DIGITALISERINGSSTYRELSEN

Til høringsparterne
Se vedlagte liste

26. juni 2018

Høring i forbindelse med opdatering af National Standard for Identiteters Sikringsniveau til version 2.0.

Digitaliseringsstyrelsen har revideret vedlagte Nationale Standard for Identiteters Sikringsniveauer til version 2.0, herefter kaldet NSIS, sammen med den tilhørende vejledning på baggrund af de første erfaringer med arbejdet med standarden. Høringen er sendt til de myndigheder og organisationer m.v., der fremgår af vedlagte høringsliste.

Høringsbrev, høringsliste og NSIS standard og tilhørende vejledning er også tilgængeligt på høringsportalen.

Baggrund

Der anvendes i dag en lang række forskellige digitale identitetsløsninger og akkreditiver i forskellige sammenhænge, til forskellige behov - og med tilsvarende forskellige sikringsniveauer.

I en digital fremtid, hvor der er behov for at skabe sammenhængende tjenester og forretningsprocesser på tværs af organisationer, domæner, teknologier og på tværs af private og offentlige grænser, er der i stigende grad brug for en fælles ramme for tillid til digitale identiteter.

Korrekte digitale identiteter er en forudsætning for, at borgere og virksomhedernes medarbejdere sikkert kan agere digitalt med myndigheder, virksomheder og med hinanden.

I forbindelse med arbejdet med valide identiteter i den offentlige sektor og arbejdet med at anskaffe MitID og NemLog-in3 er der identificeret et behov for at indføre mulighed for større fleksibilitet i forbindelse med identifikation over for forskellige selvbetjeningsløsninger (flere sikringsniveauer) og samspil mellem løsninger på tværs af den offentlige sektor. Samtidig har EU- Kommissionen i medfør af eIDAS forordningen vedtaget en gennemførelsesretsakt vedr. sikringsniveauer (Levels of Assurance, LoA) (EU) 2015/1502 (EU) 910/2014. Digitaliseringsstyrelsen udarbejdede på den baggrund i 2016 en dansk pendant som en National Standard for Identiteters Sikringsniveauer, hvis formål er at skabe rammer for tillid til digitale identiteter samt digitale identitetstjenester, og som definerer fire sikringsniveauer for identitetssikring og autentifikation.

Den danske standard er baseret på den nævnte gennemførelsesretsakt om sikringsniveauer, således at der bliver en konsistent vurdering af, hvilket sikringsniveau en løsning har, når den anvendes internt i Danmark henholdsvis i et andet EU-land. I relevante sammenhænge er kravene i NSIS dog præciseret i

forhold til eIDAS-forordningen for at sikre et sikringsniveau tilpasset danske forhold og tillid mellem danske tjenester og eID-løsninger. Inden Digitaliseringsstyrelsen offentliggjorde standarden i 2016, blev den sendt i bred offentlig høring hos en række organisationer og myndigheder.

Anmeldelsesblanket, revisionserklæringer og vejledning til standarden blev herefter udgivet i juni 2017.

Behov for opdatering

Siden første udgave af NSIS fra 2016 er der sket en række udviklinger inden for identitetsområdet, som har nødvendiggjort en opdatering af standarden:

- Første udgave af NSIS blev skrevet parallelt med, at de implementerende retsakter og vejledning for eIDAS sikringsniveauer blev udarbejdet, hvilket har ført til en række forskelle.

- Siden publiceringen af NSIS har Digitaliseringsstyrelsen udarbejdet en fællesoffentlig referencearkitektur for brugerstyring. Dette har affødt et behov for at klarlægge og ensrette terminologien i NSIS, så den er i overensstemmelse med referencearkitekturen.

- Digitaliseringsstyrelsen har modtaget en række spørgsmål og tilbagemeldinger fra interessenter og dels gjort sig en række erfaringer i arbejdet med MitID og NemLog-in3 projekterne, herunder i forhandlingsforløbet med leverandørerne. I forhold til den nuværende infrastruktur vil NemLog-in3 eksempelvis introducere føderation med lokale IdP'er og overtage erhvervsløsningen fra NemID, hvorfor der er behov for at håndtere sikringsniveauer for juridiske personer i NSIS.

- Der er et arbejde i gang i Digitaliseringsstyrelsen med at revidere de nuværende certifikatpolitikker for OCES certifikater, hvilket også indebærer en koordinering og tilretning i NSIS.

