

Høringsnotat

5. oktober 2018

Behandling af indkomne høringssvar i forbindelse med den officielle høring af National Standard for Identiteters Sikringsniveau (NSIS) version 2.0

Digitaliseringsstyrelsen har ved høringsfristens udgang den 3. september modtaget en række høringssvar fra de organisationer og myndigheder, som fik tilsendt høringen. I alt er der modtaget høringssvar fra 14 organisationer og myndigheder, hvoraf 1 myndighed ikke havde kommentarer (jf. kapitel 9 i nærværende høringssnotat).

Høringsparternes besvarelser er i dette høringssnotat indarbejdet i ikke-redigeret form, så de følger strukturen i NSIS og ikke som samlede svar. Herved opnås et overblik over de samlede kommentarer til hvert punkt, hvilket giver læseren en bedre fornemmelse af, hvad andre evt. har svaret til de samme punkter.

De generelle kommentarer til NSIS er medtaget under punkt 1.

Der er generelt blevet taget godt imod opdateringen af NSIS til en version 2.0. Det fremgår af størstedelen af høringssvarene, at parterne finder NSIS relevant og berettiget, og at der generelt er fokus på, at tillid til digitale identiteter er essentielt i et digitaliseret samfund som det danske.

Vejledning til NSIS, vejledning til tjenesteudbydere og revisionsinstruks til NSIS vil blive opdateret, så de afspejler de ændringer, der er foretaget i NSIS v. 2.0. Dokumenterne vil blive offentliggjort inden udgangen af november 2018. De tre dokumenter følger pt. NSIS version 1.0.1.

God læselyst.

Indholdsfortegnelse

1. INDLEDNING og overordnede kommentarer	4
1.2 Introduktion.....	9
1.3 Formål og scope	10
1.4 Eksempler på Identitetstjenester og sikringsniveauer.....	11
1.5 Terminologi	11
2. LIVSCYKLUS FOR AKKREDITIVER.....	18
3. NORMATIVE KRAV	19
3.1 REGISTRERINGSPROCESSEN	21
3.1.1 Ansøgning	21
3.1.2 Verifikation af Identitet (fysiske personer).....	22
3.1.3 Verifikation af Identitet (juridiske personer)	23
3.2 UDSTEDELSE OG HÅNDTERING AF AKKREDITIVER	23
3.2.1 Styrke af akkreditiver	24
3.2.2 Levering og aktivering.....	27
3.2.3 Suspendering, spærring og genaktivering	30
3.2.4 Fornyelse og erstatning	31
3.3 ANVENDELSE OG AUTENTIFIKATION.....	31
3.3.1 Autentifikationsmekanismer	31
4. ORGANISATORISKE- OG TVÆRGÅENDE KRAV.....	35
4.1.1 Generelle krav.....	35
4.1.2 Oplysningspligt.....	37
4.1.3 Informationssikkerhedsledelse.....	37
4.1.4 Dokumentation og registerføring.....	38

4.1.5 Faciliteter og personale.....	38
4.1.6 Tekniske kontroller.....	39
4.1.7 Anmeldelse og revision.....	39
5. ELEKTRONISKE IDENTIFIKATIONSMIDLER ASSOCIERET TIL JURIDISKE PERSONER	40
5.1 UDSTEDELSE AF AKKREDITIVER.....	40
5.2 BINDING (ASSOCIERING) MELLEM AKKREDITIVER FOR FYSISKE OG JURIDISKE PERSONER.....	40
6. KRAV TIL IDENTITETSBROKERE	41
7. GOVERNANCE.....	50
7.1 EJERSKAB OG VEDLIGEHOLDELSE AF STANDARDEN.....	50
7.2 OPHØR OG FRATAGELSE.....	50
7.3 ANSVAR OG FORSIKRING.....	50
7.4 OMKOSTNINGER	51
7.5 DELING AF SIKKERHEDSHÆNDELSER.....	51
8. REFERENCER.....	51
9. HØRTE PARTER.....	53

1. INDLEDNING og overordnede kommentarer

Danske Regioner
<p>Danske Regioner har modtaget et forslag til revidering af National Standard for Identiteters Sikringsniveauer (NSIS) til version 2.0.</p> <p>I Danske Regioner og regionerne hilser vi forslaget velkomment. Vi er enige i de foreslåede ændringer i NSIS 2.0.</p> <p>Vi bemærker dog, at vi finder det problematisk at anvende begrebet ”<i>akkreditiv</i>”. Vi foreslår, at der i stedet anvendes begrebet ”<i>identifikationsmiddel</i>”. Vi opfordrer til, at man på tilsvarende vis tilretter begrebsanvendelsen i referencearkitekturen, således at der er overensstemmelse mellem begreberne.</p>
<p>Svar:</p> <p>Digitaliseringsstyrelsen har opdateret begrebsanvendelsen i NSIS, således at begrebet ’Elektronisk Identifikationsmiddel’ erstatter begrebet ’Akkreditiv’. Herved er der på dette punkt overensstemmelse mellem eIDAS forordningen og NSIS.</p>

