

# National Standard for Identiteters Sikringsniveauer (NSIS)

Status: Version 1.0

Version: 15.12.2016

<b>1</b>	<b>INDLEDNING</b>	<b>4</b>
1.1	FORORD	4
1.2	INTRODUKTION	4
1.3	FORMÅL OG SCOPE	4
1.4	EKSEMPLER PÅ IDENTITETSTJENESTER OG NIVEAU'ER	5
1.5	TERMINOLOGI	6
<b>2</b>	<b>LIVSCYKLUS FOR EID'ER</b>	<b>9</b>
<b>3</b>	<b>NORMATIVE KRAV</b>	<b>11</b>
3.1	REGISTRERINGSPROCESSEN	11
3.1.1	Ansøgning	11
3.1.2	Verifikation af identitet (fysiske personer)	12
3.2	UDSTEDELSE OG HÅNDTERING AF EID	13
3.2.1	Styrke af eID	13
3.2.2	Levering og aktivering	13
3.2.3	Suspendering, spærring og genaktivering	14
3.2.4	Fornylse og udskiftning	14
3.3	ANVENDELSE OG AUTENTIFIKATION	15
3.3.1	Autentifikationsmekanismer	15
<b>4</b>	<b>ORGANISATORISKE- OG TVÆRGÅENDE KRAV</b>	<b>18</b>
4.1.1	Generelle krav	18
4.1.2	Oplysningspligt	18
4.1.3	Informationssikkerhedsledelse	19
4.1.4	Dokumentation og registerføring	19
4.1.5	Faciliteter og personale	20
4.1.6	Tekniske kontroller	21
4.1.7	Anmeldelse og revision	22
<b>5</b>	<b>ELEKTRONISKE IDENTIFIKATIONSMIDLER ASSOCIERET TIL JURIDISKE PERSONER</b>	<b>23</b>
5.1	UDSTEDELSE AF ELEKTRONISKE IDENTIFIKATIONSMIDLER	23
5.2	BINDING (ASSOCIERING) MELLEM ELEKTRONISKE IDENTIFIKATIONSMIDLER FOR FYSISKE OG JURIDISKE PERSONER	23
<b>6</b>	<b>KRAV TIL IDENTITETSBROKERE</b>	<b>25</b>
<b>7</b>	<b>GOVERNANCE</b>	<b>27</b>
7.1	EJERSKAB OG VEDLIGEHOLDELSE AF STANDARDEN	27
7.2	OPHØR OG FRATAGELSE	27
7.3	ANSVAR OG FORSIKRING	27
7.4	OMKOSTNINGER	28



## DIGITALISERINGSSTYRELSEN

7.5	DELING AF SIKKERHEDSHÆNDELSE	28
8	REFERENCER	29

# 1 Indledning

## 1.1 Forord

Dette dokument indeholder første version af en offentlig standard for identiteters sikringsniveauer (NSIS), hvis formål er at skabe rammer for tillid til digitale identiteter samt digitale identitetstjenester. Standarden er udarbejdet og administreres af Digitaliseringsstyrelsen og stilles til rådighed som referenceramme bl.a. i forbindelse med udbud af næste generation NemID, arbejdet med brugerstyring i den offentlige sektor samt vurdering af NemID i forbindelse med anmeldelse til Kommissionen i henhold til EU's forordning nr. 910/2014 om elektronisk identifikation og tillidstjenester til brug for elektroniske transaktioner på det indre marked med tilhørende retsakter, herunder EUs trust framework.

Dokumentet tager afsæt i internationale standarder og rammeværk med henblik på at sikre videndeling, certificering, akkreditering og understøttelse af det indre marked, herunder væsentligst eIDAS reguleringen (herunder den tilhørende retsakt om ”levels of assurance”) og ISO 29115.

Denne standard etableres på baggrund af en bred offentlig høringsproces. NSIS Standarden og høringsnotat offentliggøres på Digitaliseringsstyrelsens hjemmeside.

## 1.2 Introduktion

Nærværende standard definerer krav til styrken i sikringen af en autentifikationsproces samt den underliggende identifikation af en bruger. Dette kan også udtrykkes, som graden af tillid en tjenesteudbyder kan have til brugerens digitale identitet – eller på engelsk ”Level of Assurance” (LoA). Disse begreber er altså udtryk for den samme egenskab.

Standarden indeholder en række krav til ID-tjenester på fire forskellige sikringsniveau'er (Niveau 1 – 4). Det laveste niveau (1) har relativt lave krav, mens de høje niveau'er (3 og 4) har relativt høje krav. Tilgangen med fire niveau'er er valgt med udgangspunkt i gængs praksis for rammeværk som ISO 29115, STORK QAA, NIST SP 800-63 og Kantara Initiative's IAF. eIDAS-forordningen opererer med tre niveau'er (”low”, ”substantial” og ”high”) der svarer til niveau hhv. 2, 3 og 4 i denne standard.

Hensigten er, at en tjenesteudbyder kan definere kravene til ønsket sikringsniveau for brugerne baseret på en risikovurdering som beskrevet i vejledninger [OIO-A-LEVEL] samt [LOA-ØS], og at leverandører af identitetstjenester måles mod disse niveau'er. Herved afpasses risici i tjenesten (”risikoniveau'er”) med styrken af kontroller (”sikringsniveau'er”).

Kravene til de fire sikringsniveau'er kan være tekniske, organisatoriske, økonomiske osv., idet mange faktorer har indflydelse på tilliden til digitale identiteter og - løsninger.

## 1.3 Formål og scope

Denne standard er gældende for nationale fællesoffentlige elektroniske identifikationsmidler og identitetshåndtering til både borgere (fysiske personer) og medarbejdere i organisationer (fysiske personer associeret med en juridisk person). 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 eID-tjenester. Ud fra en modenhedsbetragtning er identitetshåndtering for organisationer, devices og Internet of Things ikke omfattet i første omgang. I takt med at disse områder modnes, og der evt. fremkommer internationale

rammeverk herfor, kan områderne med tiden blive indlemmet i denne standard, hvis det vurderes hensigtsmæssigt.

Der behandles alene forhold vedrørende udstedelse og brug af elektroniske identifikationsmidler, men der findes naturligt en lang række øvrige aspekter, man bør tage stilling til, når det samlede sikringsniveau for en tjeneste skal fastlægges som fx autorisation, konfidentialitet og tilgængelighed. De vigtigste forhold beskrives relativt kortfattet, uden at der nødvendigvis opstilles en udtømmende mængde af krav. Hensigten er således, at standarden er operationel og let at anvende.

