SignaturGruppen

Signaturgruppens NSIS program

Registrering af medarbejdere på NSIS sikringsniveau betydelig.

NSIS er den nye standard, der supplerer NemID medarbejdersignatur fremadrettet, når medarbejderne skal på nationale tjenester, som behandler følsomme data. NSIS er udgivet i en version 1.1 pr. 05.01.2017 og der er udsendt en høringsversion 2.0 pr. 26.06.2018.

For at blive compliant med NSIS sikringsniveauerne betydelig og høj (også benævnt Assurancelevel 3 og 4 i refererende dokumenter fra f.eks. AULA og fælleskommunal rammearkitektur), skal organisationerne årligt indlevere en revisionserklæring fra en uafhængig statsautoriseret revisor om overholdelsen af NSIS standardens krav. Revisionserklæringen skal suppleres af en ledelseserklæring.

Dette whitepaper opsamler Signaturgruppens anbefalinger i forhold til etablering af sikker registrering af medarbejdere, som kan opfylde kravene i NSIS på sikringsniveau betydelig.

Kravene til registrering af medarbejdere på NSIS betydlig

Herunder vises de centrale krav fra NSIS høringsversion 2.0.

NSIS 2.0 afsnit 3.1.2 ser for niveau betydelig således ud:

Betydelig	4) 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 de samme identifikationsprocesser som benyttes ved udstedelse af dansk pas eller kørekort anvendes. 5) Dokumentation kontrolleres med henblik på at fastslå, at den er gyldig 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 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. 7) 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. 8) Hvis registreringen gennemføres af en anden person end ansøgeren, skal denne være autentificeret på sikringsniveau Betydelig eller Høj.

NSIS 2.0 afsnit 3.1.2 betydelig – Verifikation af identitet

De eksisterende registreringsprocedurer for NemID, som bla. Kommunernes borgerservice understøtter, vurderes at opfylde kravene på NSIS sikringsniveau betydelig. Praktisk talt skal man etablere lignende procedurer og uddannelse for selv at registrere medarbejdere på NSIS sikringsniveau betydelig, hvilket er en opfattende opgave!

NSIS giver dog også mulighed for at anvende f.eks. privat NemID til at registrere en erhvervsidentitet, som det ses af nedenstående udpluk af NSIS 2.0 afsnint 3.1.2.

> Kravene i nedenstående tabel er møntet på ny-udstedelse baseret på ikke-elektronisk dokumentation. Generelt er det tilladt at basere identifikation på Autentifikation med gyldige Akkreditiver på mindst samme NSIS Sikringsniveau, såfremt de nødvendige oplysninger (personidentifikationsdata) tilvejebringes gennem denne Autentifikation. Akkreditiver behøver ikke være fra den samme udsteder. Her skal det i givet fald kunne verificeres, at det pågældende Akkreditiver er gyldige og ikke spærret.

NSIS 2.0 afsnit 3.1.2 betydelig – Verifikation af identitet

Hvad anbefaler Signaturgruppen?

Signaturgruppen anbefaler, at organisationerne understøtter selvbetjent registrering af medarbejderidenitets med autentifikation med privat NemID, da dette er den simpleste, sikreste og mest effektive løsning.

Er det derudover nødvendigt at kunne understøtte en manuel registreringsproces? Vi mener det som udgangspunkt ikke. I mange organisationer er der dog en forsigtighed omkring anvendelse af privat NemID i arbejdssammenhæng. Datatilsynet har i 2012 udtalt sig om anvendelsen af privat NemID som medarbejder login i Kommuner[1].
Hovedhensynet her er at anvendelsen af privat NemID til log-in skal være et frivilligt tilbud.
Det er dog ikke anvendelsen af privat NemID til udstedelse af en medarbejderidentitet, som Datatilsynets udtalelse går på, men derimod daglig brug i arbejdssammenhæng.

Privat NemID anvendes allerede i dag i forbindelse med straksudstedelse af NemID medarbejdersignatur. De kommende NemLog-in3 medarbejderidentiteter vil også som hovedregel basere sig på autentifikation med det kommende private MitID, som det for eksempel ses i dokumentet "Notat om fremtidens infrastruktur for digitale identiteter"[2], hvorfra nedenstående udklip stammer.

[1] https://www.datatilsynet.dk/tilsyn-og-afgoerelser/historiske-afgoerelser/2012/mar/udtalelse-til-kl-om-brug-af-privat-nemid-som-medarbejder-log-in-i-kommuner-opdateret/
[2] https://digst.dk/media/13657/fremtidens-infrastruktur-for-digitale-identiteter_tilg%C3%A3-ngeliggjort.pdf

Registreringsautoriteter i erhvervsløsningen

Virksomheder og andre organisationer med et tilknyttet CVR-nummer vil fortsat have mulighed for at oprette medarbejderidentiteter som med den hidtidige administrator-rolle i NemID Medarbejdersignatur. Dog vil der ske en ændring i forhold til opretholdelse af de sikringsniveauer for personidentiteter, der defineres med NSIS-standarden. Virksomheder vil som udgangspunkt kun kunne udstede erhvervsidentiteter til deres medarbejdere på det NSIS-sikringsniveau, de kan certificeres til. Efterfølgende vil det være muligt at hæve sikringsniveauet for en sådan identitet til det ønskede niveau, fx ved at medarbejderen validerer sin erhvervsidentitet ved hjælp af sin private personidentitet (eller en anden personlig erhvervsidentitet).

"Notat om fremtidens infrastruktur for digitale identiteter"

Signaturgruppen anbefaler at selvbetjent registrering af medarbejderne med privat NemID integreres i brugernes dagligdag, sådan som SoloID løsningspaletten gør. Ved brugerens første anvendelse af SoloID opfordres brugeren til at registrere sig med privat NemID, og SoloID løsningen samler derefter den nødvendige dokumentation og logning til understøttelse af den årlige NSIS revision.

Figur: Vigtigste løsningsvarianter for SoloID

SoloID – Sikker som NemID, let som SMS