Digitaliserings-
styrelsen

# Vejledning til valg af NSIS-Sikringsniveau for tjenesteudbydere

Version 2.0.3 (opdateret 3. december 2024)

## Introduktion

Denne vejledning er henvendt til offentlige myndigheder og sekundært private tjenesteudbydere, som udbyder online tjenester med behov for brugerautentifikation – eksempelvis digitale selvbetjeningsløsninger henvendt til borgere og virksomheder. Vejledningen guider til valg mellem de tre Sikringsniveauer (hhv. Lav, Betydelig og Høj), der er beskrevet i National Standard for Identiteters Sikringsniveauer (NSIS). Dette sker ved at forklare ansvar og forpligtelser samt illustrere, hvordan en vurdering af nødvendigt Sikringsniveau kan gennemføres på baggrund af en risikovurdering.

NSIS har fokus på at definere tre Sikringsniveauer samt stille krav til Elektroniske Identifikationsordninger og Identitetsbrokere som *udsteder* Elektroniske Identifikationsmidler og *videreformidler* Identiteter på disse Sikringsniveauer.

Denne vejledning har fokus på den modsatte side, nemlig *tjenesteudbydere, der aftager Identiteter* (i form af autentificerede brugere) fra disse løsninger og skal give adgang til deres tjeneste på baggrund af den tillid, der følger af Sikringsniveauet. Den grundlæggende præmis er, at Sikringsniveauet, som en bruger opnår gennem autentifikation, mindst skal modsvare det krævede Sikringsniveau for den forretningstjeneste, som ønskes tilgået.

Den primære målgruppe for dokumentet er it-ansvarlige, projektledere og it-arkitekter hos offentlige myndigheder, men principperne kan sagtens anvendes af private tjenesteudbydere også. I en vis udstrækning gælder dette også tjenesteudbydere, der i medfør af eIDAS-forordningen udbyder tjenester til borgere og virksomheder i andre EU-lande, idet eIDAS opererer med tilsvarende Sikringsniveauer til [NSIS].

## Terminologi

Denne vejledning anvender samme terminologi som NSIS, hvorfor der henvises til denne for forklaring af begreber. Begreber med stort begyndelsesbogstav er således defineret i [NSIS].

For en detaljeret behandling af, hvordan Sikringsniveauer for Identiteter opnås for Elektroniske Identifikationsordninger og Identitetsbrokere, henvises til [NSIS]. For yderligere, generelle informationer om håndtering af it-sikkerhed og -risici henvises til ISO 27000-familien af standarder.

## Baggrund og motivation

Håndteringen af differentierede Sikringsniveauer er et afgørende element i den nationale, digitale identitetsinfrastruktur i form af MitID- og NemLog-in3-løsningerne. I denne infrastruktur findes et bredere udvalg af Elektroniske Identifikationsmidler på forskellige Sikringsniveauer.

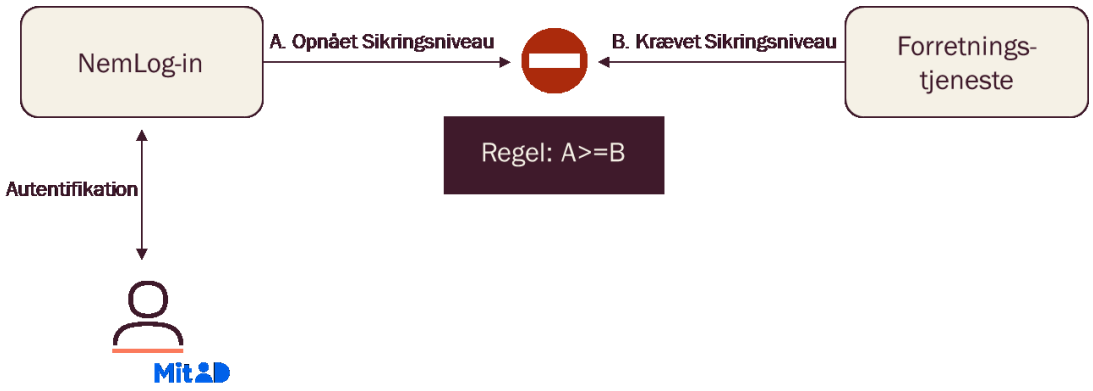
På den anden side har forretningstjenester forskellige behov for sikkerhed for brugernes Identitet, og krav til Sikringsniveau bør stilles ud fra en konkret vurdering af tjenestens behov og risikoprofil - herunder konsekvenserne ved forkert identifikation af brugere. Eksempelvis kan der være stor forskel på konsekvenserne af fejlagtigt log-in til sundhed.dk sammenlignet med en side hos en kommune, hvor borgerne kan bestille tid hos borgerservice.

