# NSIS-design for lokal IdP

## Forslag til praktisk tilgang

pwc

juni 2020

# Indhold

# 1 Indledning

Den offentlige infrastruktur for autentifikation er under forandring. Digitaliseringsstyrelsen er i gang med at udskifte NemID med MitID, og NemLog-in 2 med NemLog-in 3. Herunder har Digitaliseringsstyrelsen udarbejdet en standard for identiteters sikringsniveauer, NSIS, som vil sætte rammerne for, hvordan MitID og NemLog-in 3 kommer til at fungere teknisk såvel som organisatorisk.

NSIS er en standard, som grundlæggende handler om at have et vist niveau af tillid til de parter, som arbejder sammen.

Alle, der anvender autentifikation mod offentlige systemer, vil have behov for at vurdere eksisterende løsninger for autentifikation, og hvordan disse skal ændres for at passe ind i den kommende infrastruktur.

# 2 Kort om NSIS

NSIS, eller National Standard for Identiteters Sikringsniveauer, er udarbejdet af Digitaliseringsstyrelsen i forbindelse med overgangen fra NemID og NemLog-in 2 til MitID og NemLog-in 3. NSIS er den danske fortolkning af den europæiske eIDAS-forordning.

NSIS arbejder med tre sikringsniveauer: lav, betydelig og høj. Fremover skal alle tjenesteudbydere vurdere, om deres tjenester skal udbydes på et lavt, betydeligt eller højt sikringsniveau. Dette niveau kaldes LOA (Level Of Assurance). Vurderingen skal bero på en konkret risikovurdering af de systemer og data, der gives adgang til. Er det eksempelvis data, som i henhold til GDPR bliver klassificeret som følsomme personoplysninger, og gives der adgang til data for et stort antal personer, må antagelsen være, at der skal kræves LOA = høj for at få adgang til disse data. Men det er en vurdering, som tjenesteudbyderen skal foretage og håndhæve efterfølgende. Kræver tjenesten LOA = betydelig, kan man som identitet ikke tilgå tjenesten, medmindre man som minimum kan fremvise det samme sikringsniveau = betydelig.

Adgang til en tjenesteudbyders tjenester styres gennem en føderation. En føderation er kendetegnet ved, at tjenesteudbyderen som udgangspunkt ikke kender de identiteter, der skal tilgå tjenesten, men i stedet får en billet fra ”kunden”, der indeholder informationer om identiteten hos kunden. Dermed bliver det et tillidsforhold, der opstår mellem ”kunden” og tjenesteudbyderen. Et tillidsforhold, som NSIS er med til at sætte standarden for.

Som protokol til denne dataudveksling anvendes SAML. Digitaliseringsstyrelsen har udarbejdet en særlig dansk version i forbindelse med MitID og NemLog-in 3 kaldet OIO-SAML 3.0, som MitID og NemLog-in 3 skal overholde.

LOA-værdien skal i henhold til OIO-SAML 3 være stemplet i den SAML-billet, der udstedes hos ”Kunden”, således at tjenesteudbyderen kan afgøre, om identiteten hos ”kunden” skal have adgang til tjenesten eller ej.

PwC’s fortolkning af NSIS-standarden er, at den LOA-værdi, der stemples i SAML-billetten til tjenesteudbyderen, er nødt til at blive beregnet dynamisk ”just in time”. Dette skyldes, af NSIS arbejder med en række sikringsniveauer på ”kunde”-siden, og det er disse sikringsniveauer, der samlet set giver LOA-værdien. Sikringsniveauerne på ”kunde”-siden vil variere, alt efter hvilken situation den enkelte identitet befinder sig i. De sikringsniveauer der omtales i dette design er:

- IAL  Identity assurance level
- AAL Authenticator assurance level
- FAL  Federation assurance level
- LOA Level of assurance (LOA = MIN [ IAL, AAL, FAL ])

Eksempelvis kan en identitet være logget ind på to forskellige pc’er med forskellige identifikationsmidler. På den ene pc er der logget ind med brugernavn og password, og på den anden er der logget ind med et smartcard og pinkode. Sessionen, der er autentificeret med smartcard og pinkode, vil som minimum have en AAL = betydelig og vil derfor give andre muligheder for at tilgå offentlige systemer end den session, der blot er autentificeret med brugernavn og password og dermed er AAL = lav. Man er derfor nødt til at kunne skelne mellem de to forskellige login sessioner, selvom de er foretaget med samme identitet.