Datatilsynet
<p>Ved e-mail af 26. juni 2018 har Digitaliseringsstyrelsen anmodet om Datatilsynets bemærkninger til ovennævnte udkast.</p> <p>Generelt bemærkes, at Datatilsynet går ud fra, at den behandling af personoplysninger, som udkastene indebærer, sker inden for rammerne af databeskyttelsesforordningen og databeskyttelsesloven.</p> <p>Datatilsynet skal i den forbindelse understrege, at tilsynet med afgivelsen af dette høringssvar ikke har foretaget en vurdering af de omtalte eksisterende løsninger, herunder af hvorvidt den behandling af personoplysninger, som disse anvendes ved, lever op til databeskyttelsesforordningens krav om sikkerhed mv., og om løsningerne vil kunne anvendes.</p>
<p>Svar:</p> <p>Datatilsynets bemærkninger er taget til efterretning.</p>

Erhvervsstyrelsen
Erhvervsstyrelsens Team Effektiv Regulering (TER) vurderer, at

bekendtgørelsesudkastet medfører administrative konsekvenser under 4 mio. kr. årligt for erhvervslivet. De bliver derfor ikke kvantificeret yderligere.

Svar:

Digitaliseringsstyrelsen vurderer, at NSIS kan bidrage til øget standardisering af sikringsniveauer for digitale tjenester, hvilket alt andet lige vil føre til øget sikkerhed, øget modenhed og øget interoperabilitet, som er grundlag for yderligere digitalisering. I forlængelse heraf kan det endvidere oplyses, at det forventes at være en ganske lille del af danske virksomheder (under 100), som vil få brug for at anmelde en identifikationsordning eller identitetsbroker til Digitaliseringsstyrelsen.

Finans Danmark

Finans Danmark støtter generel, at der i stigende grad er brug for en fælles ramme for tillid til digitale identiteter samt behovet for at indføre mulighed for større fleksibilitet gennem anvendelse af flere sikringsniveauer ved identifikation over for forskellige selvbetjeningsløsninger og skabe samspil mellem løsninger på tværs af den offentlige sektor. Opdateringen giver anledning til konkrete bemærkninger og forslag til ændringer. Disse følger nedenfor.

Svar:

Digitaliseringsstyrelsen er enig i de overordnede betragtninger.

KOMBIT

Generelle bemærkninger

KOMBIT bemærker, at der generelt kan være et behov for nærmere at beskrive standardens anvendelse/ikke anvendelse, når der er tale om almindelige personoplysninger, der skal behandles fortroligt og denne behandlings sammenhæng med standardens behandling af ”følsomme personoplysninger”.

KOMBIT bemærker også, at der – forudsat, at der er tale om det samme - kan være behov for en mere konsekvent brug af begreberne ”ID-tjenester” og ”Identitetstjenester”, og hvis der ikke er tale om det samme, at forskellen præciseres.

Svar:

Standarden er præciseret i forhold til sondringen mellem fortrolige og følsomme

oplysninger.

Ligeledes er begrebet Identitetstjeneste konsekvent erstattet med begrebet ID-tjeneste.

Lakeside

Lakeside anerkender det grundige arbejde Digitaliseringsstyrelsen har lagt i ajourføringen af NSIS og har ingen grundlæggende indvendinger til opdateringerne til standarden.

Svar:

Bemærkningen er taget ad notam.

Nets

Den opdaterede NSIS standard er blevet mere klar i det benyttede sprogbrug. Definitionen af Autentifikation er blevet mere præcis og indførelsen af sikringsniveau (LoA) har gjort dokumentet mere præcist.

Den danske NSIS standard V 2.0 synes imidlertid på visse områder at bevæge sig væk fra teksterne i eIDAS forordningen, ” eIDAS Implementing Regulation (EU) 2015/1502” og ” Guidance for the application of the levels of assurance which support the eIDAS Regulation”.

Dette kan være et problem i forhold til danske eID løsningers accept i andre europæiske lande og omvendt, idet både danske og europæiske tjenesteudbydere og eID tillidstjenesteudbydere orienterer sig imod de nationale tekster, og således må opleve, at bestemmelser og tolkninger ikke er ensartede på tværs af landegrænser.

Dette kan for eksempel skabe tvivl om, hvorvidt et generelt ansvar for sikring af data som i Danmark vurderes at kunne opfyldes med et dansk eID med sikringsniveau Høj også kan opfyldes med fx et spansk eID med et spansk sikringsniveau Høj. Det må formodes at hensigten har været, at ansvaret for sikring af data skal kunne basere sig på ensartede sikringsniveauer.

Derfor anbefales det, at overensstemmelse med de europæiske tekster tilstræbes, og særlige danske præciseringer placeres synligt uden for det europæiske rammeværk.

Svar:

Digitaliseringsstyrelsen anerkender hensynet bag bemærkningen, men mener samtidig, at der nationalt er brug for en mere tydelig ramme som NSIS, som på visse områder er tilpasset danske forhold. Det er i videst mulige omfang tilstræbt, at et elektronisk identifikationsmiddel, som opfylder NSIS på et bestemt

sikringsniveau, også ville kunne opfylde eIDAS-kravene på samme sikringsniveau. Det er dog samtidig forventningen, at de færreste danske Elektroniske Identifikationsordninger skal anmeldes som nationale elektroniske identifikationsordninger under eIDAS, mens der er et stort behov for at anmelde lokale danske ordninger til Digitaliseringsstyrelsen, herunder identitetsbrokere i form af lokale IdP'er for en virksomhed.

