

Til høringsparterne
Se vedlagte liste

17. maj 2016
CSS/MAPAN

Høring i forbindelse med ny National Standard for Identiteters Sikringsniveau.

Digitaliseringsstyrelsen har udarbejdet vedlagte nationale standard for identiteters sikringsniveau, herefter kaldet NSIS. Høringen er sendt til de myndigheder og organisationer m.v., der fremgår af vedlagte høringsliste.

Høringsbrev, høringsliste og NSIS 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. Denne erkendelse er kommet til udtryk i en række forskellige sammenhænge:

- Sundhedsdatastyrelsen, tidligere National Sundheds-it, har i foråret 2015 gennemført en analyse af offentlige sikkerhedsstandarder og – løsninger. Her fremstår det som en klar anbefaling til det videre arbejde, at der etableres et trust framework tilpasset danske forhold.
- KOMBIT, som er kommunernes it-fællesskab, har defineret en fælleskommunal rammearkitektur baseret på en føderationsmodel, hvor de enkelte kommuner bliver udbydere af digital identitet overfor fælleskommunale løsninger. Dette forudsætter en fælles ramme for kvaliteten af disse identiteter gennem et etableret framework for dette.
- Digitaliseringsstyrelsen forbereder på fællesoffentlige vegne den næste generation af NemID. I den forbindelse indgår der overvejelser om, der skal være mulighed for flere løsninger på forskellige sikringsniveauer (og med forskellig brugervenlighed) – evt. ved at private aktører på markedet kan tilbyde deres løsninger. Dette forudsætter en ramme, som definerer kravene til sådanne løsninger, og som sikrer transparens for modtageren af en digital identitet.

EU har med Forordning om elektronisk identifikation og tillidstjenester til brug for elektroniske transaktioner på det indre marked (eIDAS-reguleringen), indført et EU trust framework for identiteter med henblik på at skabe gensidig tillid og

interoperabilitet på tværs af landegrænser. Herigennem vil digitale tjenesteudbydere i ét medlemsland kunne have tillid til digitale identiteter udstedt i et andet medlemsland. Samme tilgang, der benyttes til at skabe tillid og sammenhæng mellem medlemslande i EU, vil altså kunne anvendes tilsvarende til at skabe sammenhæng og tillid mellem danske identitetsløsninger i Danmark.

Selvom NemID umiddelbart har løst det generelle behov for et (fællesoffentligt) højt sikringsniveau for identitet og autentifikation¹, er det samlede landskab af identitetsløsninger blevet mere og mere fragmenteret. Der er pt. ingen fællesoffentlig koordinering af sikringsniveauer for bruger-identiteter og akkreditiver, mens man på den anden side har taget de første skridt vedrørende risikoniveauer i [OIO-A-LEVEL] samt [LOA-ØS]². Typisk dikteres kravene i en standard, et forretningsdomæne gennem en specifik implementering / løsning som fx NemID til offentlige selvbetjeningsløsninger eller en AD brugerkonto til en intern applikation hos en myndighed.

På baggrunden af dette delvist fragmenterede billede af digitale identitetsløsninger samt fordelene ved at have et dansk trust framework, som kan mappes op med EU-trust frameworket, har Digitaliseringsstyrelsen set nødvendigheden af at udarbejde et dansk trust framework.

Forretningsmæssige muligheder

Formålet med NSIS er altså at skabe en standard, der angiver graden af tillid til en given identitet eller digital tjeneste - på tværs af offentlige og private grænser mv.

Dermed vil NSIS muliggøre en effektiv arbejdsdeling, hvor specialiserede identitetstjenester kan levere de for andre tjenester nødvendige identiteter. Dette vil være en stor fordel for både brugere og leverandører af tjenester – og en vigtig forudsætning for et fleksibelt, digitalt økosystem på tværs af offentlige og private tjenester.

En offentlig standard for identiteters sikringsniveau kan således åbne for en række forretningsmæssige muligheder og fordele:

- En fælles forståelse samt koordinering / governance af sikringsniveau'er.
- Transparens gennem tydelig "varedeklaration".
- Mulighed for certificeringsordninger mod kravene, hvor private (og offentlige) aktører kan få certificeret deres løsninger mod et givet sikringsniveau (levels of assurance).
- Sammenhængende løsninger på tværs af domæner via gensidig tillid og anerkendelse af "fremmede" akkreditiver og identiteter.

¹ NemID giver ikke svar på andre attributter som fx arbejdsrelaterede/studiemæssige roller.

² Digitaliseringsstyrelsen planlægger separat at opdatere de tidligere publikationer på området, så disse kan komplementere denne standard.

- Effektiv decentral brugerstyring uden dublering af brugeridentitet i alle løsninger men i stedet føderering fra ”kilden” (autoritative systemer).
- En flerleverandørstrategi med mulighed for private aktører som udbydere af tillidstjenester - hvor det er ønskeligt og økonomisk fordelagtig.
- Valgfrihed for borgere og virksomheder mellem forskellige identitetsudbydere.
- Lettelse af udbud og kravspecifikation (samt evt. lovgivning), idet der kan henvises til den nationale standard for identiteters sikringsniveau.