# 3 Autentifikationsmetoder

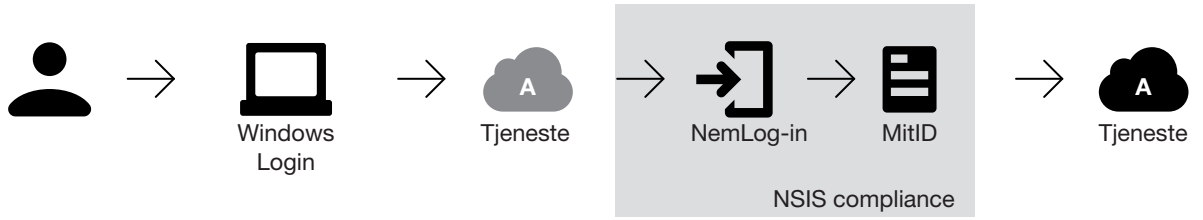
Hvis man som virksomhed i dag udelukkende anvender NemID og medarbejdersignatur som autentifikations- og loginmetode mod offentlige systemer, vil der være en række forandringer, som man skal implementere for at blive i stand til at anvende den nye offentlige infrastruktur. Dette skyldes bl.a., at den nuværende medarbejdersignatur-nøglefil udfases og erstattes af en ny erhvervsidentitet via NemLog-in 3.

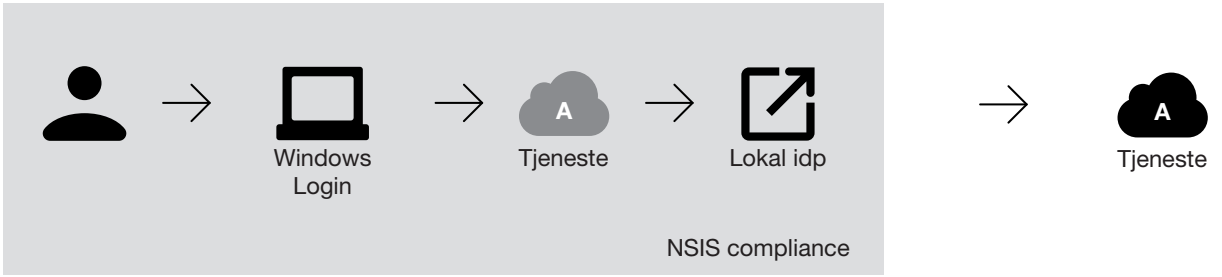
I den nye infrastruktur vil virksomheden anvende enten 1) NemLog-in 3 som identity provider (logintjeneste) til at tilgå de offentlige systemer og en af de MitID-autentifikationsmetoder, som bliver tilgængelige, eller virksomhedens egen identity provider (lokal IdP) og lokalt udstedte identifikationsmidler.

Hvis man som virksomhed anvender det, der kaldes lokal IdP, altså at virksomheden selv er ansvarlig for at udstille identiteter mod de offentlige systemer, er der en række andre krav, som man skal være opmærksom på. Langt de fleste virksomheder vil typisk anvende en kombination af de her nævnte metoder.

Dette designnotat er primært henvendt til virksomheder med egen lokal IdP. Formålet med designnotatet er at gøre virksomheden i stand til at vurdere, hvilke tekniske tiltag der skal foretages i virksomhedens infrastruktur for at kunne leve op til NSIS-standarden og fremvise en praktisk tilgang til krav til implementeringen.

Med egen IdP er det virksomheden selv, der har hele ansvaret for sikkerheden i forhold til den identitet, der skal have adgang til det offentlige system, herunder compliance i forhold til NSIS. Dette illustreres i tegningen nedenfor. Såfremt virksomheden ønsker at tilgå offentlige systemer med LOA = betydelig eller høj, vil det kræve en revisionserklæring som bevis på compliance.