Kravene tager udgangspunkt i og er i tråd med eIDAS reguleringen, således at en dansk eID-tjeneste, som opfylder et givet niveau i denne standard, i udgangspunktet også vil kunne opfylde kravene til samme niveau i forhold til eIDAS-forordningen. I den forbindelse skal det dog bemærkes, at den nationale standard vil være tilpasset nationale forhold og være mere detaljeret end den gennemførelsesretsakt [LOA], som definerer niveauerne 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 tjenesteudbydere ansvar i forbindelse med risikoafvejning og valg af sikringsniveau. Ansvar for vurdering af krav til sikringsniveau og risikoniveau for den enkelte tjeneste ligger hos de enkelte tjenesteudbydere, som er dataansvarlige myndigheder for de data, som udstilles og kan tilgås via tjenesten. Der kan i denne forbindelse henvises til publikationerne [OIO-A-LEVEL] samt [LOA-ØS], som indeholder vejledning til tjenesteudbydere om risikovurdering, der kan fastlægge behov for niveau af autenticitetssikring. For virksomheder mv. og myndigheder, som behandler personoplysninger, vil afdækning af risikoniveau 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 identitetstjenester og niveau'er

<b><i>NemID og NemLog-in</i></b>	I dag har vi med NemID og OCES-standard en fastlagt sikringsniveau gennem en konkret implementering. I fremtiden vil der evt. være større differentiering mellem forskellige implementeringer, der henviser til samme referenceramme.
<b><i>Private ID-tjenester</i></b>	Standarden definerer betingelserne for et kendt sikringsniveau, således at private eID-tjenester med et veldefineret sikringsniveau vil kunne vurderes i forhold til anvendelse i offentligt regi.
<b><i>Kommunal Identity Provider</i></b>	I den kommende, fælleskommunale infrastruktur vil kommunerne agere som Identity Providers og udstedere af elektroniske identifikationsmidler for egne medarbejdere. På den baggrund vil en medarbejders lokale log-in til et domæne (fx AD) kunne blive fødereret til eksterne, fælleskommunale systemer. Kommunerne har forskellige "identity proofing" processer og forskellige sikringsniveauer, så der er behov for standardiserede krav at måle

	dette op imod.
<b><i>Sundhedsområdet (Security Token Services)</i></b>	Sundhedsområdet har etableret Security Token Services <sup>1</sup> både nationalt og på regionernes serviceplatforme (NSP'er), som udsteder såkaldte ID-kort for sundhedsfaglige identiteter. 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.
<b><i>Uddannelsesområdet</i></b>	Der er en række ID-tjenester og føderationer etableret på uddannelsesområdet. Uddannelsesinstitutioner validerer personer i egne organisationer. Tjenester som Uni-Login og WAYF agerer hhv. som Identity Provider og Proxy, som fødererer disse identiteter.
<b><i>Udenlandske eID'er</i></b>	Som følge af eIDAS forordningen skal EU-landene gensidigt anerkende nationale eID ordninger, som er anmeldt til Kommissionen. Medlemslandenes løsninger er vidt forskellige, men gensidig tillid opnås gennem en fælles standard, der definerer et antal kendte sikringsniveauer.

## 1.5 Terminologi

Nedenfor er de vigtigste begreber beskrevet. Terminologien er for en stor dels vedkommende hentet fra ISO 24760-1 for at sikre konsistens med andet arbejde.

<b>Adgangskontrol</b>	Proces i en tjeneste, der afgør hvilke funktioner og data en bruger får adgang til på baggrund af brugerens attributter og tjenestens sikkerhedspolitik.
<b>Attribut</b>	Karakteristika eller egenskaber ved en Entitet. Dette kan fx være et brugernavn, et pseudonym, et CPR nummer, bopæl, rolle etc.
<b>Autentifikation</b>	En proces som genkender og verificerer en identitet for en entitet på baggrund af tilhørende elektroniske identifikationsmidler.
<b>Autentifikations-faktor</b>	En del af et elektronisk identifikationsmiddel eller andet bevis anvendt i en autentifikation, som kan være i kategorierne "noget kun brugeren er" (fx biometri), "noget kun brugeren ved" eller "noget kun brugeren er i besiddelse af". Sidstnævnte kategori vil typisk være et token

---

<sup>1</sup> Billetudstedere som giver adgang til sundhedstjenester.



## DIGITALISERINGSSTYRELSEN

eller en nøgle (fx nøglekort, nøglefil eller smart card).

### **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

### **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 lånt fra ISO/IEC 15408 "Information technology – Security techniques – Evaluation criteria for IT security" og ISO/IEC 18045 "Information technology – Security techniques – Methodology for IT security evaluation".

### **Dynamisk autentifikation**

En elektronisk proces, som anvender kryptografi eller andre teknikker til på forlangende at skabe et elektronisk bevis for, at den kontrollerede har adgang til eller er i besiddelse af et elektronisk identifikationsmiddel, og som ændres ved hver autentifikation mellem den, der søger adgang til systemet, og det system, der kontrollerer dennes identitet

### **eID-tjeneste**

En betroet tjeneste, som leverer en eller flere af de processer, som er underlagt krav i denne standard. Dette kan fx være identitetssikring, udstedelse af elektroniske identifikationsmidler eller drift af en broker. Bemærk, at eIDAS reguleringen bruger det komplementerende begreb "tillidstjeneste" om tjenester involveret i udstedelse af digitale signaturer/certifikater, validering af certifikaters gyldighed og tidsstempling.

### **Elektronisk identifikationsmiddel (eID)**

Et elektronisk eller fysisk objekt/genstand, der kan anvendes til at gennemføre en autentifikation af en identitet. Eksempler kan være brugernavn/kodeord, et NemID nøglekort, et certifikat med tilhørende privat nøgle, et SAML token etc.

### **Elektronisk identifikationsordning**

Et system til elektronisk identifikation, under hvilket der udstedes elektroniske identifikationsmidler til fysiske eller juridiske eller fysiske personer, der repræsenterer juridiske personer.

### **Entitet**

Et subjekt / en bruger som skal have adgang til en tjeneste. I denne standard betragtes kun fysiske personer, som evt. kan være associeret med en juridisk person som en entitet.