Ovenstående betyder, at tjenesteudbydere aktivt skal tage stilling til valg af nødvendigt Sikringsniveau for deres tjeneste på baggrund af en risikovurdering.

## Samspil med NemLog-in

I praksis vil offentlige tjenesteudbydere anvende NemLog-in-løsningen som broker til at få autentificeret slutbrugere og få fastlagt et aktuelt NSIS-Sikringsniveau for autentifikationen. Principperne er helt de samme, hvis der anvendes en anden Identitetsbroker, som lever op til NSIS.

Efter brugerautentifikation skal tjenesten beslutte, om adgang til forespurgte ressourcer/data kan tildeles (adgangskontrol) ud fra en adgangspolitik. Kontrol af brugerens aktuelle Sikringsniveau er en del af adgangskontrollen, og sker i praksis ved at inspicere den attribut i tokenet fra NemLog-in (eller tilsvarende Identitetsbroker), som angiver brugerens aktuelle Sikringsniveau. Dette er illustreret på nedenstående figur:




Figur 1: Kontrol af Sikringsniveau i tjeneste

Nedenfor er angivet en række tænkte eksempler, som illustrerer princippet:

a) En kommunal tjeneste til bestilling af ekstra skraldespande kan ud fra en risikovurdering komme frem til, at det er tilstrækkeligt, at brugerne er autentificeret på Sikringsniveau Lav. En bruger, som anvender et Elektronisk Identifikationsmiddel på dette niveau (fx baseret på brugernavn/kodeord), bør derfor få adgang.
b) En tjeneste, som giver borgere adgang til egne sundhedsdata, kan ud fra en risikovurdering komme frem til, at det er nødvendigt, at brugerne er autentificeret på mindst Sikringsniveau Betydelig. En bruger, som anvender et Elektronisk Identifikationsmiddel på dette niveau (fx baseret på MitID chip) bør derfor få adgang. Derimod skal en bruger, som anvender et Elektronisk Identifikationsmiddel på Sikringsniveau Lav, blive afvist af tjenesten.
c) En tjeneste, som giver sundhedsfaglige medarbejdere adgang til følsomme personoplysninger om et meget stort antal borgere, kan ud fra en risikovurdering komme frem til, at det er nødvendigt, at brugerne er autentificeret på Sikringsniveau Høj[1]. En bruger, som anvender et Elektronisk Identifikationsmiddel på dette niveau (fx baseret på sikker hardware som et smart card), bør derfor få adgang[2]. Derimod skal en bruger, som anvender et Elektronisk Identifikationsmiddel på niveau Lav eller Betydelig, blive afvist af tjenesten.

## NemLog-ins vilkår

Tjenesteudbydere, der tilslutter tjenester til NemLog-in, er ifølge Digitaliseringsstyrelsens vilkår forpligtede til at gennemføre en formel risikovurdering af tjenestens krav til Sikringsniveau for brugeridentiteter. Endvidere skal tjenesteudbydere gennem NemLog-ins obligatoriske test cases i forbindelse med tilslutningsprocessen sikre, at brugere på for lavt Sikringsniveau afvises af tjenesten. Dette arbejde skal ses som et led i tjenesteudbydernes generelle ansvar for, at et tilstrækkeligt sikkerhedsniveau etableres for egne tjenester. For tjenester, der behandler personoplysninger, vil dette endvidere være en naturlig del i overholdelse af databeskyttelsesforordningens krav.