Skatteforvaltningen

Forventninger til myndighedernes sikkerhedsniveauer

Standarden og den tilhørende vejledning beskriver nogle forskellige kategorier af krav på hhv. ”lav, betydelig og høj” niveau. Men ingen steder fremgår det, at det forventes at en myndighed lever op til fx ”betydelig” eller ”høj” niveau. Det er op til myndighederne selv at vælge hvilket niveau, deres sikringstjenester skal fungere på.

Vi savner en vejledning i hvilke sikkerhedsniveauer, myndighederne skal kræve i forhold til de opgaver, som skal udføres. F.eks. bør sikkerhedsniveauet for verifikation af en identitet defineres ens for alle myndigheder, idet identiteter anvendes på tværs af myndigheder og ikke kun ift. den enkelte myndigheds egne digitale tjenester. En generel vejledning i valg af sikkerhedsniveau til konkrete tjenester (gerne eksemplificeret) vil hjælpe os til at vælge konsistente niveauer på tværs af myndighederne.

Svar:

Digitaliseringsstyrelsen henleder opmærksomheden på flg. passus i NSIS:

Ansaret for vurdering af krav til Sikringsniveau og risikoniveau for den enkelte forretningstjeneste ligger hos den enkelte myndighed/udbyder, som er dataansvarlig for de data, som udstilles og kan tilgås via tjenesten. Der kan i denne forbindelse henvises til publikationen [TU-LoA], som indeholder vejledning til tjenestudbydere om risikovurdering, der kan guide til fastlæggelse af behov for Sikringsniveau.

Den ønskede vejledning er således separat fra NSIS.

Datatilsynet

1. Forskelle på eIDAS og NSIS

Datatilsynet kan umiddelbart konstatere, at der er forskel på begrebet "IDtjeneste", som anvendes i NSIS, og det relaterede begreb "tillidstjeneste", som anvendes i eIDAS3. "ID-tjeneste" dækker over alle processer og således mere end begrebet "tillidstjeneste" i eIDAS.

På den baggrund foreslår Datatilsynet, at forskellen nævnes i vejledningens pkt. 1.2 om forskelle på eIDAS og NSIS.

Svar:

Begrebet "tillidstjeneste" er blevet yderligere beskrevet under begrebet 'ID-tjeneste' i NSIS.

KOMBIT

Bemærkninger til udkast til vejledning til NSIS, version 2.0

Generelle bemærkninger

Nogle af kravene mangler konkrete objektive opfyldelseskriterier fx vedrørende entropi af passwords. Formålet forudsættes at sikre ensartethed, og resultatet af at overlade den slags til den enkeltes vurdering indebærer en risiko for det modsatte. Det foreslås, at der hentes inspiration vedrørende dette punkt i den tilsvarende vejledning fra NIST, som fremstår tydeligere.

Sikkerheden på den enhed (PC/mobiltelefon) brugeren benytter er åbenbart til dels uden for scope – en præcisering heraf kunne være ønskelig. Når eksempelvis en SSO session benyttes til udstedelse af et sikkerhedstoken fra en broker er det vurderingen, at det vil være af afgørende betydning, at brugerens enhed er beskyttet på samme niveau, som de tjenester NSIS stiller krav til. Det foreslås, at det præciseres, hvorfor beskyttelsen af akkreditiver behandles, også når det har implikationer for brugerens enhed, mens beskyttelsen af fx session cookies ikke behandles.

Specifikke bemærkninger

Kapitel 6, punkt 10 i skema

- det foreslås, at "følsomme personoplysninger" ændres til "almindelige fortrolige personoplysninger og følsomme personoplysninger"
- i vejledningstekst til ovenstående er netop "fortrolige" oplysninger nævnt sammen med "følsomme" oplysninger, jf. KOMBIT's forslag om samme.

<p>Svar:</p> <p>Detaljerede krav til passwordlængder og entropi vurderes at være for specifikt til det niveau, NSIS er specificeret på. NSIS er som beskrevet i indledningen udformet som en såkaldt 'outcome-baseret' standard i tråd med eIDAS – modsat NIST standarden, som er langt mere teknisk specifik. Det samme gælder specifikke krav til udstyr. I stedet stilles krav til det sikkerhedsniveau, som skal opnås som resultat, hvilket indirekte vil omfatte krav til den underliggende tekniske implementering.</p> <p>Det bemærkes, at krav til sessionsbeskyttelse findes beskrevet i kapitel 6 vedr. Identitetsbrokere.</p> <p>Endelig er formuleringen vedr. følsomme personoplysninger blevet udvidet til også at dække fortrolige oplysninger.</p>

