DIGITALISERINGSSTYRELSEN

Revisionsvejledning
til
National Standard for
Identiteters Sikringsniveauer (NSIS)

Status: Version 2.0.3

Version: 18.03.2021

1 Indledning

Dette dokument indeholder en revisionsvejledning til version 2.0.1 af National Standard for Identiteters Sikringsniveauer (NSIS).

Ved anmeldelse af en Elektronisk Identifikationsordning og/eller Identitetsbroker til Digitaliseringsstyrelsen, skal der på Sikringsniveau Betydelig og Høj vedlægges en revisionserklæring fra en statsautoriseret revisor eller et overensstemmelsesvurderingsorgan (jf. eIDAS artikel 3, stk. 1, nr. 18).

Dette dokument beskriver kravene til revisionserklæringen og giver vejledning og eksempler på udformning af denne.

Dokumentet er målrettet organisationer, der ønsker at anmelde deres løsninger til Digitaliseringsstyrelsen som Elektronisk Identifikationsordning og/eller Identitetsbroker, samt de revisorer, der skal udarbejde tilhørende erklæringer.

Læsere af dette dokument forventes at have indsigt i NSIS-standarden.

1.1 Skema til anmeldelse

Som supplement til dette dokument er der udarbejdet et Excel-skema, der skal udfyldes og vedlægges anmeldelsen (se bilag A). Skemaet indeholder NSIS kravene og tilhørende felter, som skal udfyldes af henholdsvis anmelder af løsningen og revisor. Derudover findes der en anmeldelsesskabelon med stamoplysninger om den anmeldte løsning samt ledelseserklæring.

De første kolonner i Excel-skemaet indeholder samtlige krav i NSIS opsat på struktureret form og udgør den primære dokumentation for efterlevelsen af kravene. For hvert enkelt krav er det angivet, om kravet er relevant for hhv. Elektroniske Identifikationsordninger, for Identitetsbrokere eller begge typer løsninger. Kun krav, der er relevante for anmeldelse af den pågældende type løsning, skal udfyldes.

I tilknytning til de respektive NSIS-krav indeholder skemaet to kolonner, som skal udfyldes af anmelderen af en løsning, og to kolonner, som efterfølgende skal udfyldes af anmelders revisor:

Anmelders beskrivelse af opfyldelse (Praksis)	Anmelders beskrivelse af kontrolmål (SMART)	Revisionshandlinger ved udført revision	Resultat af udført revision
Udfyldes af NSIS anmelder	*Udfyldes af NSIS anmelder*	*Udfyldes af revisor*	*Udfyldes af revisor*
Udfyldes af NSIS anmelder *Udfyldes af NSIS anmelder*	*Udfyldes af NSIS anmelder* *Udfyldes af NSIS anmelder*	*Udfyldes af revisor* *Udfyldes af revisor*	*Udfyldes af revisor* *Udfyldes af revisor*

Hensigten med de enkelte kolonner gennemgås nedenfor:

- **Anmelders beskrivelse af opfyldelse (praksis)**
  Her beskriver anmelder, hvorledes de tilhørende NSIS-krav på det relevante sikringsniveau er opfyldt. Redegørelsen indeholder en beskrivelse af implementerede tekniske-, processuelle- eller organisatoriske- tiltag. Den kan med fordel udarbejdes i form af en 'praksis' som fx kendes fra dokumentation af overholdelse af certifikatpolitikker (via CPS – Certification Practice Statement).
- **Anmelders beskrivelse af kontrolmål (SMART)**

Her beskriver anmelder i form af kontrolmål, hvordan man konkret kan kontrollere, om den beskrevne praksis er opfyldt / implementeret. Punktet bør formuleres som et SMART[1] krav, så det sikres, at det er entydigt og målbart.

- **Revisionshandlinger ved udført revision**
  Her angiver revisor, hvilke revisionshandlinger og observationer, som benyttes ved vurdering af det konkrete krav.
- **Resultat af udført revision**
  Her udtrykker revisor en konklusion vedr. den udførte revision for det pågældende krav.

I udvælgelsesprocessen af revionshandlingerne ved vurderingen, anbefales det at anvende følgende principper:

Princip	Beskrivelse
Forespørgsel	Interview, møde, forespørgsel med ansvarligt personel hos leverandøren
Observation	Observation af gennemførelsen af kontrol
Inspektion	Gennemgang og evaluering af politikker, procedurer og dokumentation vedrørende kontrollens resultater. Dette omfatter gennemlæsning og evaluering af rapporter og anden dokumentation for at vurdere, om specifikke kontroller er udformet og implementeret. Desuden vurderes det, om kontrollerne overvåges og kontrolleres tilstrækkeligt og med passende intervaller.
Genudførsel af kontrol	Gentagelse af de relevante kontrolelementer for at verificere udførslen af kontrolfunktionerne.