- I forbindelse med Digitaliseringsstyrelsens deltagelse i internationale arbejdsgrupper under eIDAS forordningen samt i processen med notificering af elektroniske identifikationsordninger fra andre EU-lande, er fortolkningen af lovgivningen blevet tydeligere, hvilket der kan være et behov for at afspejle i NSIS.

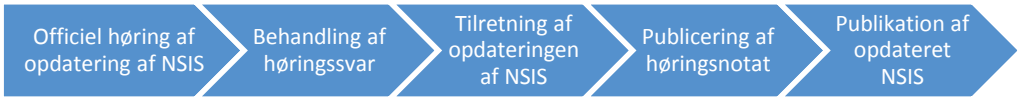
De vigtigste ændringer i NSIS 2.0

Nedenfor er oplistet de vigtigste ændringer i NSIS 2.0 – der er dog mange detailændringer, så høringsparterne opfordres til at gennemgå den nye version i detaljer:

- Terminologien er blevet ensrettet med den fællesoffentlige referencearkitektur for brugerstyring, bl.a. anvendes begrebet 'akkreditiv' nu konsekvent i stedet for forkortelsen 'eID'. Endvidere er dele af begrebsmodellen fra referencearkitekturen indsat som støttende forklaring.
- Det laveste sikringsniveau "Begrænset" er udgået, da det ikke havde nogen reel anvendelse, og da eIDAS forordningen endvidere kun opererer med tre sikringsniveauer. De tre tilbageværende niveauer (Lav, Betydelig, Høj) bibeholdes.
- Beskrivelsen af begrebet sikringsniveau (LoA) er blevet suppleret med de underliggende dele, herunder IAL (Identity Assurance Level) som beskriver styrken af Identitetssikringen, og AAL (Authentication Assurance Level) som beskriver Autentifikationsprocessens styrke, og FAL (Federation Assurance Level), som beskriver sikringsniveau'et for en Identitets-broker.
- Kravene til binding (associering) mellem Akkreditiver for fysiske og juridiske personer er blevet tydeliggjort.
- Det er indført som nyt krav, at der skal gives en kvittering for spærring.
- Der er som et nyt område i NSIS indført krav til identitetssikring af juridiske personer.
- Krav til identitetssikring af fysiske personer er justeret, bl.a. er kravene til kontrolspørgsmål blevet erstattet af mere generelle krav til at håndtere risikoen for at fremlagte beviser kan være blevet tabt, stjålet, suspenderet, tilbagekaldt eller være udløbet.
- Der fremgår nye krav i medfør af GDPR.
- Kravene om ISO 27001 certificering på niveau 'Høj' er omformuleret, således at organisationen på andre, tilsvarende måder kan dokumentere efterlevelsen af krav til informationssikkerhedsledelse.
- Krav til end-to-end kryptering af security tokens for identitetsbrokere er omformuleret, således at dette kun er påkrævet, når der kommunikeres via brugerens browser eller tokenet indeholder følsomme personoplysninger.
- Krav om, at medarbejdere og ledelse skal sikkerhedsgodkendes i henhold til statens sikkerhedscirkulære udgår. I stedet fremgår, at det generelt 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.
- Sikkerhedskrav til identitetsbrokeres håndtering af private nøgler er skærpet.

Bemærk, at ovenstående ikke er en udtømmende liste over ændringer og således blot kan opfattes som udvalgte eksempler.

Videre proces
NSIS version 2.0 forventes publiceret ultimo oktober 2018, og den følgende proces er illustreret i nedenstående figur 1.



Figur 1 – illustration af den følgende proces indtil publicering af opdateringen af standarden.

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

Det skal understreges, at kravene i NSIS 2.0 og den tilhørende vejledning er foreløbige og kan blive ændret som følge af høringssvarene.

Digitaliseringsstyrelsen vil efter modtagelse af høringssvar udarbejde høringsnotat, eventuelle tilretninger til NSIS samt den tilhørende vejledning, der publiceres sammen med standarden. Efter den opdaterede standard er endelig, opdateres den tilhørende anmeldelsesformular og revisionserklæring.

Digitaliseringsstyrelsen anmoder om, at bemærkninger til den vedlagte offentlige standard for identiteters sikringsniveau NSIS 2.0 sendes til saslh@digst.dk. Høringssvar skal være Digitaliseringsstyrelsen i hænde **senest mandag den 3. september 2018 kl. 12:00.**

Eventuelle spørgsmål vedrørende standarden sendes til Sandra Schöne Leth Hansen saslh@digst.dk.