Skatteforvaltningen
<p>Anvendelse af data på tværs af løsninger med forskellige sikkerhedsniveauer</p> <p>Når vi indfører og opererer med forskellige sikkerhedsniveauer (LoA) introducerer vi måske en afledt problemstilling om klassificering af datas rigtighed. Hvis data f.eks. er indsamlet fra en borger under et lavt sikkerhedsniveau på én myndigheds selvbetjeningsløsning, bør en anden myndighed ikke anvende dem til formål, der kræver et betydeligt sikkerhedsniveau. Denne problemstilling kunne nævnes som et opmærksomhedspunkt i vejledningen.</p>
<p>Svar:</p> <p>Relevansen af den beskrevne problemstilling anerkendes, men NSIS har ikke til formål at regulere forhold vedr. dataudveksling mellem myndigheder eller klassificering af data. Fokus er alene på identiteters sikringsniveau.</p>

1.2 Introduktion

KOMBIT
<p>Kapitel 1.2, 4. afsnit</p> <p>- ”bl.a.” det foreslås, at det kort angives, hvilke yderligere krav, der</p>

måtte være relevante ud over de nævnte samt eventuel henvisning til, hvor disse eventuelle yderligere krav er beskrevet.
Svar: Der er ikke yderligere krav til NSIS udover dem som står i standarden. Teksten, som nævnes, står i introduktionen for at sætte scenen for, at NSIS omfatter krav både til tekniske-, juridiske- og økonomiske forhold.

1.3 Formål og scope

Danske Regioner
Desuden mangler vi i høj grad en præcisering af anvendelsen af sikringsniveauer i forhold til de data, der tilgås. I afsnit 1.3 påpeges det, at tilgang til persondata stiller særlige krav – det ville være fornuftigt at få det konkretiseret og konkrete henvisninger til Persondataloven m.v. Der henvises endvidere til "Vejledning af sikringsniveau for identiteter" af marts 2017. Den trænger i høj grad også til en præcisering og opstramning, således at kravene til risikovurderingerne bliver tydelige og skarpe. Måske skulle denne vejledning lægges ind i vejledningen til NSIS for at gøre sammenhængen klar. Denne vejledning skal også gennemgås for rettelsen af den tidligere anførte begrebsfejl.
Svar: NSIS har eksplicit ikke til formål at stille krav til, hvilke sikringsniveauer en myndighed skal kræve i bestemte situationer, men derimod hvilket sikringsniveau et Elektronisk Identifikationsmiddel kan opnå. Digitaliseringsstyrelsen henleder i den forbindelse opmærksomheden på flg. passus i NSIS: <i>Ansaret for vurdering af krav til Sikringsniveau og risikoniveau for den enkelte forretningstjeneste ligger hos den enkelte myndighed/udbyder, som er dataansvarlig for de data, som udstilles og kan tilgås via tjenesten. Der kan i denne forbindelse henvises til publikationen [TU-LoA], som indeholder vejledning til tjenestendbydere om risikovurdering, der kan guide til fastlæggelse af behov for Sikringsniveau.</i> Denne formulering er tydeliggjort som følge af bemærkningerne hertil. Digitaliseringsstyrelsen opdaterer begreberne som følge af høringssvarene, idet 'Akkreditiv' bl.a. erstattes af 'Elektronisk Identifikationsmiddel', og vil konsekvensrette i de tilhørende vejledninger. Bemærk, at vejledningen til myndigheders risikovurderinger helt bevidst er meget overordnet, idet det som ovenfor nævnt er en eksplicit forudsætning, at den dataansvarlige myndighed selv

er ansvarlig for vurderingen, og ofte har brug for at tage højde for specifikke og konkrete forhold ved udformningen af denne risikovurdering

KOMBIT

Afsnit 1.3

- Publikation der henvises til [TU-LoA] er ikke opdateret og har således stadig 4 niveauer
- Det nævnes at identitetsbrokere er omfattet af NSIS, og så henvises der til, at enheder/devices og IoT på nuværende tidspunkt ikke er omfattet. Det foreslås, at det præciseres, hvad denne skelnen betyder for fx systemer, klientapplikationer og lignende.

Svar:

De øvrige publikationer og vejledninger vil blive konsekvensrettet, når NSIS 2.0 er færdig.

Sætningen, der henvises til i andet punkt, er et udtryk for, at Digitaliseringsstyrelsen finder, at området vedr. håndtering og identiteter for bl.a. IoT enheder ikke er tilstrækkeligt modent til, at det giver mening at standardisere endnu. Digitaliseringsstyrelsen følger området og vil overveje at opdatere NSIS, når modenheden af området er på et tilstrækkeligt højt niveau.

1.4 Eksempler på Identitetstjenester og sikringsniveauer

Ingen bemærkninger til dette punkt.

1.5 Terminologi

FR1

Side 6: ”... der afgør hvilke funktioner og data en bruger får adgang til...”. Rummer adgangskontrol både autentifikation af bruger og kontrol af adgangsrettigheder eller kun det sidste?

Svar:

Adgangskontrol er i NSIS beskrevet som separat fra autentifikation. Autentifikationen giver som output en identitet (hvem er vedkommende), som er

input til den efterfølgende adgangskontrol (hvad må vedkommende).

FR1

Side 6: "Akkreditiv". Brug ordet 'autentifikator' i stedet for 'akkreditiv' – ligesom NIST bruger ordet 'authenticator'. Men ellers er definitionen god.