Designet forholder sig specifikt til de tekniske forhold, som er relevante for at kunne leve op til NSIS-standardens tre sikringsniveauer IAL, AAL og FAL og den resulterende LOA-værdi (lav, betydelig, høj), som tjenesteudbydere kommer til at kræve for at muliggøre login mod tjenesten.

De organisatoriske forhold, som NSIS ligeledes omhandler, er ikke uddybet i dette design.

# 4 Tekniske forhold

I afsnittet herunder gennemgås de tre væsentlige sikringsniveauer, som forefindes på "kunde"-siden IAL, AAL og FAL, og hvordan virksomheden kan ændre sine tekniske systemer.

## 4.1 Identity assurance level (IAL)

IAL-værdien er en forholdsvis statisk værdi, som er tilknyttet selve identiteten. IAL-værdien har primært at gøre med organisatoriske forhold, hvordan identiteten blev verificeret af virksomheden, og hvilke kontroller der er udført i den forbindelse, herunder hvilke legitimationsbeviser der er fremvist ved udlevering af identifikationsmidlet.

Verifikation af identiteten via en MitID-autentifikation vil være en gyldig metode til at fastslå IAL-værdien.

Når det siges, at IAL-værdien er forholdsvis statisk, hænger det sammen med den livscyklus, som et identifikationsmiddel gennemløber. Bl.a. kan der være behov for at tilbagekalde et identifikationsmiddel. I et sådan tilfælde skal IAL-værdien naturligvis tilsvarende ændres.

IAL-værdien (lav, betydelig, høj) registreres for identiteten i et it-system, typisk virksomhedens HR-system.

Det skal være muligt for identiteten dynamisk at slå denne værdi op.

For virksomheder, som anvender en identity management (IdM)-løsning, vil det være oplagt at overføre IAL-værdien som en af identitetens attributter fra HR til IdM, således at IAL-værdien kan findes ved et dynamisk opslag i IdM-løsningen på identiteten.

Såfremt virksomheden anvender en IdM-løsning til at administrere identiteter, kunne IAL-værdien automatisk sættes et niveau ned efter en given periode (fx fra betydelig til lav), således at der indbygges en forebyggende kontrol. Kun en aktiv handling i form af en gen-verifikation vil da kunne løfte IAL-værdien igen.

I IdM-løsningen vil det være muligt at indbygge kontroller, såsom ACL eller kryptering, således at kun få relevante konti har adgang til at kunne ændre IAL-værdien.

## 4.2 Authenticator assurance level (AAL)

AAL-værdien beskriver det sikringsniveau, med hvilket selve autentifikationen er foretaget. Når virksomheden anvender lokal IdP, vil AAL-værdien kunne fastsættes på to måder:

- Ved identitetens login til virksomhedens netværk (typisk via en Windows-pc)
- Ved just-in-time step-up-autentifikation, såfremt den service, der tilgås, forlanger en højere LOA-værdi end den, der initielt bliver præsenteret i SAML-billetten.

AAL-værdien er dermed dynamisk og må på ingen måde stemples på identiteten som en prædefineret værdi.
AAL-værdien skal sættes ved hvert login og/eller step-up-autentifikation.

Det er uden for scope for dette designnotat at gennemgå, hvilket AAL-sikringsniveau der kan opnås ved forskellige kombinationer af identifikationsmidler (fx brugernavn og password kombineret med en anden faktor fra en mobiltelefon).

De nævnte to autentifikationsmåder vil i høj grad spille sammen med den slutbrugeroplevelse, som man ønsker, at virksomhedens brugere skal have. Dette hænger sammen med, hvor mange gange identiteten skal autentificeres i løbet af en dag. Hvis den nødvendige AAL opnås med login på pc'en, forventes det, at man i henhold til NSIS kan bevare denne AAL-værdi og benytte den i efterfølgende SAML-billetter, også selvom pc'en i perioder har været i skærmlåst tilstand.

