Digitaliseringsstyrelsen · Landgreven 4 · Postboks 2193 · 1013 København K

Til høringsparterne

Maj 2024

Høring over opdateringer i standard, vejledning og revisionsvejledning til National Standard for Identiteters Sikringsniveauer (NSIS)

Digitaliseringsstyrelsen har i foråret 2024 foretaget en evaluering af National Standard for Identiteters Sikringsniveauer, herefter kaldet NSIS. Evalueringen er gennemført i samarbejde med Kommunernes Landsforening (KL), kommuner, regioner, revisorer og andre interessenter på NSIS-positivlisten.

På baggrund af erfaringer med implementering og anvendelse af NSIS samt den gennemførte evaluering er standarden, vejledning og revisionsvejledning til NSIS blevet revideret. Den reviderede standard, vejledning til NSIS og revisionsvejledning sendes hermed i bred offentlig høring.

Digitaliseringsstyrelsen har tilstræbt at præcisere og tilrette dokumenterne med henblik på en klarere forståelse for standardens krav samt en tydeligere og enklere anmeldelses- og revisionsproces for alle anmeldere.

De vigtigste ændringer i de tre opdaterede NSIS-dokumenter

Nedenfor er oplistet de vigtigste ændringer i de reviderede NSIS-dokumenter. Der findes endvidere mindre detailændringer, som ikke fremgår af denne oversigt. Ændringer fremgår med ændringsmarkeringer, og høringsparterne opfordres til at gennemgå de reviderede dokumenter i detaljer:

National Standard for Identiteters Sikringsniveauer (NSIS)
• Terminologiafsnittet er udbygget med forklaring af centrale begreber (Lokal IdP og FullService IdP), og der er indført en ny illustration af begreberne Entitet, Digital Identitet og Identifikationsmiddel. • Der er indført et afsnit om 'tillidskæden for digitale identiteter' med henblik på at forklare roller og ansvar for de forskellige parter, der håndterer digitale identiteter. • Der er indført en præcisering af, hvornår et eksisterende identifikationsmiddel kan anvendes til at udstede et nyt identifikationsmiddel. • Krav 4.1.1 punkt 2) om overholdelse af lovgivning undtages fra revisionspligten, da der ikke føres tilsyn fra Digitaliseringsstyrelsen med overholdelse af generel lovgivning. • Forhold omkring oplysningspligten er præciseret.

- Revisionserklæringer kan udformes af registrerede revisorer og statsautoriserede revisorer med relevante faglige kompetencer (4.1.7).
- I afsnit 7.2 er det præciseret, at man ved nedlukning af en ID-tjeneste skal aflevere en afsluttende revisionserklæring for at undgå, at der findes længere perioder uden revision og dermed mulig tvivl om sikkerheden i perioden.
- I afsnit 7.3 er formuleringen omkring ansvar bragt i overensstemmelse med standardens krav, herunder at erhvervsansvarsforsikringer i visse sammenhænge kan erstattes af andre ordninger.

Vejledning til National Standard for Identiteters Sikringsniveauer
• Vejledning er udbygget vedr. kontrol af legitimation (3.1.2) ved verifikation af fysiske personer samt retningslinjer for validering af digitale kørekort. • Vejledning er udbygget vedr. levering og aktivering (3.2.2), herunder fortolkning af kravene ved elektroniske udleveringsprocesser. • Der er indført eksempler på, hvornår automatisk spærring kan være aktuel (3.2.3). • Sikkerhed af autentifikationsmekanismer er udbygget (3.3.1). • Sikkerhedstest af autentifikationsmekanismer er udbygget (3.3.1). • Håndtering af underleverandører og deres ansvar er mere detaljeret beskrevet (4.1.1). • Der er beskrevet eksempler på alternativer til ansvarsforsikringer (4.1.1 punkt 4). • Bestemmelser vedr. oplysningspligt er udbygget (4.1.2). • Vejledning til ISMS er udbygget (4.1.3). • Krav til fysisk sikkerhed er udbygget (4.1.5 punkt 3). • Beskrivelser af betroede medarbejdere og baggrundstjek er udbygget (4.1.5 punkt 5). • Vejledning til nøglelængder og kryptografi er udbygget (4.1.5 punkt 7). • Håndtering af medarbejderidentiteter (kapitel 5) er væsentligt udbygget, herunder vedrørende spærring og brug af autoritative kilder og procedurer for medarbejderes livscyklus. • Vejledning vedrørende omveksling af eIDAS til NSIS-sikringsniveauer er indført i afsnit 6.1 og 6.2. • Forhold vedr. sessionsstyring for brokere er udbygget (6.5). • Logningskrav er udbygget (6.7).

I mange tilfælde refererer vejledningsteksterne nu til de tilsvarende områder i ISO 27001 Annex A, således at anmeldere lettere kan genfinde kontrolbeskrivelser og andet eksisterende materiale fra deres øvrige sikkerhedsarbejde.

Revisionsvejledning til National Standard for Identiteters Sikringsniveauer
• Dokumenttitel ændret fra "Revisionsvejledning til National Standard for Identiteters Sikringsniveauer (NSIS)" til "Vejledning om anmeldelses- og revisionsproces for National Standard for Identiteters Sikringsniveauer (NSIS)" for at tydeliggøre, at dokumentet ikke kun er rettet mod revisorer men også mod anmelderne. • Struktur: Opdeling af kapitler. • Eksempler på udfyldelse af skema er uddybet og præciseret (2.1.1) • Afsnit 1.3 Krav til revisionserklæringer er ændret til kapitel 3: Anmeldelser på niveau Betydelig og Høj. • Præcisering af krav til dokumentation for tilsyn med underleverandører (3.4). • Udvidelse af frist for indsendelse af Type 2-erklæringer fra 60 kalenderdage til 90 kalenderdage fra den dag, hvor 12-måneders perioden udløber (3.1). • Nyt kapitel om anmeldelser på niveau Lav (kapitel 4). • Nyt kapitel indført om anmeldelse af flere organisatoriske enheder (CVR-numre) (kapitel 5). • Nyt kapitel indført om forhold der kan medføre afnotering (kapitel 6). • Nyt kapitel indført om revision ved ophør af ID-tjeneste (kapitel 7).

Videre proces

Den endeligt reviderede standard, vejledning og revisionsvejledning til NSIS forventes publiceret i juni 2024.

Figur 1: Videre proces op til udgivelsen af de tre endeligt reviderede NSIS-dokumenter.

Høringen er sendt til de myndigheder og organisationer m.v., der fremgår af vedlagte høringsliste.

De tre reviderede NSIS-dokumenter samt dette høringsbrev offentliggøres desuden på Høringsportalen på www.hoeringsportalen.dk. På baggrund af modtagne høringssvar udarbejdes et høringsnotat, som offentliggøres på Høringsportalen efter høringsfristens udløb sammen med eventuelle yderligere tilretninger til de tre NSIS-dokumenter.

Frist og kontaktmulighed

Interessenter og høringsparter opfordres til at afgive kommentarer og supplerende oplysninger, som findes relevante for høringen.

Digitaliseringsstyrelsen anmoder om, at eventuelle bemærkninger til de tre reviderede NSIS-dokumenter sendes pr. e-mail til tilsyn_nsis@digst.dk **senest søndag den 2. juni 2024 kl. 23:59.**

Eventuelle spørgsmål til de tre reviderede dokumenter kan også sendes til ovenstående e-mail.