DIGITALISERINGSSTYRELSEN

3. oktober 2019

Vejledning til valg af NSIS Sikringsniveau for tjenesteudbydere

Version 2.0.1

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 version 2.0 af 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-standarden 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 Sikrings-niveauet. Den grundlæggende præmis er, at Sikringsniveauet, 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].

Vejledningen erstatter den tidligere vejledning fra Økonomistyrelsen med titlen "Autenticitetssikring - Vejledning til autenticitetssikringsniveau for den fællesoffentlige log-in-løsning" (2008).

Terminologi

Denne vejledning anvender samme terminologi som NSIS-standarden, 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 vil være et afgørende element i næste generation af den nationale, digitale Identitetsinfrastruktur i form af MitID og NemLog-in3 løsningerne. I denne infrastruktur forventes et bredere udvalg af Elektroniske Identifikationsmidler på forskellige Sikringsniveauer modsat nuværende situation med NemID og OCES, hvor de fleste tjenester de facto har betragtet de forskellige typer identifikationsmidler (nøglekort, nøglefil, hardware, nøgleApp) på samme Sikringsniveau.

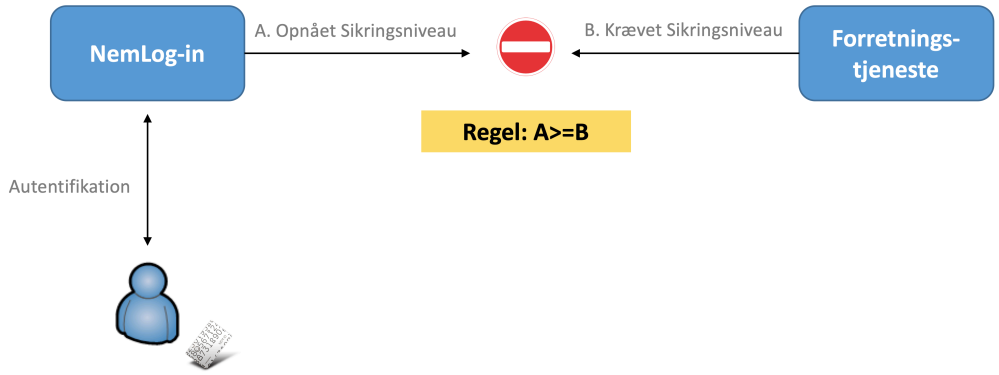
På den anden side har forretningstjenester forskellige behov for sikkerhed for brugernes Identitet, og krav til Sikringsniveau bør stilles ud fra en konkret vurdering af tjenestens behov og risikoprofil - herunder konsekvenserne ved forkert identifikation af brugere. Eksempelvis kan der være stor forskel 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 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-standarden.

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 SAML 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 NemID nøgleapp) 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.

[1] Bemærk at det først med MitID infrastrukturen bliver muligt at få udstedt Elektroniske Identifikationsmidler på Sikringsniveau Høj.

[2] Naturligvis forudsat at øvrige betingelser i adgangspolitikken er opfyldt.

NemLog-in's 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-in's 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 tilsluttes 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 NemID eller digital signatur (eller opnår niveau "Betydelig" i NSIS), idet næste generation af NemLog-in og MitID som nævnt forventes udvidet til at omfatte 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].

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.

[3] Denne kontrol skal efterprøves i praksis inden systemet sættes i drift.

Vurdering af Sikringsniveau

Den resterende del af denne vejledning har til formål at give forslag til, hvorledes en tjenesteudbyder kan fastlægge krav til Sikringsniveau for deres konkrete tjenester (som angivet i punkt 5.b ovenfor). Det beskrives *ikke*, hvorledes tjenesteudbyderen 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.

Det er som tidligere nævnt udelukkende de dataansvarlige myndigheders ansvar at fastlægge krav til Sikringsniveauer for de forretningstjenester, som aftager Identiteter. Som hjælp til gennemførsel af risikovurdering henvises til ISO 27005 og ISO 3000, der beskriver forslag til proces for risikovurdering, eksempelvis ved kortlægning af kritiske data, følsomme personoplysninger, konsekvenser, trusler og kontroller som beskrevet nedenfor. Dette er i tråd med GDPR, som kræver at den dataansvarlige (og i øvrigt også databehandlere) træffer passende tekniske og organisatoriske foranstaltninger for at sikre et sikkerhedsniveau, der passer identificerede risici. Der kan i øvrigt henvises til Datatilsynets vejledning vedr. risikovurdering[4]. Valg af NSIS Sikringsniveau kan med andre ord opfattes som en del af denne forpligtelse om at træffe passende foranstaltninger, som naturligvis skal suppleres med en lang række øvrige tiltag.