## DIGITALISERINGSSTYRELSEN

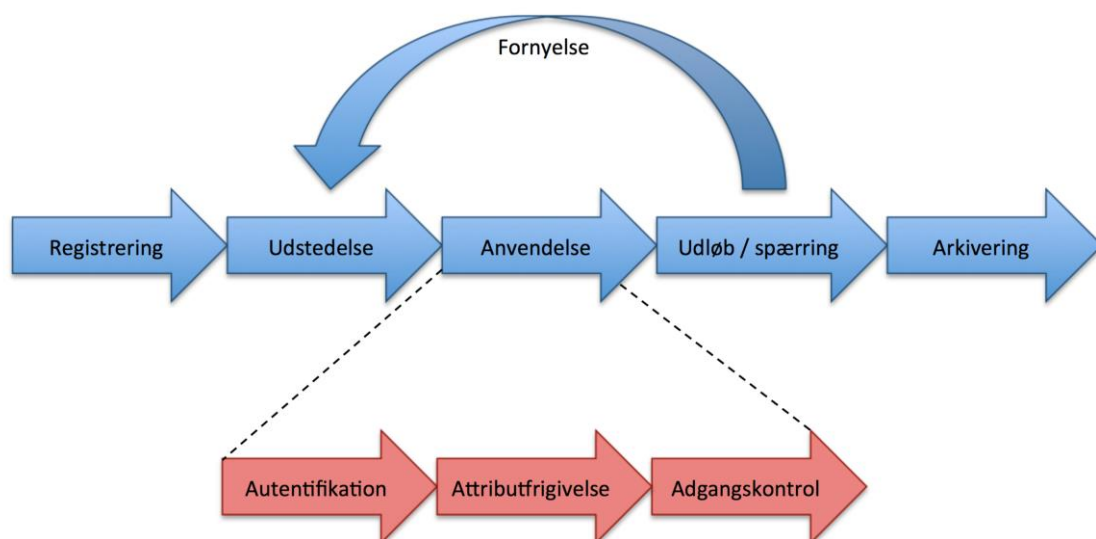
<b>Identitet</b>	En digital persona repræsenteret ved et sæt af attributter, som fx kan repræsentere en fysisk eller juridisk person, eller en fysisk person, der repræsenterer en juridisk person. En identitet kan rumme Personidentifikationsdata.
<b>Identitetsbroker</b>	En eID-tjeneste som formidler en autentificeret digital identitet til tredjeparter på baggrund af en autentifikation foretaget af broderen selv eller evt. af en anden tredjepart (brokere i flere led, men som ikke selv foretager identitetssikring eller udstedelse af akkreditiver. En Identitetsbroker er en tjeneste, som kræver tillid (en såkaldt <i>trusted third party</i> ) fra forretningstjenester, og derfor er de underlagt krav i dette rammeværk.
<b>Identitetsregister</b>	En funktion/register, der registrerer information om entiteter (fx borgere). Dette kan fx være CPR-registret og CVR-registret som eksempler blandt flere registre.
<b>Identitetssikring</b>	En proces hvor identiteten af en entitet fastlægges, og hvor attributter eller dele heraf (fx navn og CPR nummer eller tilknytning til juridisk person) efterprøves. Kaldes for <i>identity proofing</i> på engelsk.
<b>Personidentifikationsdata</b>	Et sæt data, der gør det muligt at fastslå identiteten af en fysisk eller juridisk person eller en fysisk person, der repræsenterer en juridisk person.
<b>Sikringsniveau</b>	Graden af tillid til en påstået identitet (på engelsk " <i>Level of Identity Assurance</i> ") og ofte også benævnt <i>autenticitetsniveau</i> . Defineres i dette dokument som fire niveauer, der stiller krav til de forskellige delprocesser i forbindelse med registrering, udstedelse og anvendelse af elektroniske identifikationsmidler.



## 2 Livscyklus for eID'er

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 procestrin kan udføres af forskellige aktører / tjenester. Som et tænkt, konkret eksempel kan registreringen i NemID løsningen ske i samarbejde mellem Borgerservice, CPR-registret og Nets DanID, udstedelsen foretages af Nets/DanID, autentifikationen kan foregå i NemLog-in løsningen (ved brug af NemID), mens sikkerhedskonteksten og autorisationen for brugeren kan etableres i Borger.dk ved adgang til en borgerrettet tjeneste.



Figur 1: Livscyklus for et eID

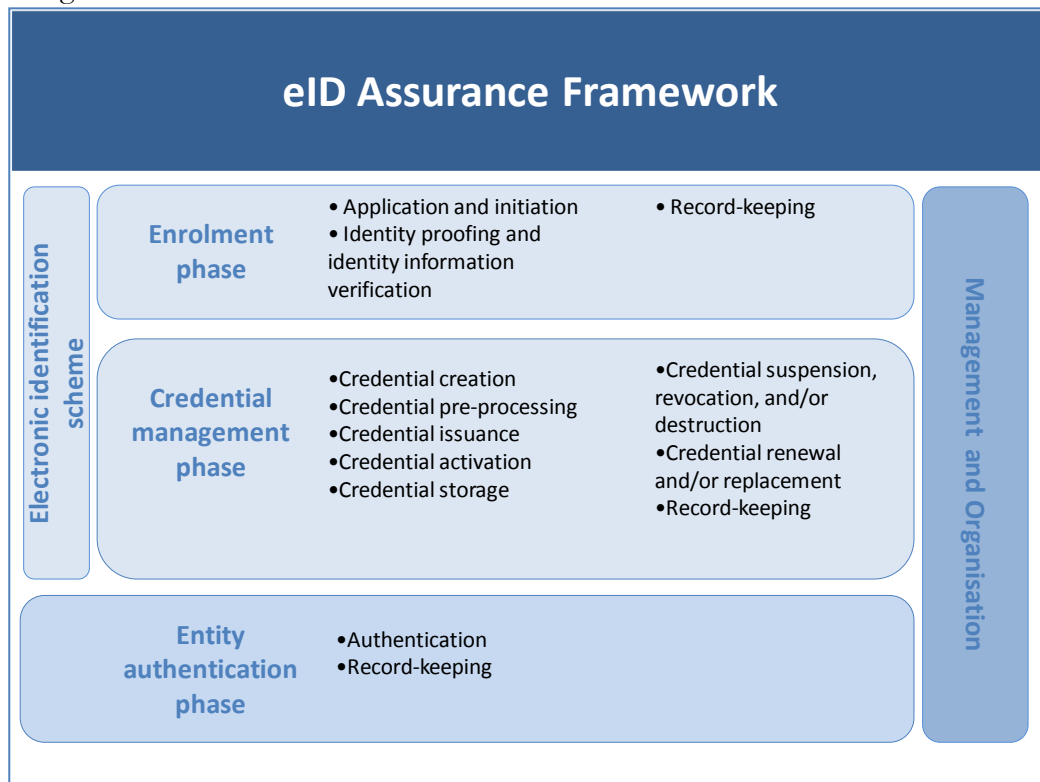
OBS: Hensigten med figuren er at give læseren et overblik over de forskellige stadier - strukturen er afspejlet i kapitlerne med de normative krav, men der er dog ikke en fuldstændig en-til-en relation.