For digitale selvbetjeningsløsninger, der ikke er tilsluttet NemLog-in, er vurdering af behov for NSIS-Sikringsniveau ikke et formelt krav men dog en klar anbefaling, der bl.a. følger af den fællesoffentlige referencearkitektur for brugerstyring [REF-ARK].

Det skal understreges, at tjenesteudbydere *ikke* bør antage, at brugere autentificeret via NemLog-in automatisk er logget på med MitID eller digital signatur (eller opnår niveau "Betydelig" i NSIS), idet NemLog-in og MitID omfatter flere Identifikationsmidler og Sikringsniveauer. Brugerens aktuelle Sikringsniveau vil altså afhænge af hvilket Elektronisk Identifikationsmiddel, brugeren vælger at anvende til den konkrete autentifikation. Tjenesteudbydernes systemer *skal* derfor aktivt kontrollere brugerens aktuelle Sikringsniveau mod løsningens krav[3].

[1] Bemærk, at det først med MitID-infrastrukturen blev muligt at få udstedt Elektroniske Identifikationsmidler på Sikringsniveau Høj.
[2] Naturligvis forudsat at øvrige betingelser i adgangspolitikken er opfyldt.
[3] Denne kontrol skal efterprøves i praksis inden systemet sættes i drift.

Ansvarsområderne er summeret i nedenstående skema:

**Ansvar for Identitetsbroker (fx NemLog-in):**

- Autentificere bruger.
- Udstede adgangsbillet med opnået NSIS-Sikringsniveau.

**Ansvar for tjenesteudbyder:**

- Vurdere krævet Sikringsniveau på baggrund af risikovurdering.
- Verificere SAML-adgangsbillet for brugere udstedt af Identitetsbroker.
- Sammenligne opnået NSIS-Sikringsniveau i adgangsbillet med krævet Sikringsniveau.
- Håndhæve adgangspolitik og give korrekt adgang til data og funktioner på baggrund af opnået Sikringsniveau og øvrige forhold (herunder autorisationer). Dette omfatter bl.a. at afvise brugere med for lavt Sikringsniveau.

## Vurdering af Sikringsniveau

Den resterende del af denne vejledning har til formål at give forslag til, hvorledes tjenesteudbydere konkret kan fastlægge krav til Sikringsniveau for deres tjenester (som beskrevet ovenfor). Det beskrives *ikke*, hvorledes tjenesteudbydere teknisk bygger kontrollen af brugersessionens aktuelle niveau mod det krævede niveau ind i adgangskontrollen i deres løsninger, da dette vil variere betydeligt fra system til system. De fleste systemer til adgangskontrol er dog temmelig fleksible, og kan relativt let konfigureres til at tage højde for dette i adgangsbeslutninger.

Bemærk endvidere, at denne vejledning *ikke* beskæftiger sig med autorisation på anden måde end håndtering af Sikringsniveau for Identiteter. Det er således tjenesteudbyderens eget ansvar at definere en lokal politik for, hvem der skal have adgang til hvilke ressourcer.

### Risikovurdering

Det er som tidligere nævnt den dataansvarlige myndigheds eneansvar at fastlægge krav til Sikringsniveauer for egne forretningstjenester, som aftager Identiteter. Dette gøres bedst på baggrund af en risikovurdering, der bl.a. tager højde for nedenstående aspekter:

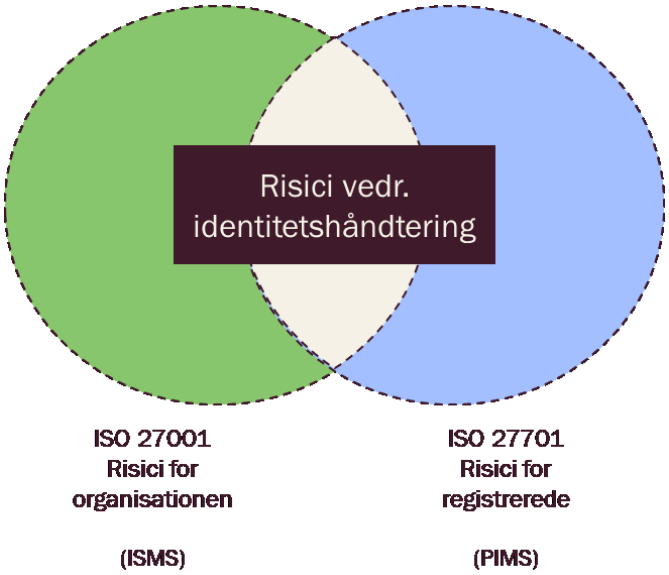
a) Risici for tjenesteudbyderen selv.
b) Risici for de registrerede (hvis tjenesten udstiller eller på anden måde behandler personoplysninger).

En bruger med en 'forkert' identitet, som tilgår en tjeneste, kan således udløse negative konsekvenser af begge slags.

Som generelt metodegrundlag for gennemførsel af risikovurdering kan peges på ISO/IEC 27005, der er målrettet risici for organisationen, og ISO/IEC 27701 som adresserer risici for registrerede.

En risikobaseret tilgang er i tråd med databeskyttelsesforordningen (GDPR), som forudsætter, at den dataansvarlige (og i øvrigt også databehandlere) træffer passende tekniske og organisatoriske foranstaltninger for at sikre et sikkerhedsniveau, der matcher identificerede risici. Tjenesteudbyderens valg og implementering af et bestemt NSIS-Sikringsniveau i tjenesten kan med andre ord opfattes som en del af de foranstaltninger, som skal træffes, og som naturligvis skal suppleres med en lang række øvrige tiltag.

Nedenstående figur illustrerer NSIS i en risikokontekst, hvor risici vedr. digitale identiteter er en lille (men vigtig) delmængde af de samlede risici, en tjenesteudbyder skal håndtere både i forhold til egen organisation og i forhold til registrerede:




Figur 2: NSIS-vurdering som en del af den samlede risikohåndtering

Risici vedr. digitale identiteter, som håndteres og kvantificeres af NSIS, spiller således ind i både ISMS (Information Security Management System) for organisationen og PIMS (Privacy Information Management System) for personoplysninger.

**Vurdering af Sikringsniveau gennem Excel-ark**

Til at støtte tjenesteudbydere i vurderingen af behov for Sikringsniveau har Digitaliseringsstyrelsen i samarbejde med KOMBIT udarbejdet et Excel-ark, som er publiceret på digst.dk/NSIS/. Værktøjet er bevidst holdt simpelt og skal alene betragtes som en støtte til vurderingen, som guider gennem relevante overvejelser. Der vil som oftest være særlige forhold i en tjeneste, som ikke kan dækkes af et generelt værktøj, og værktøjet skal derfor anvendes forsigtigt og med dette for øje:

| |
|---|
| Valg af Sikringsniveau er i sidste ende en forretningsmæssig og sikkerhedsmæssig samlet vurdering, som ikke kan dikteres af et Excel-ark. |

For at kunne fastlægge det rette Sikringsniveau for Identiteter, er det relevant at identificere mulige konsekvenser af, at brugerens Identitet ikke er fastslået tilstrækkeligt eller korrekt – fx ved at en bruger kan udgive sig for at have en anden Identitet end den faktiske, eller ved en fejl har fået tildelt en forkert identitet. Konsekvenserne vil variere vidt fra system til system og fra brugergruppe til brugergruppe. Eksempelvis kan konsekvenserne af at en superbrugers eller administrators identitet er kompromitteret

være højere, når denne vil have en meget vidtgående adgang til systemet og dets data, end en almindelig borger, der måske har en begrænset adgang til egne data. I en sådan situation kan det give mening, at Sikringsniveauet for den administrative brugers adgang bliver sat højere end for den almindelige bruger.