Ordet 'akkreditiver' har i øvrigt i tekster som denne været anvendt til at betyde hele 3 forskellige ting, og det er nyttigt at der opnås en præcisering. De 3 ting er:

- 1) Det, som en bruger får i hænde til at autentificere sig med (autentifikatorer).
- 2) De data, som en bruger producerer vha sin(e) autentifikator(er) mhp at autentificere sig (kald disse data for autentifikations-data)
- 3) De data, som haves centralt mhp at verificere autentifikations-data og knytte korrekt e-identitet dertil. Disse data kunne kaldes verifikationsdata.

Det er den første betydning som definition her foreslår. Man skal være opmærksom på ikke at anvende ordet i de andre betydninger.

I øvrigt anbefales det at tilføje følgende:

Kombinationen af 2 (eller flere) akkreditiver (autentifikatorer), kaldes også et akkreditiv (autentifikator), når denne kombination anvendes til samlet 2-faktor /multi-faktor autentifikation.

Svar:

På baggrund af de mange høringssvar vedr. begrebsanvendelsen har Digitaliseringsstyrelsen valgt at udskifte begrebet 'Akkreditiv' med 'Elektronisk Identifikationsmiddel', hvilket også er det anvendte begreb i eIDAS. Samtidig er det præciseret i NSIS, at en kombination af flere Elektroniske Identifikationsmidler tilsammen kan opfattes som et Elektronisk Identifikationsmiddel.

FR1

Side 7: "...en løs kobling mellem Akkreditiver og Identiteter." En e-identitet kan have flere autentifikatorer. Men gælder omvendt at en autentifikator kan være knyttet til flere e-identiteter?

Svar:

Ja, dette er muligt men altid for samme Entitet. Dette er præciseret i teksten.

FR1

Side 7: "...Elektronisk Identifikationsmiddel...". Begrebet er ikke defineret. Mht definitionen, Skriv f.eks. Autentifikationsfaktor
Et element, som er kontrolleret af bruger og som skal anvendes ifm en autentifikation. Elementet tilhører en af kategorierne:....

Svar:

Begrebsanvendelsen er opdateret jf. tidligere kommentar, således at begrebet 'Akkreditiv' erstattes med 'Elektronisk Identifikationsmiddel', som også er det anvendte begreb i eIDAS.

FR1

Side 7-8: "... I dette dokument anvendes begreberne *basalt*, *moderat* og *højt* om forskellige angrebsstyrker. Terminologien er taget fra [ISO15408]."

Hent definitionerne fra ISO-dokumentet og gengiv dem i dette dokument.

Svar:

Digitaliseringsstyrelsen vil overveje at udbygge vejledningen til NSIS med yderligere forklaringer, uden at ISO15408 på nogen måde kan gengives i sin fulde længde, da dette er en meget omfangsrig standard.

FR1

Side 8: "Dynamisk Autentifikation".

Definér kort: Autentifikation baseret på éngangskoder eller andet der ikke kan anvendes til mere end ét autentifikationsforsøg.

Svar:

Digitaliseringsstyrelsen ønsker at bevare den nuværende definition, da denne er

mere åben og ikke låst til en bestemt implementering (fx engangskoder). Definitionen er i øvrigt taget direkte fra eIDAS.

Lakeside

1. I afsnit 1.5 anvendes stadig begrebet 'Elektronisk Identifikationsmiddel' i stedet for det mere generelle begreb 'Akkreditiv' (som ikke behøver at være elektronisk) under begrebsforklaringen for 'Autentifikationsfaktor' og 'Dynamisk Autentifikation'. Det forslås at fjerne 'Elektronisk Identifikationsmiddel' til fordel for 'Akkreditiv', samt fjerne selve begrebsforklaringen for 'Elektronisk Identifikationsmiddel' (som peger på 'Akkreditiv').
2. Sproglig forbedringsforslag til afsnit 1.5 under 'Identitetsbroker': Erstat '.... Som kræver tillid (**en** såkaldt *trusted third party*) fra forretningstjenester...' med '... som kræver tillid (**optræder som** såkaldt *trusted third party*) fra forretningstjenester...'.
3. I figur 1 afbildes 'Akkreditiv', som om at det kun kan være et 'Smart card' eller et 'Nøglekort'. Figuren bør for god ordens skyld udvides til at tillade andre (og ikke nærmere bestemte) typer af akkreditiver.

Svar:

1. Begrebsanvendelsen vedr. 'Akkreditiv' og 'Elektroniske Identifikationsmidler' er opdateret jf. tidligere kommentarer.
2. Kommentaren vedr. *trusted third party* er implementeret.
3. Kommentarer er indarbejdet.

Finans Danmark

Afsnittet definerer begrebet "Identitet (Elektronisk)". I de øvrige definitioner henvises både til "Identitet" og "identitet", hvilket skaber forvirring. Finans Danmark finder, at det bør fremgå klart, når der er tale om "Identitet (Elektronisk)" for også at sikre en klar adskillelse til begrebet "Entitet". Finans Danmark finder samtidig, at der er behov for en definition af begrebet "Elektronisk Identifikationsmiddel", idet begrebet anvendes under beskrivelsen af "Autentifikationsfaktor". Herudover henvises til bemærkningerne under afsnit 3.2.1 vedrørende begrebet "Akkreditiv".