Ved step-up-autentifikation må det forventes, at identiteten skal autentificere sig, hver gang en ny tjeneste tilgås. Når en tjeneste forlades, bør SAML-token blive ugyldiggjort, og dermed skal der autentificeres igen, næste gang den samme eller en anden service tilgås. Dette vil naturligvis påvirke slutbrugeroplevelsen af arbejdsprocessen, og for mange autentifikationer i løbet af en arbejdsdag vil nedsætte effektiviteten.

Specielt i sundhedssektoren vil der være særlige use-cases, der skal understøttes for at opnå en god slutbrugeroplevelse, bl.a. grundet den udbredte brug af fælles pc'er, der er logget ind med en fælles konto. Anvendelse af fælles konti vil ikke være acceptabelt under NSIS.

NSIS beskriver ikke direkte, hvilken lifetime en SAML-billet kan tillades at have, men PwC har antaget, at lifetime maksimalt bør være en time – og ideelt set kun med gyldighed for den igangværende session.

Rent teknisk er AAL-værdien den sværeste at håndtere, da der ikke findes en AAL-værdi, som bringes med rundt i fx et Windows-økosystem sammen med brugerens gøren og laden. På Windows-platformen er det en Kerberos-billet, som giver brugeren autentifikation (og autorisation) til at udføre opgaver i Windows-miljøet og eventuelle andre miljøer, der ligeledes anvender Kerberos.

Ved login på en Windows-platform vil det være den såkaldte authentication provider, der afgør, hvilket identifikationsmiddel, der bliver anvendt ved login. Hvert identifikationsmiddel har hver sin egen authentication provider. Dermed vil man kunne skelne mellem et login, der er foretaget med brugernavn/password (og en AAL = lav), og fx et login, der anvender en pinkode i kombination med et smartcard. (Forventet AAL = betydelig / høj).

## 4.3 Federation assurance level (FAL)

Selve fødereringskomponenten, kaldet identity provider (IdP), vil være den komponent, der er ansvarlig for at udstede identiteten imod en offentlig eller privat tjenesteudbyder.

De sikringselementer, der er omtalt i NSIS-standarden, omhandler primært, hvordan it-sikkerheden er implementeret i forhold til selve IdP-komponenten, og det vil således være it-sikkerheden, der primært vil være genstand for den it-revision, der skal fastsætte FAL-niveauet.

For at IdP'en dynamisk kan beregne LOA-værdien på baggrund af MIN [IAL, AAL, FAL)], vil det være revisors opgave at stemple FAL-niveauet i en fil eller lignende, hvorfra værdien kan læses til den dynamiske beregning.

Såfremt der anvendes en enterprise access manager-løsning som IdP, vil det være muligt at beskytte FAL-værdien på forskellige måder, således at integriteten af værdien kan dokumenteres over tid.

## 4.4 Dynamisk beregning af LOA

Som nævnt i afsnittet herover, skal der være en komponent, der kan beregne LOA-værdien dynamisk og stemple denne værdi i den dynamiske SAML-token.

Såfremt virksomheden anvender en enterprise access manager-løsning som IdP, vil opsætningen af denne kunne definere et regelsæt, der dynamisk trækker på de relevante informationer og stempler den korrekte dynamiske LOA-værdi i SAML-billetten.

## 4.5 PwC rådgivning

Denne publikation er udarbejdet alene som en generel orientering om forhold, som måtte være af interesse, og gør det ikke ud for professionel rådgivning. Du bør ikke disponere på baggrund af de oplysninger, der er indeholdt i denne publikation, uden at indhente specifik professionel rådgivning. Vi afgiver ingen erklæringer eller garantier (udtrykkeligt eller underforstået) hvad angår nøjagtigheden og fuldstændigheden af de oplysninger, der findes i publikationen, og, i det omfang loven tillader, accepterer eller påtager PricewaterhouseCoopers Statsautoriseret Revisionspartnerselskab, dets aktionærer, medarbejdere og repræsentanter sig ikke nogen forpligtelse, ansvar eller agtpågivenhedspligt for eventuelle konsekvenser, som følger af, at du eller andre handler eller undlader at handle i tillid til de oplysninger, der findes i publikationen, eller for eventuelle beslutninger truffet på baggrund af publikationen.