### Vurdering af risikoelementer

Den første del af Excel-arket (fanen "#2 Risikoelementer") opstiller 6 områder, hvor forskellige risici relateret til fejl i identitetshåndteringen skal vurderes:

- Brugerens adgang til personoplysninger
- Brugerens adgang til øvrige typer oplysninger
- Konsekvenser for registrerede ved at forkert bruger (impersonering) tilgår systemet inkl. registreredes data
- Konsekvenser for tjenesteudbyder eller leverandør ved at forkert bruger (impersonering) tilgår systemet inkl. tjenesteudbyders/leverandørs data (fortrolighed)
- Brugerens mulighed for at påvirke integritet for systemets eller data (herunder ændre/ødelægge data eller opførsel)
- Brugerens mulighed for at påvirke tilgængelighed for system eller data (herunder slette data eller ødelægge systemet)

Risikoelementerne går således både på omfang, typen og følsomheden af data, som kan tilgås via tjenesten, og de potentielle konsekvenser ved forkert identitetshåndtering, herunder tab af fortrolighed, integritet og tilgængelighed af data og system.

Hvert element gives en score i intervallet 1-3, og det samlede risikoniveau beregnes som maksimumværdien af de enkelte risikoelementer. Til de enkelte risikoelementer er der angivet en vejledende tekst i form af en indikator for det pågældende niveau.

### Vurdering af kontrolelementer

Den anden del af Excel-arket (fanen "#3 Kontrolelementer") opstiller 7 kontrolområder, der kan mitigere risici vedr. fejl i identitetshåndteringen:

- Adgangskontrol og rolledesign
- Robusthed, test og assurance
- Logning og overvågning
- Vejledninger og instruks til anvendere af tjenesten
- Funktionsadskillelse
- Sikre forbindelser
- Kontrol med brugersessioner

Her skal tjenesteudbyderen vurdere, hvor stærke mitigerende kontroller, der er planlagt eller implementeret i tjenesten. Rationalet er, at kontroller som fx finkornet rolledesign, funktionsadskillelse og overvågning kan reducere konsekvenserne af fejl i identitetshåndteringen.

Hvert element gives en score i intervallet 1-3, og det samlede risikoniveau beregnes som gennemsnittet af de enkelte kontrolelementer. Til de enkelte kontrolelementer er der angivet en vejledende tekst i form af en indikator for det pågældende niveau.

### Vurdering af samlet Sikringsniveau

Det samlede Sikringsniveau findes ved at kombinere scoren for risikoelementer (1-3) med scoren for kontrolelementer (1-3), så der opnås en balancering af de to dimensioner:

Excel-arket viser på fanen "#1 Samlet vurdering", hvorledes risiko- og kontrolelementer foreslås kombineret til en indikation af samlet Sikringsniveau:

| Kontrolelement | | | | |
|---|---|---|---|---|
| | [ 2,5 - 3,0 ] | L | B | B |
| | [ 2,0 - 2,5 [ | L | B | H |
| | [ 1,5 - 2,0 [ | L | B | H |
| | [1,0 - 1,5 [ | B | B | H |
| | | 1 | 2 | 3 |
| | | Risikoelement | | |

Figur 3: Indikation af sikringsniveau med farve- og bogstavkode

I figuren ovenfor indikerer den grønne farve med bogstav L Sikringsniveau Lav, den gule farve med bogstav B indikerer Sikringsniveau Betydelig, og den røde farve med bogstav H indikerer Sikringsniveau Høj. Som tidligere nævnt skal dette alene tages som en foreløbig indikation, der ikke må bruges ukritisk, og der skal under alle omstændigheder anlægges en samlet, forretningsmæssig vurdering.