NSIS er afgrænset til at omhandle digitale tjenester og medtager således ikke fx systemer, devices og internet of things (IOT). Denne afgrænsning følger af, at en standard for identiteters sikringsniveau, som også indeholder systemer, devices og IOT ikke eksisterer på nuværende tidspunkt, og styrelsen har vurderet, at det derfor vil være præmaturot og yderst ressource- og tidskrævende at udarbejde.

Digitaliseringsstyrelsen har i tråd med EU-retsakten om sikringsniveauer, valgt en resultatorienteret tilgang til vurdering af sikringsniveauer i den nationale standard for identiteters sikringsniveau. Det betyder, at NSIS ikke fortæller specifikt, hvordan en løsning skal implementeres, eller hvad den skal indeholde, men i højere grad beskriver hvordan resultatet bør være.

Fordelen herved er, at der opnås en langt større fleksibilitet i forhold til design og implementering af en given løsning, og ligeledes et større rum for at valg af teknologi for tjenesterne.

Overvejelser om NemID varianter

Datatilsynet har i en række sager udtalt sig om autentifikation over åbne net og har generelt anbefalet brug af digital signatur eller to-faktor autentifikation³ ved adgang til følsomme personoplysninger. Udtalelserne på Datatilsynets hjemmeside er af forholdsvis generel karakter og kommer ikke ind på de dybere, tekniske forskelle på signatur- eller to-faktor autentifikationsløsninger.

Den nuværende NemID medarbejdersignatur findes i en række forskellige varianter af hensyn til at honorere forskellige behov i hhv. små og store virksomheder samt i forskellige domæner – eksempelvis har sundhedsområdet særlige behov.

Hovedtyperne af NemID medarbejdersignaturer er:

³ Se fx <http://www.datatilsynet.dk/afgoerelser/seneste-afgoerelser/artikel/borgeradgang-til-mobil-udgave-af-rudersdal-kommunes-selvbetjeningsloesning/>
<http://www.datatilsynet.dk/afgoerelser/arkiv-over-afgoerelser/artikel/login-ved-adgang-til-skoleintra/>

- Medarbejdersignatur baseret på *nøglekort* (papkort – samme princip som borgerløsningen).
- Medarbejdersignatur baseret på *nøglefil* (både i lokale og centrale varianter, se Appendiks A).
- Medarbejdersignatur baseret på *hardware* (fx USB stick eller smart card).

Fælles for de forskellige løsninger til medarbejdersignaturer er, at de bygger på samme certifikatpolitik, og at de alle tilvejebringer en digital signatur, som vurderes at være omfattet af Datatilsynets generelle udtalelser vedr. stærk autentifikation.

I certifikatpolitikken for medarbejdersignaturer opereres der med et fælles ansvar for certifikatindehaver og certifikatholder, som tilsammen definerer en sikkerhed for, at en identifikation stammer fra den pågældende medarbejder i den pågældende organisation. En grundlæggende forudsætning for sikkerheden i disse har endvidere været, at privilegerede brugere i virksomheden ikke misbruger deres adgange – ved fx at udstede en signatur i falsk navn eller tiltvinge sig adgang til andres signaturer gennem deres betroede adgange til systemer.

Der er en række tekniske forskelle på varianterne af medarbejdersignaturen, som ud fra en risikobetragtning har forskellige styrker/svagheder mod forskellige typer angreb.

For NemID medarbejdersignaturer baseret på nøglekort eller på hardware vurderes der ikke umiddelbart at være udfordringer med at honorere eIDAS / NSIS kravene på niveau 3 om to autentifikationsfaktorer fra forskellige kategorier. Begge løsninger rummer således både et personligt kodeord samt et fysisk token (papkort eller USB stick / smart card).

For nøglefiler er sagen imidlertid ikke lige så klar, og vurderingen kan afhænge af den konkrete implementering. Som et eksempel kan en nøglefil på en enkeltbruger PC (uden central administrator) umiddelbart betragtes som et ”multifactor soft token”, der kan opfylde kravene på niveau ”Substantial”. Nøglefilen kan med andre ord opfattes, som noget brugeren er i besiddelse af, da den ligger på brugerens PC, hvis denne vel at mærke beskytter mod andres adgang til nøglefilen. Dette er i øvrigt konsistent med vurderingen i NIST 800-63 standarden, som er et anerkendt rammeværk for autenticitetssikring. Derimod kan det være mere vanskeligt at argumentere for, at en central signaturserver (som dem regionerne benytter) med en ”roaming” nøglefil kan opfylde kravene på niveau ”Betydelig”. Her skal brugeren først taste brugernavn og kodeord for at logge ind på netværket (fx AD) på en vilkårlig PC i domænet, og dernæst tages et (andet) kodeord for at tilgå nøglen i den roamede nøglefil. Dermed er begge autentifikationsfaktorer fra samme kategori (et kodeord fra kategorien ”noget kun brugeren ved”), og løsningen kategoriseres dermed som niveau 2 i NSIS (”Low” i eIDAS

standarden), selvom den måske ud fra en risikobetragtning er på niveau med førnævnte variant med nøglefiler på en enkeltbruger pc.