Svar:

Begrebsanvendelsen er opdateret jf. tidligere svar.

FR1

Side 8: "Identitet (Elektronisk): En digital persona repræsenteret ved et sæt af attributter, som fx kan repræsentere en fysisk eller juridisk person, eller en fysisk person, der er associeret med en juridisk person. En Identitet *kan* rumme Personidentifikationsdata men kan også være pseudonym. "

Udtrykket 'digital persona' er ikke nogen hjælp, fordi det i sig selv kræver nogen forklaringer og faktisk er et helt overflødigt begreb.

Følgende konkrete definition bør overvejes:

En elektronisk Identitet består af

- 1) En brugerID og den eller de tilhørende (aktive) autentifikator(er), hvormed ejeren kan autentificere sig.
- 2) Information, der entydigt angiver den fysiske eller juridiske person, der ejer den elektroniske Identitet og har kontrol over autentifikator(er).

Det anbefales at man skelner mellem en de karakteristika, som udpeger en fysisk eller juridisk person, og så dennes eventuelle e-identitet. Der skal så at sige mere til e-identiteten, nemlig det der sætter personen i stand til at agere som identitet overfor digitale services.

Brug derfor gerne termen e-identitet eller e-ident, så man tydeligt skelner, også når man ikke ønsker at bruge den lange term 'elektronisk identitet'.

Svar:

Digitaliseringsstyrelsen finder, at de foreslåede formuleringer vedr. brugerID er for specifikke, og at karakteriseringen af en Identitet som en samling attributter er alment udbredt bl.a. i den fællesoffentlige referencearkitektur for brugerstyring. Derfor er den nuværende definition bevaret.

FR1

Side 8: "Identitetsbroker".

Identitetsbroker skal defineres klarere. Regnes en tjenesteudbyder, der foretager en SSO som en Identitetsbroker?

Svar:

Definitionen er blevet præciseret. Det fremgår af NSIS, at man skal formidle identiteter til tredjeparter for at være Identitetsbroker, så i det nævnte eksempel vil der ikke i udgangspunktet være tale om en Identitetsbroker.

FR1

Side 9: ”Graden af tillid til en påstået Identitet...”

Brug ’autentificeret’ i stedet for ’påstået’.

Svar:

Forslaget er indarbejdet i NSIS.

FR1

”...Begrebet LoA kan dekomponeres i flere underbegreber: **IAL** (*Identity Assurance Level*) som beskriver styrken af Identitetssikringsprocessen, **AAL** (*Authentication Assurance Level*) som beskriver Autentifikationsprocessens styrke, og **FAL** (*Federation Assurance Level*), som beskriver sikringsniveauet for en Identitetsbroker.”

Når man senere læser, hvad IAL, AAL og FAL står for, må man konstatere at fx sikkerhed omkring tildeling af autentifikatorer ikke er medtaget.

Men tilliden til en autentificeret e-Identitet afhænger dog i høj grad af om brugeren har fået givet sine autentifikatorer i hænde på sikker vis. Faktisk er der gode grunde til at forvente at netop indrullering / genindrullering vil være de svage punkter i fremtiden.

Konklusion: Brug ikke LoA baseret på kun IAL, AAL og FAL. Det gør NIST heller ikke mere.

Hvis man ønsker at tale om et samlet sikringsniveau, så skal alle tabeller medtages. NIST vælger vist blot at tale om sikringsniveau for enkelte tabeller.

Definitionen bør derfor genovervejes, hvis sikringsniveau’er primært er noget man angiver for de enkelte del-processer -for at specificere deres styrke- snarere end at angive den samlede tillid til autentificeret e-Identitet.

Svar:

Digitaliseringsstyrelsen finder, at der både er behov for at definere sikringsniveauer for delprocesser (IAL, AAL og FAL) og for det samlede niveau (LoA). Det samlede niveau er også udgangspunktet i eIDAS forordningen.

Begreber IAL og AAL er yderligere præciseret i NSIS, og inkl. hvilke delprocesser, som indgår i vurderingen af disse.

Datatilsynet

2. Begreber

Det fremgår af udkast til NSIS version 2, pkt. 1.5, at "person" defineres som en fysisk eller juridisk person.

Datatilsynet skal i den sammenhæng bemærke, at verifikationen af juridiske personer fremstår cirkulær i brugen af begrebet "person" (tilsynet kan ikke vurdere, om dette er tilsigtet).

I vejledningen er der primært henvist til, at fysiske personer i sidste ende verificerer tegningen af den juridiske person.

Den nuværende konstruktion, som fremgår af den nationale standard, giver mulighed for verifikation udelukkende gennem juridiske personer.

Herudover kan Datatilsynet konstatere, at begrebet "ansøger" ikke anvendes på en konsistent måde, ligesom begrebet ikke er defineret.

Svar:

Hvis Datatilsynet henviser til formuleringen om, at registrering kan gennemføres af en 'person', som så iflg. definitionen både kan være en fysisk eller juridisk person, er dette helt tilsigtet.

Begrebet 'ansøger' er blevet præciseret i afsnit 3.1.1.

FR1

Figur 1, side 10: "...Akkreditiv".

Menes der, at samme Akkreditiv kan tilknyttes flere Identiteter?

