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 | <ol style="list-style-type: none"> 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). |

| | |
|------------------|---|
| | <p>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.</p> <p>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.</p> <p>5) Alle medier, som indeholder personlige, kryptografiske eller andre fortrolige eller følsomme oplysninger, lagres, transporteres og bortskaffes på en sikker måde.</p> |
| Betydelig | <p>6) Følsomt kryptografisk materiale anvendt til udstedelse af et Elektronisk Identifikationsmiddel og Autentifikation, som lagres vedvarende, skal beskyttes mod manipulation.</p> <p>7) Der må ikke benyttes kryptografiske algoritmer eller protokoller med kendte sårbarheder eller med utilstrækkelige nøglelængder.</p> |
| 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, offentliggør Digitaliseringsstyrelsen en kort beskrivelse af løsningen og det anmeldte Sikringsniveau på Digitaliser.dk.

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:

| Sikringsniveau | Krav |
|-----------------------|---|
| Lav | <p>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.</p> <p>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.</p> <p>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.</p> |
| Betydelig | <p>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,</p> |



DIGITALISERINGSSTYRELSEN

| | |
|------------|---|
| | <p>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.</p> <p>5) Revisionserklæringen er udarbejdet i henhold til revisionsinstruk-sen for NSIS på niveau Betydelig, som findes publiceret på https://www.digitaliser.dk/group/3426134/resources</p> |
| Høj | <p>6) Revisionserklæringen er udarbejdet i henhold til revisionsinstruk-sen for NSIS på niveau Høj, som findes publiceret på https://www.digitaliser.dk/group/3426134/resources</p> |

5 Elektroniske Identifikationsmidler associeret til juridiske personer

Dette kapitel omhandler krav til Elektroniske Identifikationsmidler for 'fysiske personer associeret med en juridisk person'. Associationen 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 (som det fx kendes fra OCES Medarbejdercertifikater), men kan også bestå af en logisk tilknytning mellem en fysisk person og en juridisk person uden udstedelse af nye Elektroniske Identifikationsmidler (fx ved CVR-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 person 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. Dette kan være en fordel i situationer, hvor der er behov for straksudstedelse af et nyt Elektronisk Identifikationsmiddel, hvis medarbejderen fx har mistet adgangen til sit Elektroniske Identifikationsmiddel og derfor ikke kan udføre sit arbejde.

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

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

| Sikringsniveau | Krav |
|----------------|---|
| Lav | <ol style="list-style-type: none">1) Det skal være muligt at suspendere og/eller ophæve en forbindelse for begge parter.2) Den juridiske person 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 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 persons konkurs eller likvidering.4) Godtgørelse af Identiteten af den fysiske person, der handler på vegne af den juridiske person, kontrolleres på Sikringsniveau »lav« eller derover.5) Forbindelsen kan oprettes på grundlag af opslag i CVR-registret |



DIGITALISERINGSSTYRELSEN

| | |
|------------------|---|
| | <p>eller anden Autoritativ Kilde, herunder den juridiske person selv.</p> <p>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 person.</p> |
| Betydelig | <p>7) Sikringen af Identiteten af den fysiske person, der handler på vegne af den juridiske person, foretages på Sikringsniveau »Betydelig« eller »Høj«.</p> <p>8) Forbindelsen er etableret under kontrol af den juridiske person fx via en udpeget administrator eller via oplysninger fra en Autoritativ kilde.</p> <p>9) Procedurer til grund for etableringen af forbindelsen er underlagt revision.</p> <p>10) Forbindelsen er blevet kontrolleret på grundlag af et entydigt identifikationsnummer (fx CVR-nummer), der repræsenterer den juridiske person, og som bruges i dansk virksomhedsregistrering, og på grundlag af oplysninger, der entydigt repræsenterer den fysiske person, fra en Autoritativ kilde.</p> <p>11) Den fysiske og juridiske person notificeres om etablering af forbindelsen.</p> |
| Høj | <p>12) Sikringen af Identiteten af den fysiske person, der er knyttet til en juridisk person, kontrolleres på Sikringsniveau »Høj«.</p> |