Grænserne mellem de ovenstående eksempler er delvist flydende, idet en fil både kan beskyttes logisk (fx ved kodeord til et centralt fildrev eller AD) eller fysisk (liggende på en fysisk enhed, som andre personer ikke har adgang til). Hvis slutbruger pc'en opbevares et sted med fri adgang, reduceres den fysiske beskyttelse til et spørgsmål om at kende kodeordet til pc'en, hvorfor nøglefilen ikke længere med rette kan opfattes som et token og dermed en ekstra faktor. Det afgørende er i den forbindelse, om nøglefilen er noget brugeren er i besiddelse af / har kontrol over.

En tilsvarende udfordring kan gælde kommunale log-in brokere (*Identity Providers*), som via SAML protokollen føderer et lokalt log-in (typisk baseret på AD) til en ekstern adgang med en signeret SAML billet. Her vælger flere kommuner, at adgang til brokern alene sker med AD brugernavn + kodeord. Uden en ekstra autentifikationsfaktor i en anden kategori vil sådanne løsninger blive klassificeret på niveau 2 ("Low").

Overgangsperiode til næste generation NemID

Som det fremgår af ovenstående vil forskellige løsninger til medarbejdersignatur i henhold til NSIS afsnit 3.2.1 om styrke af eID og eIDAS retsakt 2015/1502 afsnit 2.2.1, kunne blive vurderet på forskellige sikringsniveauer, selvom de måske ud fra en risikovurdering kan siges at have et sammenligneligt sikkerhedsniveau.

Dette foreslås håndteret ved flg. tilgang:

- Der anbefales en overgangsordning, hvor eksisterende typer af nøglefilsløsninger fortsat kan anvendes som hidtil – også selvom NSIS og eIDAS kravene objektivt set indplacerer selve eID'et på niveau 2. Det bemærkes, at disse løsninger vurderes at opfylde kravene i Datatilsynets hidtidige udmeldinger.
- Overgangsordningen gælder kun de eksisterende medarbejdersignaturer med nøglefil og kan begrundes med, at der er foretaget en grundig, samlet risikovurdering af disse løsninger.
- Overgangsordningen kan gælde indtil næste generation NemID kan sættes i drift med nye typer eID og signaturer til medarbejdere. Overgangsordningen skal bl.a. sikre, at eksisterende investeringer i nuværende teknologi og løsninger ikke er tabt, samt at der er fornøden tid for organisationerne til at implementere nye løsninger for medarbejdersignaturer, der er fuldt compliant med NSIS.
- Nye autentifikationsløsninger skal fremadrettet opfylde NSIS kravene på minimum niveau 3, når de anvendes til at tilgå følsomme personoplysninger over åbne netværk.

Med næste generation NemID anbefales det at udvikle nye ”ægte” to-faktor løsninger, som kan opfylde NSIS og eIDAS krav på minimum niveau 3⁴. Disse skal kunne anmeldes til Kommissionen på dette niveau med henblik på gensidig anerkendelse. Dette skal sikre, at danske virksomheder kan autentificere sig mod selvbetjeningsløsninger i andre EU-lande og derved ikke går glip af de fordele og muligheder, som disse måtte kunne give.

Videre proces

NSIS forventes publiceret ultimo juni 2016, og den følgende proces er illustreret i nedenstående figur 1.



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

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

Det skal understreges, at bemærkninger og vurderinger i NSIS er foreløbige og kan blive ændret som følge af høringssvarene.

Digitaliseringsstyrelsen vil efter modtagelse af høringssvar udarbejde høringsnotat, eventuelle tilretninger til NSIS samt en supplerende vejledning til NSIS, som rummer en mere detaljeret vejledning med eksempler og et anmeldelsesskema til selvdeklarering. **Bemærk, at vejledning og anmeldelsesskema endnu ikke er udarbejdet og derfor heller ikke er en del af dette høringsmateriale.** Et eksempel på formen for en kommende vejledning kan ses i EU's vejledning, LOA guidance til EU gennemførelsesretsakt om sikringsniveauer, som er vedlagt dette høringsmateriale.

Digitaliseringsstyrelsen anmoder om, at bemærkninger til det vedlagte udkast til den offentlige standard for identiteters sikringsniveau NSIS sendes til nsis@digst.dk. Eventuelle spørgsmål vedrørende standarden sendes til Martin Park Andersen mapan@digst.dk. Høringssvar skal være Digitaliseringsstyrelsen i hænde **senest fredag den 17. juni 2016**.

⁴ Og evt. også løsninger på niveau 4 som supplement.