Det kan give mening. Men kan samme akkreditiv også tilknyttes flere forskellige

(fysiske) personer?

Svar:

Ja, et Akkrediv (nu Elektronisk Identifikationsmiddel) kan være tilknyttet flere Identiteter, men altid for samme Entitet.

2. LIVSCYKLUS FOR AKKREDITIVER

Lakeside

I afsnit 2 beskrives 'Suspending' processen som en del af livscyklussen, men denne mangler at blive tilføjet til figur 2.

Svar:

Figuren er opdateret.

KOMBIT

Side 11

- Figur 2, Processer afspejles i figuren og listes derefter i teksten, men processerne "Aktivering" og "Suspending" vises ikke på figur, kun i teksten. Ligesom tre underprocesser i figuren ikke kommenteres i teksten.

Svar:

Figuren er opdateret.

Danske Regioner

Den mest generelle og væsentligste kommentar, har drejer sig om begrebsapparatet. Begrebet *akkreditiv* er problematisk at bruge i notatet. Ihukommende ERSTs kommentar til det seneste referat fra Følgegruppen: "Det vil fx være uheldigt at kommunikere om *akkreditiver*, som er det korrekte faglige begreb, men som ingen almindelig bruger vil forstå."

Vi er i regionerne helt enige med ERST. Begrebet "akkreditiv" er ikke heldigt at anvende i denne sammenhæng. DIGST er også selv klar over, at det ikke er et heldigt begrebsvalg, idet man har fundet det nødvendigt at anføre: "begrebet 'Akkreditiv' i NSIS anvendes synonymt med begrebet 'Authenticator' i [NIST] - og altså ikke begrebet 'Credential', som i [NIST] anvendes som betegnelse for

bindingen mellem en identitet og en eller flere 'Authenticators'."

I regionerne mener vi, at begrebet "identifikationsmiddel" (eller "log-in middel", hvis det skal populariseres) er langt bedre. Vi mener, at NIST's begrebsmodel er god – så god, at det også i internationale sammenhænge er det rigtige at anvende. Så vil en anvendelse af "akkreditiv" i betydningen "Authenticator" være forkert; en bedre "oversættelse" er "Identifikationsmiddel".

Helt galt går det med figur 3, hvor "Credential" er brugt i betydningen "Authenticator" – altså for fagfolk, der kender NIST, er fuldstændigt forvirrende og en forkert grafisk fremstilling af blandt andet håndteringen af Identifikationsmidler. Under alle omstændigheder skal denne tegning ændres, så den også bliver i overensstemmelse med DIGST's brug af NIST-termer – allerhelst oversættes til dansk, så den slags misforståelser undgås.

Vi er naturligvis klar over, at bl.a. Referencearkitekturen for Brugerstyring bruger begrebet "Akkreditiv" i betydningen "Identifikationsmiddel"; men det er ikke en fejl at blive klogere – og Referencearkitekturen (og de øvrige relaterede dokumenter) bør rettes tilsvarende. Indtil det er sket, skal der blot en fodnote til at beskrive en bedre begrebsmodel end referencearkitekturens – indtil den bliver rettet.

Svar:

Begrebsanvendelsen er opdateret jf. tidligere kommentar, således at begrebet 'Akkreditiv' erstattes med 'Elektronisk Identifikationsmiddel', som også er det anvendte begreb i eIDAS.

Figur er udgået fra dokumentet, da den med begrebsopdateringen ville være vildledende, og da dens værdi er vurderet som begrænset.

3. NORMATIVE KRAV

Lakeside

I NSIS 2.0 er sikringsniveau 'begrænset' udgået. I NSIS 1.0 kunne sikringsniveauerne let mappes til en heltalsrepræsentation (fra 1 til 4), som fx kunne blive anvendt i broker-udstedte tokens. Nu hvor niveauet 'begrænset' er udgået savnes en angivelse af hvordan de bibeholdte tre niveauer bør mappes i en heltalsrepræsentation. Er det 2, 3 og 4 eller 1, 2 og 3?

Svar:

For at undgå forvirring om betegnelsen af sikringsniveauerne mellem NSIS 1.01 og NSIS 2.0 har Digitaliseringsstyrelsen bevidst fravalgt at benytte heltal men i stedet anvendt betegnelserne 'Lav', 'Betydelig' og 'Høj'. Dette samme gør sig i

øvrigt gældende for eIDAS.

FR1

Side 13: ”Normative krav”.

Ordet ’normative’ tilføjer ingen forståelsesmæssig værdi. Skriv i stedet: Krav til akkreditiver herunder udstedelse, håndtering og anvendelse.

Svar:

Betegnelsen er helt sædvanlig for tekniske standarder og tjener til at adskille indledningen fra de egentlige krav. Betegnelsen bevares derfor.

FR1

Side 13: ”... Det samlede Sikringsniveau (LoA) dikteres af det mindste Sikringsniveau opnået på de specifikke områder nedenfor. Med andre ord, skal samtlige krav til fx niveau ’Betydelig’ opfyldes, før en Elektronisk Identifikationsordning kan siges at leve op til NSIS på niveau ’Betydelig’”.

Lyder rimeligt. Det var vel det, der skulle have stået i definitionen.