[4] https://www.datatilsynet.dk/media/7900/vejledende-tekst-om-risikovurdering.pdf

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

For at kunne fastlægge det rette Sikringsniveau for Identiteter, er det relevant at identificere mulige konsekvenser af, at brugerens Identitet ikke er fastslået tilstrækkeligt – med andre ord at en bruger kan udgive sig for at have en anden Identitet end den faktiske. Konsekvenserne vil variere vidt fra system til system og fra brugergruppe til brugergruppe. Eksempelvis kan konsekvenserne af at en superbrugers identitet er kompromitteret være højere, når denne vil have en meget bred adgang til systemet og dets data, end en almindelig borger, der måske har en begrænset adgang til egne data. Dette vil alt andet lige tilsige, at sikringsniveauet for superbrugeren bør overvejes at blive sat højere end for den almindelige bruger.

For systemer, der behandler personoplysninger, kan man med fordel gennemføre en vurdering af konsekvenser for de registrerede, fx i form en konsekvensvurdering for privatlivet. Datatilsynet og Digitaliseringsstyrelsen har udgivet en række publikationer om emnet, som findes tilgængelige på de respektive hjemmesider.

I forbindelse med vurdering af konsekvenser for registrerede kan man fx se på:

- Oplysningernes mængde og følsomhed.
- Konsekvenser for datasubjekterne (de registrerede) af kompromittering herunder muligheden for at indskrænke handlefriheden.
- Teknologiens potentiale til at krænke privatlivet, herunder risikoen for at behandle data på nye måder, som ligger uden for de oprindelige formål.
- Oplysningernes potentiale til at identificere enkeltpersoner.
- Størrelsen på brugergruppen.

- Konsekvenser for den dataansvarlige, herunder omdømme og økonomiske konsekvenser.

Vurdering af disse forhold lægger hovedfokus på risici forbundet med kompromittering af personoplysninger. Det er dog vigtigt at understrege, at der som tidligere nævnt er andre risici, som er nødvendige at overveje for at få et komplet risikobillede. For at sikre et fuldstændigt overblik over de aktuelle risici bør der gennemføres en traditionel risikovurdering. Der kan således sagtens være brugergrupper, som ikke har adgang til personoplysninger, men hvor man alligevel vil kræve sikringsniveau Betydelig eller Høj, da de pågældende brugere kan udføre kritiske handlinger fx af økonomisk betydning for tjenesteudbyderen.

Det skal igen understreges, at valget af Sikringsniveau suverænt påhviler den dataansvarlige tjenesteudbyder, og at ovenstående blot kan betragtes som en generel vurdering, der kan danne udgangspunkt for en konkret vurdering, der tager de specifikke forhold i betragtning.

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. Den kommende AULA-løsning til skoler og dagtilbud er et eksempel på en tjeneste med differentieret adgangsstyring.

I den forbindelse er det relevant at være opmærksom på, at version 3.0 af [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 eller *Level of Assurance*), definerer NSIS 2.0 også underkomponenterne IAL (*Identity Assurance Level*) og AAL (*Authenticator Assurance Level*)[5]. Disse kan ligeledes formidles fra en Identitetsbroker til tjenesten ved anvendelse af [OIOSAML] 3.0 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.

[5] For detaljer om IAL og AAL henvises til NSIS 2.0.

Appendiks A – Historik om Sikringsniveauer

Der opereres i NSIS 2.0 med tre Sikringsniveauer: Lav, Betydelig Høj. Den nuværende NemID-løsning og tilhørende OCES-certifikater blev designet før NSIS, og derfor er NSIS-kravene ikke automatisk indarbejdet i disse løsninger.

Som tidligere beskrevet forventes identitetsinfrastrukturen udvidet med understøttelse af andre Elektroniske Identifikationsmidler, som potentielt kan være klassificeret på andre niveauer. Dette kan i en løst-koblet føderation ske helt uden at påvirke tjenesteudbydernes løsninger, såfremt disse løsninger (som beskrevet ovenfor) tager højde for brugerens aktuelle niveau i deres adgangskontrol.

NemLog-in3-løsningen vil fremover benytte NSIS-standarden til vurdering af anvendte Elektroniske Identifikationsmidler, og dette indebærer, at tjenesteudbyderne ikke selv behøver at tage stilling til disse. Tjenesteudbyderne skal således blot koncentrere sig om egne løsningers behov for Sikringsniveauer i form af en indplacering i forhold til ovennævnte niveauer. Der henvises til Digitaliseringsstyrelsens hjemmeside for en guide til ibrugtagning af NSIS[6].