Nedenfor findes en kort opsummering af livscyklus for et eID:

- *Registrering* - en proces, hvor brugeren ansøger om et eID og identitetssikringen foretages.
- *Udstedelse* – en proces, hvor et eID udstedes og overdrages til brugeren.
- *Aktivering* - en proces, hvor brugeren får overdraget sit eID og gør det klar til brug.
- *Anvendelse* – de processer, hvor brugeren anvender sit eID til autentifikation (eller evt. signering) mod on-line tjenester, som herefter kan danne baggrund for øvrige processer som fx frigivelse af attributter, adgangskontrol mv.

- *Udløb* – hændelsen hvor eID’et naturligt udløber og herefter ikke længere kan anvendes.
- *Spærring* – en hændelse, hvor eID’et spærres permanent fx som følge af kompromitering. Ved midlertidig spærring (der kan ophæves) benyttes begrebet *Suspension*.
- *Arkivering* – en proces, hvor eID’et eller relaterede data langtidsarkiveres fx af hensyn til at sikre bevisværdi eller for at kunne dekryptere data mv.

En anden måde at strukturere og beskrive de underliggende processer findes i nedenstående figur:



**Figur 2: eIDAS Framework<sup>2</sup>**

<sup>2</sup> "Levels of Assurance, Draft 12". Udkast udarbejdet af UK, DE, UK, NL, DK og andre i forbindelse med arbejdet i eIDAS expert group.

## 3 Normative krav

Dette kapitel indeholder normative krav til udstedelse og anvendelse af elektroniske identifikationsmidler med udgangspunkt i eIDAS reguleringen<sup>3</sup>. Da kravene som sagt går på forskellige trin i livscyklussen, vil ikke alle krav være relevante for alle eID-tjenester – nedenstående skal altså opfattes som den samlede mængde krav.

Når der til et givet sikringsniveau er angivet flere krav, skal alle kravene opfyldes, med mindre andet eksplicit er anført. Herudover gælder, at en løsnings samlede sikringsniveau dikteres af det mindste sikringsniveau opnået på de specifikke områder nedenfor. Med andre ord, skal samtlige krav til fx niveau ”3=Betydelig” opfyldes, før en løsning kan angives at være på niveau 3.

Kravene er forsøgt formuleret resultatbaserede (*outcome-based*), således at de primært sigter på resultatet af nogle kontroller og processer (det ønskede niveau), frem for at diktere metoden til at opnå niveauet. Der er dog afvigelser fra denne tilgang, så reelt er kravene en blanding af flere tilgange.

### 3.1 Registreringsprocessen

#### 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 eID udstedes automatisk som en del af ansættelsesprocessen. I disse tilfælde skal kravene opfyldes alligevel.

Sikringsniveau	Krav
1. Begrænset	1) Ingen krav.
2. Lav	1) Ansøgeren skal gøres bekendt med betingelserne for brugen af det udstedte eID. 2) Ansøgeren skal gøres bekendt med de anbefalede sikkerhedsforanstaltninger, som har at gøre med brugen af det elektroniske identifikationsmiddel. 3) De data, som er relevante for godtgørelse og kontrol af identitet, er indsamlet.
3. Betydelig	Som Lav samt følgende: 4) Ansøgeren skal afkræves accept af betingelser/tilkendegive, at de har læst dem.
4. Høj	Som Betydelig.

---

<sup>3</sup> Ved eIDAS reguleringen forstås forordningen samt implementerende og delegerede retsakter.

### 3.1.2 Verifikation af identitet (fysiske personer)

Dette afsnit stiller krav til identitetssikring af ansøger (*identity proofing*), herunder validering og verifikation af identitet inden udstedelse af et eID.

Sikringsniveau	Krav
<b>1. Begrænset</b>	1) Der skal foreligge en beskrivelse af verifikationsprocessen, herunder de forudsætninger, der lægges til grund.
<b>2. Lav</b>	Som Begrænset samt flg.: 2) Ansøgeren vurderes med overvejende sandsynlighed at være i besiddelse af almindeligt anerkendt dokumentation for sin identitet. Dette kan være sygesikringskort, pas, kørekort, dåbsattest, forskudsopgørelse eller elektronisk ID. 3) Dokumentationen er kontrolleret som værende ægte og gyldig.
<b>3. Betydelig</b>	Som Lav samt alle nedenstående krav: 4) Det er verificeret, 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 de samme identifikationsprocesser som benyttes ved udstedelse af dansk pas eller kørekort anvendes. 5) Dokumentation kontrolleres med henblik på at fastslå, at det er gyldigt i henhold til en autoritativ kilde. 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 beviset kan være blevet tabt, stjålet, suspenderet, tilbagekaldt eller være udløbet. Ansøgeren eksisterer i autoritative registre (fx CPR) og er ikke markeret som umyndiggjort, død eller forsvundet. 7) Ansøgeren skal besidde personlig viden, som ikke forventes alment kendt (kontrolspørgsmål). 8) Kontroller udføres kun af specielt uddannet personale, der har modtaget instruktion i at verificere ægthed af dokumenter og detektere svindel.
<b>4. Høj</b>	Som Betydelig samt følgende krav: 9) Ansøgeren kan identificeres som havende den påståede identitet ved sammenligning af et eller flere af personens fysiske kendetegn med en autoritativ kilde. Sammenligningen skal udføres enten via personligt fremmøde eller en anden mekanisme, der giver en ækvivalent sikkerhed. 10) Der er med meget høj sandsynlighed et fysisk match mellem ansøgeren og den præsenterede dokumentation (fx match af billede og underskrift).