Bemærk at anmelderens udfyldelse af Excel-skemaet (bilag A) bør være dækkende og selvindeholdt. Det er dog tilladt at referere til vedlagte dokumenter i bilag A for yderligere detaljer (fx teknisk dokumentation, certifikater indenfor IT-sikkerhed og / eller beskyttelse af persondata - f.eks. ISO 2700x certifikat, diverse ISAE-erklæringer). Vær dog opmærksom på, at beskrivelsen i skemaet bør være tilstrækkelig dækkende til, at den i sig selv giver en sammenhængende redegørelse for, hvordan kravet er opfyldt.

1.1.1 Eksempel på udfyldelse af skema

I det følgende gennemgås kort et eksempel på udfyldelse af skemaet. Fokus er på at illustreret logikken i skemaet og ikke at give et udtømmende og realistisk eksempel.

Der tages udgangspunkt i flg. krav til verifikation af identitet for fysiske personer på Sikringsniveau Lav, afsnit 3.1.2:

NSIS krav afsnit 3.12

[1] **S**pecific (Specifik), **M**easurable (Målbare), **A**chievable (Opnåelige), **R**elevant (Relevante) og **T**ime-bound (Tidsbestemte)

1) Der skal gennemføres en verifikation, og der skal foreligge en beskrivelse af verifikationsprocessen, herunder de forudsætninger, der lægges til grund.
2) Ansøgeren (Entiteten) skal med overvejende sandsynlighed vurderes at være i besiddelse af almindeligt anerkendt dokumentation for sin Identitet. Dette kan fx være sygesikringskort, pas, kørekort, dåbsattest eller forskudsopgørelse.
3) Dokumentationen kan antages at være ægte og gyldig.

Kolonne i - Anmelders beskrivelse af opfyldelse (praksis)

Ansøgningen gennemføres via en online formular. Her skal alle ansøgere uploade en kopi af dansk pas eller kørekort, som registreres på ansøgningen, samt angive CPR nummer. Det kontrolleres at pas/kørekort ikke er udløbet, og ved opslag i pas- og kørekortregister sikres, at det pågældende dokument ikke er spærret. Ved opslag i CPR-registret sikres, at den pågældende person findes og ikke er død eller meldt savnet. Endelig kontrollerer en sagsbehandler manuelt, at identiteten i CPR-registret stemmer overens til identiteten i pas/kørekort ved at sammenligne for- og efternavne.

Kolonne j - Anmelders beskrivelse af kontrolmål (SMART)

For hver ansøgning findes en logning af et kontrolspor, hvor flg. oplysninger fremgår:

- Oplyst CPR nummer
- Uploadet billede af pas/kørekort
- Resultat af opslag i CPR-registret inkl. navn, adresse og status i CPR
- Resultat af opslag i pas/kørekortregister
- Sagsbehandlers godkendelse af billede inkl. entydig identifikation af sagsbehandler
- Status på sagsbehandlers godkendelse af overensstemmelse mellem identitet i CPR og pas/kørekort

Kolonne k - Revisionshandlinger ved udført revision

Der er udtaget en population på 50 tilfældige ansøgninger og verificeret, at der foreligger en logning for hver ansøgning med alle ovennævnte oplysninger. Det er verificeret, at der for alle godkendte ansøgninger er overensstemmelse mellem identitet i CPR og pas/kørekort, herunder at sagsbehandleren har foretaget en korrekt sammenligning. Det er endvidere verificeret, at ingen ansøgninger, hvor opslag på pas/kørekort/CPR viser ugyldig status, er blevet godkendt.

Der er endvidere forsøgt ansøgning med spærret pas og kørekort og konstateret, at disse afvises af systemet med korrekt fejlkode i loggen.

Endelig er der forsøgt ansøgning med CPR-nummer for død person samt ugyldigt CPR-nummer, og det er konstateret, at disse afvises med korrekt fejlkode i loggen.

Kolonne l – Resultat af udført revision

Revisionen har ikke givet anledning til bemærkninger, og det konkluderes, at de beskrevne procedurer og kontroller er implementeret og effektive.

1.2 Krav til revisionserklæring

Revisor skal udover udfyldelse af ovennævnte skema udarbejde en specifik erklæring om den anmeldte løsning. Revisionserklæringen udarbejdes efter ISAE 3000 standarden eller tilsvarende, og der skal opnås en høj grad af sikkerhed efter denne standard.

Revisionserklæringen har formål at konkludere (på baggrund af indholdet i Excel-skemaet i bilag A for de enkelte krav), hvorvidt anmelder samlet set har etableret alle relevante procedurer og udformet funktionaliteten af kontroller, der knytter sig til procedurer, som beskrevet i NSIS-standarden på det ønskede sikringsniveau. Samtlige krav på et bestemt sikringsniveau skal således være opfyldt for den relevante type løsning, før løsningen kan siges at leve op til det pågældende sikringsniveau.