Det kan endvidere være relevant at have nogle pejlemærker eller tommelfingerregler for kalibrering af den anvendte skala, som kan tages med i vurderingen:

- Sikringsniveau Betydelig er det niveau, som normalt anvendes ved adgang til selvbetjeningsløsninger indeholdende personoplysninger, og er det mest almindeligt forekommende niveau for MitID-brugere.
- Sikringsniveauet Høj forventes anvendt af en lille gruppe tjenester med særlige behov for identitetssikring som følge af meget alvorlige risici forbundet med forkert identitetshåndtering.

### Differentiering mellem brugertyper

Som tidligere nævnt kan det være relevant at differentiere mellem det krævede Sikringsniveau for flere af de arketypiske brugere, der anvender tjenesten. Der kan fx være forskel på behov for Sikringsniveau for en borger, en sagsbehandler og en administrator. Det kan derfor være relevant at gennemføre vurderingen i Excel-arket flere gange (én per brugertype).

## Avanceret brug af Sikringsniveauer

Nogle tjenester kan have brug for en mere avanceret håndtering af Sikringsniveauer, end der er beskrevet ovenfor. I dette afsnit gennemgås en række eksempler, som illustrerer kendte scenarier.

### Tilpasset adgang på baggrund af Sikringsniveau

Tjenester kan rumme funktioner eller data, som naturligt vil blive klassificeret på forskellige Sikringsniveauer. I stedet for at indrette adgangspolitikken som en binær adgang/ikke-adgang, hvor det øverste Sikringsniveau sætter barrieren for adgang, kan det i visse tilfælde give mening, at tjenesten filtrerer de data og funktioner, brugeren har adgang til, på baggrund af det aktuelt opnåede Sikringsniveau. Et simpelt eksempel kunne være, at brugere på Sikringsniveau Lav får adgang til funktioner og data i tjenesten med Lav risikoprofil, og at brugere på Sikringsniveau Betydelig får adgang til større dele af tjenesten med højere risikoprofil. Det kræver naturligvis en del modenhed af tjenesten dynamisk at kunne filtrere indholdet på baggrund af det aktuelle Sikringsniveau, men det kan samtidig give en bedre brugeroplevelse. AULA-løsningen til skoler og dagtilbud er et eksempel på en tjeneste med differentieret adgangsstyring.

I den forbindelse er det relevant at være opmærksom på, at [OIOSAML] profilen fra Digitaliseringsstyrelsen understøtter såkaldt 'step-up'-autentifikation. En tjeneste kan anvende denne funktion til at bede NemLog-in (eller anden Identitetsbroker) om at hæve en allerede autentificeret brugers Sikringsniveau – eksempelvis fordi brugeren undervejs i sessionen ønsker at tilgå data eller funktioner, som er mere følsomme.

### Adgangsbeslutninger baseret på IAL og AAL

Ud over det overordnede Sikringsniveau (LoA, *Level of Assurance*), definerer NSIS også underkomponenterne IAL (*Identity Assurance Level*) og AAL (*Authenticator Assurance Level*)[4]. Disse kan ligeledes formidles fra en Identitetsbroker til tjenesten ved anvendelse af [OIOSAML] profilen.

En tjeneste med særlige behov, kan inddrage de aktuelle IAL og AAL-værdier for brugerautentifikationen i sin adgangspolitik, og på den måde opnå en finkornet politik, der baserer sig på et større datagrundlag. I så fald bør dette afspejle sig i den risikovurdering, som er gennemført.

[4] For detaljer om IAL og AAL henvises til [NSIS].

## Referencer


[OIOSAML] ”OIOSAML Web SSO Profile”, Digitaliseringsstyrelsen.
https://digst.dk/OIOSAML/

[NSIS] ”National Standard for Identiteters Sikringsniveau (NSIS)”.
https://digst.dk/NSIS/

[REF-ARK] ”Referencearkitektur for brugerstyring”.
https://arkitektur.digst.dk/referencearkitekturer/brugerstyring/referencearkitektur-brugerstyring