Kravene i ovenstående tabel er møntet på ny-udstedelse baseret på ikke-elektronisk dokumentation. Generelt er det tilladt at basere identifikation på autentifikation med et gyldigt eID på mindst samme sikringsniveau, såfremt de nødvendige oplysninger (personidentifikationsdata) tilvejebringes gennem denne autentifikation. eID'et behøver ikke være fra den samme udsteder. Her skal det i givet fald kunne verificeres, at det pågældende eID er gyldigt og ikke spærret.

## 3.2 Udstedelse og håndtering af eID

### 3.2.1 Styrke af eID

Nedenstående tabel angiver en række krav til elektroniske identifikationsmidler med henblik på brug på senere autentifikation.

Sikringsniveau	Krav
<b>1. Begrænset</b>	1) Ingen krav.
<b>2. Lav</b>	2) Det elektroniske identifikationsmiddel skal gøre brug af mindst en autentifikationsfaktor. 3) Det elektroniske identifikationsmiddel er designet, så det er personligt (delte identiteter (fællesbrugere) eller elektroniske identifikationsmidler ikke tilladt). 4) Der er taget rimelige skridt til at sikre, at det kun er den person, som det tilhører, der har kontrol over eller er i besiddelse af det elektroniske identifikationsmiddel, der kan anvende det.
<b>3. Betydelig</b>	5) Det elektroniske identifikationsmiddel skal gøre brug af mindst to autentifikationsfaktorer fra forskellige kategorier. 6) 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 eller er i besiddelse af det.
<b>4. Høj</b>	Som Betydelig samt flg.: 7) Det elektroniske identifikationsmiddel skal være beskyttet mod kopiering og manipulering af angribere med høj angrebskapacitet. 8) Det elektroniske identifikationsmiddel er udformet således, at den person, som det tilhører, kan beskytte det sikkert mod, at andre bruger det.

Styrken af den enkelte autentifikationsfaktor bør nøje vurderes – herunder fx entropien af kodeord eller kryptografiske nøgler samt tilhørende kontroller.

Eksempler på elektroniske identifikationsmidler på niveau 2, 3 og 4 er hhv. kodeord, NemID nøglekort implementeringen og smart cards til kvalificerede signaturer.

### 3.2.2 Levering og aktivering

Nedenstående tabel angiver kravene til levering per sikringsniveau:

Sikringsniveau	Krav
<b>1. Begrænset</b>	1) Ingen krav.
<b>2. Lav</b>	1) Det elektroniske identifikationsmiddel leveres efter udstedelse via en mekanisme, som gør det muligt at antage, at det kun leveres til den tilsigtede person.
<b>3. Betydelig</b>	1) 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.
<b>4. Høj</b>	<ol style="list-style-type: none"> <li>1) Aktiveringsprocessen kontrollerer, at det elektroniske identifikationsmiddel kun blev udleveret til den person, som det tilhører.</li> <li>2) Udleveringen skal beskyttes mod angreb, hvor elektroniske identifikationsmidler stjæles under transport samt insider-angreb i udleveringsfunktionen hos udstederen ved fx at benytte to uafhængige forsendelseskanaler eller funktionsadskillelse.</li> </ol>

### 3.2.3 Suspendering, spærring og genaktivering

Nedenstående tabel angiver kravene til suspendering og spærring per sikringsniveau:

Sikringsniveau	Krav
<b>1. Begrænset</b>	1) Ingen krav.
<b>2. Lav</b>	<ol style="list-style-type: none"> <li>1) Det skal være muligt for brugeren at suspendere (midlertidigt forhindre anvendelse) og/eller spærre (permanent forhindre anvendelse) hurtigt og effektivt.</li> <li>2) Der skal etableres foranstaltninger, som sikrer mod, at elektroniske identifikationsmidler spærres eller suspenderes uretmæssigt i et forsøg på at lukke en legitim brugers adgang.</li> <li>3) Reaktivering skal kun finde sted, hvis de samme sikringskrav som forud for udstedelsen fortsat er opfyldt.</li> <li>4) eID-udstederen har en selvstændig pligt til at spærre et eID, hvis der er mistanke om kompromittering eller tab af kontrol over dette, hvis der konstateres fejl i eID (fx forkerte data), hvis der ikke længere foreligger en gyldig aftale mellem udsteder og ansøger, eller hvis ansøgerens virksomhed ophører eller går konkurs.</li> </ol>
<b>3. Betydelig</b>	<p>Som Lav samt følgende:</p> <ol style="list-style-type: none"> <li>5) Suspenderings- og spærrefunktion bør være til rådighed døgnet rundt og have en høj grad af tilgængelighed.</li> <li>6) eID-udstederen har selvstændig pligt til at spærre et eID, hvis ansøger er død.</li> </ol>
<b>4. Høj</b>	Som Betydelig.

### 3.2.4 Fornyelse og udskiftning

Nedenstående tabel angiver kravene til fornyelse og udskiftning pr. sikringsniveau:

Sikringsniveau	Krav
<b>1. Begrænset</b>	1) Ingen krav.
<b>2. Lav</b>	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.

<b>3. Betydelig</b>	Som Lav.
<b>4. Høj</b>	Som Lav samt følgende:  2) Hvor fornyelsen baseres på en gyldig elektronisk identifikation, skal personidentifikationsdata verificeres på ny mod en autoritativ kilde.

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

### 3.3 Anvendelse og autentifikation

#### 3.3.1 Autentifikationsmekanismer

Nedenstående tabel angiver kravene til autentifikationsmekanismer pr. sikringsniveau, gennem hvilken en entitet anvender sit eID til at bevise sin identitet mod en tjeneste:

Sikringsniveau	Krav
<b>1. Begrænset</b>	1) Ingen krav.
<b>2. Lav</b>	1) Frigivelsen af personidentifikationsdata finder sted efter en pålidelig kontrol af det elektroniske identifikationsmiddel og dets gyldighed. 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 det elektroniske identifikationsmiddel, 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.
<b>3. Betydelig</b>	Som lav samt følgende:  4) Frigivelsen af personidentifikationsdata finder sted efter en pålidelig kontrol af det elektroniske identifikationsmiddel og dets gyldighed via en dynamisk autentifikationsmekanisme. Frigivelsen af personidentifikationsdata finder sted efter en pålidelig kontrol af det elektroniske identifikationsmiddel og dets gyldighed via en dynamisk autentifikationsmekanisme. Autentifikationsmekanismen implementerer sikkerhedskontroller til at efterprøve det elektroniske identifikationsmiddel, 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