Det er anmelderens ansvar at udforme alle relevante procedurer og kontroller til sikring af, at kravene i NSIS- standarden overholdes. Det er revisors ansvar at udtrykke en konklusion om, hvorvidt de af ledelsen etablerede procedurer og kontroller var hensigtsmæssigt udformet og implementeret på ansøgningstidspunktet, og hvorvidt disse fungerede hensigtsmæssigt i hele erklæringsperioden (se afsnit 1.2.1nedenfor).

I bilag A er angivet kontrolmål, som skal være omfattet af revisionserklæringen, samt eksempler på konkrete revisionshandlinger, der kan udføres. Revisionen skal omfatte procedurer og kontroller inden for alle kontrolmålene. Det er revisors ansvar at tilpasse revisionshandlingerne til de konkrete procedurer og kontroller, der er etableret hos anmelderen.

1.2.1 Periode for erklæring

Hvis der er tale om en ny løsning under udvikling, kan der anvendes en ISAE 3000 erklæring gående på løsningens design til den første anmeldelse, og erklæringsperioden kan omfatte én given dato, som ikke er på mere end 90 dage fra anmeldelsesdatoen. Hvis løsningen er færdigimplementeret men ikke idriftsat, kan der anvendes en ISAE 3000 type 1 erklæring (design og implementering) til den første anmeldelse, og er der tale om anmeldelse af en kørende løsning, kan der til den første anmeldelse anvendes en ISAE 3000 type 2 erklæring (design, implementering og operationel effektivitet).

Anvendes en ISAE-3000 erklæring alene på design som første erklæring, skal anmelder senest 4 måneder efter idriftsættelsen levere en type-1 erklæring for at sikre, at implementeringen efterlever designet.

Herefter skal anmelder én gang årligt indsende en tilsvarende ISAE 3000 type 2 erklæring fra en godkendt revisor. Erklæringsperioden for disse erklæringer skal dække fra datoen for sidste erklæring. Erklæringen skal være Digitaliseringsstyrelsen i hænde seneste 60 kalenderdage regnet fra den dag, hvor 12-måneders perioden udløber.

Digitaliseringsstyrelsen vil ved gennemgang af revisionserklæringer fra anmelder anvende kontrolmål fra Excel-skemaet til at vurdere, om revisors erklæring omfatter de nødvendige forhold. Hvis der er områder, som ikke er relevante, skal anmelders revisor begrunde, hvorfor forholdet ikke er relevant. Eksisterer der forhold, som er væsentlige og som ikke er indeholdt i områderne nedenfor, skal disse områder medtages i den afgivne revisionserklæring.

I det tilfælde at en revisionserklæring afgives med forbehold, kan dette medføre afvisning eller afnotering som godkendt udbyder af en Elektronisk Identifikationsordning eller Identitetsbroker. I det tilfælde der fremgår bemærkninger af erklæringen (ofte af mindre væsentlig karakter), skal Digitaliseringsstyrelsen senest 60 kalenderdage fra erklæringsperiodens

udløb modtage en skriftlig redegørelse fra anmelder indeholdende en beskrivelse af forholdene og en detaljeret handlings- og tidsplan for udbedring af forholdet. Overholdes dette ikke, kan dette ligeledes medføre afnotering.

1.2.2 Opdateringer efter anmeldelse

Hvis der foretages signifikante ændringer til den anmeldte løsning, kan der uden for den normale revisionscyklus beskrevet ovenfor indsendes en opdateret anmeldelse med en 'delta-erklæring', som adresserer de relevante ændringer, hvorefter Digitaliseringsstyrelsen registrering af løsningen kan blive opdateret. Eksempler på sådanne signifikante ændringer kunne være, at løsningen opdateres fra at være på sikringsniveau Betydelig til Høj, at der indføres helt nye typer af identifikationsmidler eller helt nye processer for identitetssikring etc. Ændringer til løsningen, der ikke vurderes som signifikante, medfører ikke krav om ny anmeldelse, og vil blive håndteret af den næste, årlige revision.

1.2.3 Håndtering af serviceleverandører

Hvis anmelder anvender serviceleverandører, underleverandører eller tilsvarende, skal anmelders erklæring som udgangspunkt udformes efter 'helhedsmetoden', så alle leverandører i kæden er omfattet af samme erklæring. Helhedsmetoden er en metode til håndtering af de ydelser, en serviceunderleverandør leverer, hvor serviceleverandørens beskrivelse af sit system omfatter arten af de ydelser, en serviceunderleverandør leverer, og hvor serviceunderleverandørens relevante kontrolmål og tilknyttede kontroller indgår i serviceleverandørens beskrivelse af sit system og i omfanget af serviceleverandørens revisors opgave.

Hvis brug af helhedsmetoden ikke er praktisk mulig, kan partielmetoden undtagelsesvis anvendes på underleverandører af kommercielle standardløsninger, og der skal så vedlægges en supplerende begrundelse for, hvorfor helhedsmetoden ikke er anvendt i henhold til 'følg-eller-forklar' princippet.