[6] https://digst.dk/it-loesninger/implementeringssite/screeningsvaerktoej-til-brugerorganisationer-og-tjenesteudbydere/nsis-ibrugtagning-af-standarden/

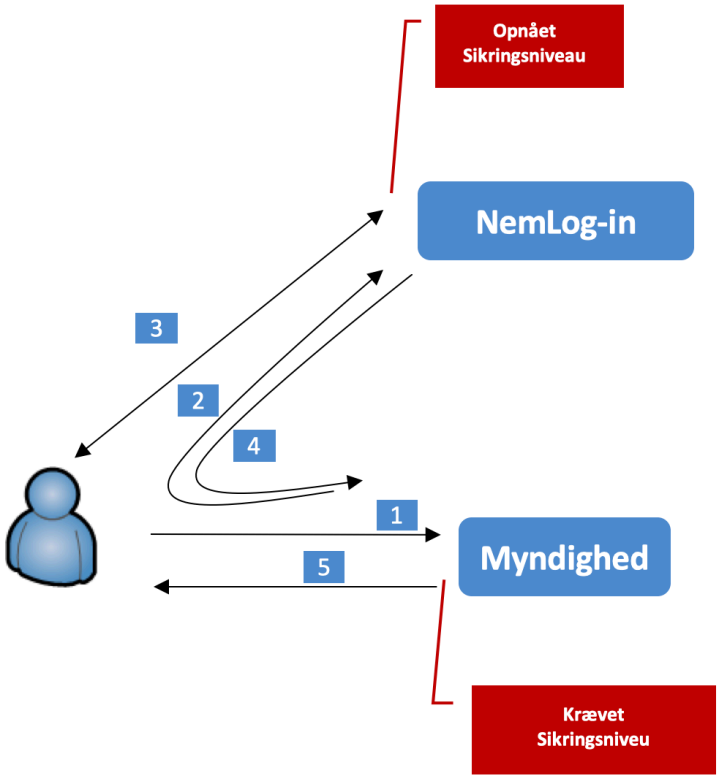
Appendiks B – Detaljeret SAML forløb

Når tjenester anvender en ekstern Identitetsbroker som NemLog-in, flyttes håndteringen af brugerautentifikation (log-in) til en ekstern løsning. På den måde slipper hver enkelt tjenesteudbyder for selv at skulle udstede Elektroniske Identifikationsmidler, etablere en log-in-løsning, og brugerne kan opnå Single Sign-On (SSO) mellem forskellige tjenesteudbyderes løsninger.

NemLog-in understøtter eksempelvis, at brugerne kan logge på med forskellige typer Elektroniske Identifikationsmidler, herunder NemID nøglekort og NemID medarbejdersignatur (MOCES) i varianter med nøglekort, nøglefil, nøgleapp og hardware. Når MitID og NemLog-in3 går i luften kan det endvidere imødeses, at infrastrukturen vil blive videreudviklet til at understøtte nye typer af Elektroniske Identifikationsmidler med forskellige Sikringsniveauer.

Konkret vil samspillet mellem NemLog-in og tjenesteudbyderens løsning være som følger:

1. Brugeren tilgår en beskyttet ressource hos tjenesten.
2. Tjenesten sender brugeren over til den NemLog-in med en forespørgsel om autentikation.
3. Brugeren autentificerer sig over for NemLog-in med et Elektronisk Identifikationsmiddel. NemLog-in validerer brugerens autentifikation og fastlægger et mål for det opnåede Sikringsniveau i henhold til NSIS (Lav, Betydelig, Høj).
4. Brugeren sendes tilbage til tjenesten med et såkaldt SAML token (udstedt af log-in-løsningen), der beskriver brugerens Identitet (f.eks. CPR-nummer) såvel som det aktuelle Sikringsniveau.
5. Tjenesten validerer SAML tokenet og giver efterfølgende brugeren adgang til forespurgte ressourcer såfremt:
    a. Brugeren er autoriseret til ressourcen i henhold til den lokale adgangspolitik, OG
    b. Brugerens har opnået et Sikringsniveau, der modsvarer det fastlagte niveau for løsningen.



Figur 3: Forløb ved fødereret log-in

Bemærk at trinene ovenfor kun udføres første gang, brugeren tilgår tjenesteudbyderen indenfor en session, og at trin 3 evt. overspringes, hvis brugeren allerede er logget på NemLog-in (dvs. Single Sign-On). Bemærk også, at den samme bruger kan have flere Elektroniske Identifikationsmidler, som kan være klassificeret på forskellige sikrings-niveauer i henhold til NSIS.

Referencer

[OIOSAML] ”OIOSAML Web SSO Profile 3.0”, Digitaliseringsstyrelsen.
https://digst.dk/it-loesninger/nemlog-in/udbud/oiosaml-30/

[NSIS] ”National Standard for Identiteters Sikringsniveau (NSIS), 2.0.1”.
https://digst.dk/it-loesninger/nemlog-in/udbud/nsis-standarden/

[REF-ARK] ”Referencearkitektur for Identitets- og rettighedsstyring”.
http://arkitekturguiden.digitaliser.dk/Identitets-og-rettighedsstyring

[VILKÅR] ”Vilkår for anvendelse af den fællesoffentlige log-in-løsning”
https://www.digst.dk/It-loesninger/NemLogin/Til-myndigheder