## DIGITALISERINGSSTYRELSEN

	omgå autentifikationsmekanismen.
<b>4. Høj</b>	<p>Som betydelig samt følgende:</p> <p>5) Autentifikationsmekanismen implementerer sikkerhedskontroller til at efterprøve det elektroniske identifikationsmiddel, 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.</p>





**DIGITALISERINGSSTYRELSEN**

## 4 Organisatoriske- og tværgående krav

### 4.1.1 Generelle krav

Nedenstående tabel angiver de generelle krav til eID-tjenester inkl. brokere (se kapitel 6):

Sikringsniveau	Krav
<b>1. Begrænset</b>	1) Ingen krav.
<b>2. Lav</b>	1) Leverandører af eID-tjenester beskrevet i dette dokument skal være en registreret juridisk enhed i EU med en etableret organisation. Leverandøren skal leve op til alle krav for de tilbudte tjenester, svarende til de beskrevne processer i et eID's livscyklus (registrering, udstedelse, anvendelse, broker etc.). 2) eID-leverandører skal til enhver tid kunne dokumentere overholdelse af gældende lov herunder den gældende regulering af personoplysninger, forvaltningsloven (hvis offentlige myndighed), forordning om eID og tillidstjenester samt anden relevant lovgivning. 3) Leverandører af eID-tjenester er ansvarlige for opfyldelse af forpligtelser, som er overdraget til tredjepart.
<b>3. Betydelig</b>	Som Lav samt flg.: 1) Leverandørerne 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. 2) eID-tjenester leveret af private virksomheder skal have en beskrevet termineringsplan, som sikrer en hensigtsmæssig nedlukning eller overtagelse af tredjepart, underretning af myndigheder og brugere. Planen skal indeholde detaljer om, hvordan data opbevares, beskyttes og destrueres.
<b>4. Høj</b>	Som Betydelig.

### 4.1.2 Oplysningspligt

Nedenstående tabel angiver krav til oplysning:

Sikringsniveau	Krav
<b>1. Begrænset</b>	1) Ingen krav.
<b>2. Lav</b>	1) Der skal offentliggøres en servicebeskrivelse, som beskriver alle relevante betingelser, betalinger for og begrænsninger på brugen af servicen. Servicebeskrivelsen skal indeholde en privatlivspolitik, der beskriver, hvilke informationer der indsamles og til hvilket formål, hvordan de behandles, hvor længe de gemmes samt evt. forhold om videregivelse etc. Det skal endvidere beskrives, hvordan entiteter kan søge indsigt, kan kræve rettelser af fejlagtige

	<p>registreringer samt klagemuligheder.</p> <p>2) Leverandøren skal oplyse om ansvar og forudsætninger for brugere samt "relying parties", der forlader sig på et eID, i forhold til at opnå et givet sikringsniveau. Dette omfatter fx sikkerhedsvejledning til brugere.</p> <p>3) Det skal eksplicit kræves i betingelserne, at brugeren:</p> <ul style="list-style-type: none"> <li>○ alene anvender eID'et i overensstemmelse med udstederens politikker (herunder politikker for brug og længde af kodeord) samt</li> <li>○ ikke overdrager sine elektroniske identifikationsmidler til andre samt</li> <li>○ giver fyldestgørende og korrekte svar på alle anmodninger om information i ansøgningsprocessen samt</li> <li>○ tager rimelige forholdsregler for at beskytte sine elektroniske identifikationsmidler (herunder ved evt. sikkerhedskopiering) samt</li> <li>○ omgående anmoder om spærring af sine elektroniske identifikationsmidler i tilfælde af kompromittering eller mistanke om kompromittering af disse, samt</li> <li>○ 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 eID'et).</li> </ul>
<b>3. Betydelig</b>	Som Lav.
<b>4. Høj</b>	Som Lav.

#### 4.1.3 Informationssikkerhedsledelse

Nedenstående tabel angiver krav til informationssikkerhedsledelse for eID-tjenester:

Sikringsniveau	Krav
<b>1. Begrænset</b>	1) Ingen krav.
<b>2. Lav</b>	1) Leverandører af eID-tjenester skal etablere et effektivt ledelsessystem for informationssikkerhed (ISMS) med henblik på at håndtere risici knyttet til informationssikkerhed.
<b>3. Betydelig</b>	<p>Som Lav samt flg.:</p> <p>2) Ledelsessystemet skal være i overensstemmelse med kravene i ISO 27001 standarden.</p> <p>3) Der skal foreligge en beredskabsplan, som dækker alle væsentlige områder.</p>
<b>4. Høj</b>	<p>Som Betydelig samt flg.:</p> <p>4) Leverandøren skal være certificeret efter ISO 27001 standarden.</p>

#### 4.1.4 Dokumentation og registerføring

Nedenstående tabel angiver krav til dokumentation:

Sikringsniveau	Krav
<b>1. Begrænset</b>	1) Ingen krav.
<b>2. Lav</b>	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.
<b>3. Betydelig</b>	Som Lav.
<b>4. Høj</b>	Som Lav.

#### 4.1.5 Faciliteter og personale

Nedenstående tabel angiver krav til faciliteter og personale:

Sikringsniveau	Krav
<b>1. Begrænset</b>	1) Ingen krav.
<b>2. Lav</b>	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 og 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 følsomme oplysninger skal begrænses til autoriseret personale.
<b>3. Betydelig</b>	Som Lav samt flg.: 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, erfaring og sikkerhedsklassifikation. Det samme gælder leverandører og underleverandører. 6) Det skal sikres, at adgang til og ophold i de centrale driftslokaler videoovervåges.