6 Krav til Identitetsbrokere

Dette kapitel stiller 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. Disse benævnes i visse sammenhænge 'Identity Providers' eller 'Security Token Services'. Som eksempler kan nævnes den centrale NemLog-in løsning, der udsteder SAML Assertions til offentlige tjenesteudbydere på baggrund af en NemID autentifikation. Et andet eksempel er lokale 'Identity Providere', 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 | <ol style="list-style-type: none"> 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. |
| Betydelig | <ol style="list-style-type: none"> 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 <i>Audience Restriction</i>). 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 |



DIGITALISERINGSSTYRELSEN

| | |
|------------|---|
| | <p>der skal etableres eksplicitte procedurer for nøglehåndtering, som dækker den fulde livscyklus.</p> <p>12) For nationale tjenester⁴ skal brokerens private nøgle, der underskriver security tokens, placeres i 'tamper-resistant' kryptografisk hardware der opfylder kravene til [FIPS 140-2] level 3 eller tilsvarende.</p> |
| Høj | <p>13) Brokerens private nøgle, der underskriver security tokens, placeres i 'tamper-resistant' kryptografisk hardware, der opfylder kravene til [FIPS 140-2] level 3 eller tilsvarende.</p> <p>14) Den private nøgle skal genereres i hardware og må ikke kunne eksporteres i klar tekst.</p> |

⁴ Tjenester som agerer som brokere for vilkårlige private borgere eller personer associeret til vilkårlige virksomheder. 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 standarden.

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 Digitaliser.dk.

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 fratagelse

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, eller hvis Sikringsniveauet ønskes ændret.

Digitaliseringsstyrelsen kan til enhver tid fratage en organisation retten til at henvise til denne standard samt fjerne den Elektroniske Identifikationsordning eller Identitetsbroker fra listen 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.

7.3 Ansvar og forsikring

Anmelderen af en elektronisk Elektronisk Identifikationsordning eller Identitetsbroker bærer det fulde ansvar for at kravene beskrevet i denne standard er opfyldt. 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 medkontraahenter og er berettiget til at søge at begrænse sit ansvar i forholdet mellem sig og sine medkontraahenter i det omfang, at disse medkontraahenter er erhvervsdrivende eller offentlige myndigheder. Anmelderen er ikke berettiget til at søge at begrænse sit ansvar i forhold til private borgere, som medkontraahenter, 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 opretholde en erhvervsansvarsforsikring til dækning af eventuelle erstatningskrav med en dækningssum på minimum 10 millioner kr.

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 et aftalt kontaktpunkt 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 27001:2013 - Information technology -- Security techniques -- Information security management systems -- Requirements".
- [ISO29115] "ISO/IEC 29115:2013 Information technology -- Security techniques -- Entity authentication assurance framework".
<https://www.iso.org/standard/45138.html>
- [LOA] "KOMMISSIONENS GENNEMFØRELSESFORORDNING (EU) 2015/1502 af 8. september 2015 om fastlæggelse af tekniske minimumsspecifikationer og procedurer for fastsættelse af Sikringsniveauer for elektroniske identifikationsmidler i henhold til artikel 8, stk. 3, i Europa- Parlamentets og Rådets forordning (EU) nr. 910/2014 om elektronisk identifikation og tillidstjenester til brug for elektroniske transaktioner på det indre marked".



DIGITALISERINGSSTYRELSEN

| | |
|------------|--|
| [LOA-GUID] | <p>"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</p> |
| [NIST] | <p>"NIST Special Publication 800-63 Revision 3", NIST. https://pages.nist.gov/800-63-3/sp800-63-3.html</p> |
| [NSI] | <p>"Fællesoffentlige brugerstyringsløsninger - en analyse af sikkerhedsstandarder og -løsninger", NSI.</p> |
| [DBL] | <p>"Databeskyttelsesloven", Justitsministeriet. https://www.retsinformation.dk/Forms/R0710.aspx?id=201319</p> |
| [REF-ARK] | <p>"Referencearkitektur for brugerstyring", Digitaliseringsstyrelsen. https://arkitektur.digst.dk/rammearkitektur/referencearkitekturer/referencearkitektur-brugerstyring</p> |
| [TU-LoA] | <p>"Valg af Sikringsniveau for identiteter - vejledning i brug af NSIS for tjenesteudbydere - version 1.1", Digitaliseringsstyrelsen. https://www.digitaliser.dk/resource/3651469</p> |
| [VEJL] | <p>"Vejledning i brug af NSIS for tjenesteudbydere", Digitaliseringsstyrelsen. https://www.digitaliser.dk/resource/3651469</p> |