<b>4. Høj</b>	<p>Som Betydelig samt flg.:</p> <ol style="list-style-type: none"> <li>Medarbejdere og ledelse skal kunne sikkerhedsgodkendes i henhold til statens sikkerhedscirkulære<sup>4</sup>, hvis de skal arbejde med klassificeret materiale eller tilgår klassificerede områder, som falder ind under denne forpligtigelse. Dette gælder også for leverandører og underleverandører.</li> <li>Driftsfaciliteter skal have en perimeterbeskyttelse svarende til DS 471<sup>5</sup> eller bedre.</li> </ol>
---------------	---

#### 4.1.6 Tekniske kontroller

Nedenstående tabel angiver krav til tekniske kontroller:

Sikringsniveau	Krav
<b>1. Begrænset</b>	<ol style="list-style-type: none"> <li>Ingen krav.</li> </ol>
<b>2. Lav</b>	<ol style="list-style-type: none"> <li>Der findes rimelige tekniske kontroller, som gør det muligt at afværge trusler mod tjenesternes sikkerhed og sikre de behandlede oplysningers fortrolighed, integritet og tilgængelighed.</li> <li>Elektroniske kommunikationskanaler, som benyttes til udveksling af personhenførbare eller følsomme oplysninger, skal beskyttes mod aflytning, manipulation og genspilning (replay).</li> <li>Adgang til kryptografisk materiale brugt til udstedelse af eID 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.</li> <li>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.</li> <li>Alle medier, som indeholder personlige, kryptografiske eller andre følsomme oplysninger, lagres, transporteres og bortskaffes på en sikker måde.</li> </ol>
<b>3. Betydelig</b>	<p>Som Lav samt flg.:</p> <ol style="list-style-type: none"> <li>Følsomt kryptografisk materiale anvendt til udstedelse af eID og autentifikation, som lagres vedvarende, skal beskyttes mod manipulation.</li> <li>Der må ikke benyttes kryptografiske algoritmer eller protokoller med kendte sårbarheder eller med utilstrækkelige nøglelængder.</li> </ol>
<b>4. Høj</b>	Som Betydelig.

<sup>4</sup> "Cirkulære vedrørende sikkerhedsbeskyttelse af informationer af fælles interesse for landene i NATO, EU eller WEU, andre klassificerede informationer samt informationer af sikkerhedsmæssig beskyttelsesinteresse i øvrigt", CIR nr. 204 af 07/12/ 2001.

<sup>5</sup> <https://webshop.ds.dk/da-dk/standard/ds-4711993>

#### 4.1.7 Anmeldelse og revision

eID-ordninger, 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 anmeldelse samt 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. Styrelsen påtager sig intet ansvar for, hvorvidt anmeldte løsninger faktisk har det angivne sikringsniveau.

Nedenstående tabel angiver krav til anmeldelse og revision:

Sikringsniveau	Krav
<b>1. Begrænset</b>	1) Leverandøren skal ved anmeldelse af sin eID ordning til Digitaliseringsstyrelsen angive eID ordningens tekniske og sikkerhedsmæssige udformning samt sikringsniveau og navn.
<b>2. Lav</b>	Som Begrænset samt flg.: 1) Leverandøren skal ved anmeldelse af sin eID ordning til Digitaliseringsstyrelsen anvende selvdeklarering. Anmelderen indestår selv for, at kravene til det angivne sikringsniveau er opfyldt. 2) 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.
<b>3. Betydelig</b>	Som Lav samt flg.: 1) Ved anmeldelse anvendes selvdeklarering suppleret med en revisionserklæring fra en uafhængig statsautoriseret revisor, som bekræfter, at løsningens tekniske og sikkerhedsmæssige udformning er gennemgået, at kravene i denne standard er overholdt af løsningen på det angivne sikringsniveau, og at der er implementeret processer for løbende at sikre, at det angivne sikringsniveau opretholdes. Anmeldelsen suppleres med en ledelseserklæring underskrevet af en tegningsberettiget, hvoraf det fremgår, at alle relevante krav er opfyldt og fornødne processer for opretholdelse er implementeret. Der skal årligt indsendes en ny revisionserklæring, som bekræfter, at kravene til stadighed opfyldes. 2) Revisionserklæringens omfang er beskrevet i annek 1.
<b>4. Høj</b>	Som Betydelig samt flg.: 1) Revisionserklæringens omfang er beskrevet i annek 2.

## 5 Elektroniske identifikationsmidler associeret til juridiske personer

Dette kapitel omhandler krav til elektroniske identifikationsmidler for fysiske personer associeret med en juridisk person. Associationen dækker medarbejdere ansat i en virksomhed, men også andre relationer, hvor der ikke foreligger et ansættelsesforhold. En associering kan udmøntes ved udstedelse af et nyt selvstændigt, akkreditiv (som det fx kendes fra OCES Medarbejdercertifikater), men kan også blot bestå af en logisk forbindelse, der knytter en fysisk person til en juridisk person uden udstedelse af nye akkreditiver (fx ved CVR-opmærkning af den fysiske person, hvor den fysiske person benytter sit personlige eID i erhvervssammenhæng). Nedenfor angives specifikke krav til håndtering af livscyklus for associeringer.

### 5.1 Udstedelse af elektroniske identifikationsmidler

Når der udstedes et eID 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 fremsendelse af elektroniske identifikationsmidler kan man i stedet for folkeregisteradressen anvende virksomhedens registrerede adresse.

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 eID, hvis medarbejderen fx har mistet adgangen til sit eID 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
<b>1. Begrænset</b>	<ol style="list-style-type: none"><li>1) Det skal være muligt at suspendere og/eller ophæve en forbindelse.</li><li>2) Den juridiske person har (via en administrator) ret til at udføre suspendering eller ophævning, hvilket kan indbefatte suspendering / spærring af et tilhørende akkreditiv, hvis forbindelsen er etableret herigennem.</li><li>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 eID'et, eller i tilfælde af den juridiske persons konkurs eller likvidering.</li></ol>
<b>2. Lav</b>	Som Begrænset samt flg.: <ol style="list-style-type: none"><li>1) Godtgørelse af identiteten af den fysiske person, der handler på vegne af den juridiske person, kontrolleres på sikringsniveau »lav«</li></ol>



## DIGITALISERINGSSTYRELSEN

	<p>eller derover.</p> <ol style="list-style-type: none"><li>2) Forbindelsen kan oprettes på grundlag af dansk selskabsregistrering.</li><li>3) 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.</li></ol>
<b>3. Betydelig</b>	<p>Som Lav samt flg.:</p> <ol style="list-style-type: none"><li>1) Sikringen af identiteten af den fysiske person, der handler på vegne af den juridiske person, foretages på sikringsniveau »betydelig« eller »høj«.</li><li>2) Forbindelsen er blevet etableret på grundlag af anerkendte procedurer, som resulterede i registrering af forbindelsen i en autoritativ kilde.</li><li>3) Forbindelsen er blevet kontrolleret på grundlag af oplysninger fra en autoritativ kilde.</li><li>4) Procedurer til grund for etableringen af forbindelsen er underlagt revision.</li></ol>
<b>4. Høj</b>	<p>Som Betydelig samt flg.:</p> <ol style="list-style-type: none"><li>1) Sikringen af identiteten af den fysiske person, der handler på vegne af den juridiske person, kontrolleres på sikringsniveau »høj«.</li><li>2) Forbindelsen er blevet kontrolleret på grundlag af et entydigt identifikationsnummer, der repræsenterer den juridiske person, og som bruges i dansk selskabsregistrering, og på grundlag af oplysninger, der entydigt repræsenterer den fysiske person, fra en autoritativ kilde.</li></ol>



## 6 Krav til Identitetsbrokere

Dette kapitel stiller en række krav til såkaldte "identitetsbrokere", som videreformidler en autentifikation ved at udstede og signere et såkaldt Security Token for en elektronisk identitet. Disse benævnes i nogen sammenhænge for "Identity Providers" eller "Security Token Services". Et eksempel er NemLog-in løsningen, der udsteder SAML Assertions til offentlige tjenesteudbydere.

Leverandører af identitetsbrokere skal generelt overholde organisatoriske krav angivet i kapitel 4 på det sikringsniveau, som brokeren klassificeres til.

Derudover gælder flg. krav:

Sikringsniveau	Krav
<b>1. Begrænset</b>	1) Ingen krav.
<b>2. Lav</b>	<ol style="list-style-type: none"> <li>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.</li> <li>Det aktuelle sikringsniveau skal angives som en oplysning i det udstedte token (level of assurance), således at modtageren af tokens direkte kan aflæse dette. Sikringsniveauet i et token opgøres som mindsteværdien af sikringsniveauet for det anvendte eID til autentifikationen, brokerens eget sikringsniveau samt sikringsniveauerne for evt. identitetsbrokere, der er benyttet som underleverandører i den konkrete autentifikation.</li> <li>Tokens skal signeres med brokerens private nøgle og må kun udveksles over krypterede kanaler.</li> <li>Brokerens private nøgle, der underskriver security tokens, skal beskyttes mod uautoriseret adgang.</li> <li>Single Sign-On sessioner skal have en begrænset levetid (automatisk udløb) og det skal være muligt for brugeren at logge ud af alle sessioner på én gang (single logout).</li> <li>Single Sign-On sessioner skal beskyttes mod overtagelse.</li> <li>Alle forespørgsler til identitetsbrokeren og alle svar på disse skal skrives til en integritetsbeskyttet log.</li> </ol>
<b>3. Betydelig</b>	<p>Som Lav samt flg.:</p> <ol style="list-style-type: none"> <li>Anvendere af Identitetsbrokere, der tillader brugerautentifikation, skal i deres forespørgsel kunne fravælge Single Sign-On, hvis der fra tjenestens side er ønske om at gennemtvinge en aktiv brugerautentifikation (dvs. fravælge SSO).</li> <li>Tokenet skal være begrænset til en eller flere specifikke tjenester, og disse skal fremgå eksplicit i tokenet.</li> <li>Tokens skal end-to-end krypteres, således at indholdet kun er læsbart for modtageren.</li> <li>Sessioner skal beskyttes mod overtagelse ved fx kun at udveksle sessionsinformation over krypterede forbindelser samt ved at</li> </ol>



## DIGITALISERINGSSTYRELSEN

	forbyde sessionsinformation at blive tilgængeligt fra script i browseren. 12) For nationale tjenester <sup>6</sup> skal brokerens private nøgle, der underskriver security tokens, placeres i tamper-resistant hardware (HSM).
<b>4. Høj</b>	Som Betydelig samt flg.: 13) Brokerens private nøgle, der underskriver security tokens, placeres i "tamper-resistant" kryptografisk hardware (HSM), der opfylder kravene til FIPS 140-2 level 3 eller tilsvarende.

---

<sup>6</sup> Tjenester som udsteder eID til 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 eID ordninger 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 eID-tjenesteyder, der har anmeldt en eID ordning 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.

Digitaliseringsstyrelsen kan til enhver tid fratage en eID-ordning retten til at henvise til denne standard samt fjerne tjenesten fra listen over anmeldte tjenester, såfremt tjenesten ikke efterlever kravene i standarden.

### 7.3 Ansvar og forsikring

Anmelderen af en elektronisk eID ordning eller Identitetsbroker bærer det fulde ansvar for, at løsningen opfylder kravene beskrevet i denne standard. Anmeldere på niveau 3 og 4 skal påtage sig erstatningsansvar efter dansk rets almindelige regler overfor eID-indehavere samt tjenester, der forlader sig på et eID (*relying parties*), såfremt tabet skyldes:

- at oplysninger i eID er forkerte på tidspunktet for udstedelsen eller manglende spærring på baggrund af gyldig anmodning
- at SAML tokens udstedes i strid med kravene til identitetsbrokere i denne standard,
- manglende umiddelbar spærring eller suspension af eID/esignatur efter anmodning om spærring/suspension,
- alvorlige sikkerhedsbrud som følge af, at sikkerhedskrav ikke er opfyldt,

medmindre anmelderen kan godtgøre, 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 på niveau 3 og 4 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 eID-tjenesteyderen.

## **7.5 Deling af sikkerhedshændelser**

eID-tjenesteydere på niveau 3 og 4 skal af egen drift dele alvorlige sikkerhedshændelser med Digitaliseringsstyrelsen samt andre relevante myndigheder. 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. eID-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 eID mv.

Den Europæiske Unions Agentur for Net- og Informationssikkerhed (ENISA) har udarbejdet retningslinjer for incident rapportering.

## 8 Referencer

- [OIO-A-LEVEL] "Vejledning vedrørende niveauer af autenticitetssikring, IT- og Telestyrelsen". <http://digitaliser.dk/resource/363424>
- [PDL] "Lov om behandling af personoplysninger", Justitsministeriet. <https://www.retsinformation.dk/Forms/r0710.aspx?id=828>
- [SBK] "Sikkerhedsbekendtgørelsen", Justitsministeriet. <https://www.retsinformation.dk/Forms/R0710.aspx?id=842>
- [NSI] "Fællesoffentlige brugerstyringsløsninger - en analyse af sikkerhedsstandarder og -løsninger", NSI.
- [LOA-ØS] "Autenticitetssikring – Vejledning til autenticitetssikringsniveau for den fællesoffentlige log-in-løsning", Version 1.0, 19. september 2008, Økonomistyrelsen. <http://www.skat.dk/getFile.aspx?Id=42163>
- [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] "Electronic Authentication Guideline", NIST Special Publication 800-63-2.
- ENISA "Technical guideline for Incident Reporting" <https://www.enisa.europa.eu/publications/technical-guideline-for-incident-reporting>