Men der er en modstrid til senere, hvor LoA sættes lig minimum af IAL, AAL og FAL.

Svar:

Beskrivelsen af IAL og AAL er præciseret som følge af kommentaren.

FR1

Side 13: ” Kravene er i udgangspunktet formuleret resultatbaserede (*outcome-based*), således at de primært sigter på resultatet af bestemte kontroller og processer (det ønskede, kvalitative niveau), frem for at diktere metoden til at opnå niveauet. Dette er valgt af hensyn til at muliggøre forskellige teknologier og løsninger, og da dette også er tilgangen i [LOA]. Der er dog afvigelser fra denne tilgang, så reelt er kravene en blanding af flere tilgange.”

Kan udelades uden at der mistes noget.

Svar:

Det vurderes, at beskrivelsen bibringer en forståelse for, hvordan NSIS er udformet, som er relevant baggrundsinformation for læseren.

3.1 REGISTRERINGSPROCESSEN

Ingen bemærkninger til dette punkt.

3.1.1 Ansøgning

Nets

Afsnit 3.1.1 Ansøgning

Kommentar: NSIS V 2.0 har introduceret en ny bestemmelse jf. 4) nedenfor. Dette kan give god mening, men er en skærpelse i forhold til eIDAS Forordningen, som ikke har denne bestemmelse.
NSIS v 2.0

Betydelig 4) ”Ansøgeren skal afkræves accept af betingelser og tilkendegive at have læst dem”

I forhold til:

Commission Implementing Regulation (EU) 2015/1502 of 8. September 2015

Low:

- 1.Ensure the applicant is aware of the terms and conditions related to the use of the electronic identification means.
- 2.Ensure the applicant is aware of recommended security precautions related to the electronic identification means.
3. Collect the relevant identity data required for identity proofing and verification.

Svar:

Digitaliseringsstyrelsen er fuldt opmærksom på, at dette er en tilføjelse, og denne vurderes at være værdifuld. Det vurderes ikke problematisk, at den danske standard på dette punkt er skærpet i forhold til eIDAS.

3.1.2 Verifikation af Identitet (fysiske personer)

FR1
<p>Side 13: ”Dette afsnit stiller krav til Identitetssikring af ansøger (<i>identity proofing</i>), herunder validering og verifikation af Identitet inden udstedelse af Akkreditiver. Niveaueet af identitetssikring, som opnås jævnfør nedenstående tabel, betegnes IAL (Identity Assurance Level).”</p> <p>Identitetssikring er en del af registreringen. Dvs vi sikrer at den rette har ansøgt. Man ville forvente, at IAL også blev påvirket af selve udstedelsesprocessen, men det ser ikke ud til at være tilfældet.</p>
<p>Svar:</p> <p>Definitionerne er nu omstruktureret, så det er klarere, at hvilke krav og processer der indgår i vurderingerne af IAL og AAL.</p>

FR1
<p>Side 14: ”Betydelig”.</p> <p>Det foreslås at der tilføjes et krav:</p> <p>Processen for verifikationen af identitet skal skabe et sikkert grundlag for, at tildeling af akkreditiver sker til den rette person – enten ved informationer, der registreres om identiteten eller ved informationer, der gives til ansøger til anvendelse ved modtagelse/aktivering af akkreditiv(er).</p>
<p>Svar:</p> <p>Digitaliseringsstyrelsen finder, at den foreslåede formulering ikke er helt retvisende, idet identitetssikring handler om efterprøvelse af dokumentation – registrering er således en biproces.</p> <p>Nuværende formulering bevares derfor.</p>

Nets
<p>Afsnit 3.1.2 Verifikation af Identitet (fysiske personer)</p> <p>Kommentar: Der opfordres til, at de eksisterende identifikationsprocesser for</p>

udstedelse af pas og kørekort, (som refereret til nedenfor for sikringsniveau Betydelig pkt. 4), beskrives og indsættes i vejledningen til National Standard for Identiteters Sikringsniveauer (NSIS) til brug for RA enheder, da disse procedurer i dag kun anvendes af offentlige forvaltningsenheder og ikke kan antages at være alment kendte.

NSIS v 2.0

Afsnit 3.1.2 Verifikation af Identitet (fysiske personer)

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 an-søgeren ikke er besiddelse af dette, kan de samme identifikationsprocesser som be-nyttes ved udstedelse af dansk pas eller kørekort anvendes.”

Svar:

Indkopiering af identifikationsprocesser for udstedelse af pas og kørekort vurderes at have den ulempe, at NSIS så skal opdateres når disse processer ændres, og der vurderes derfor som værende mere smidigt at have disse beskrevet separat.

3.1.3 Verifikation af Identitet (juridiske personer)

FR1

Side 15: ” 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. Akkreditiver behøver ikke være fra den samme udsteder. Her skal det i givet fald kunne verificeres, at de pågældende Akkreditiver er gyldige og ikke spærret.”

IAL defineres tilsyneladende ikke for Juridiske Personer? Det ser kun ud til at være defineret ud fra den ovenstående tabel for fysiske personer. Er det en fejl?

Svar:

Dette var en fejl, som er rettet.

3.2 UDSTEDELSE OG HÅNDTERING AF AKKREDITIVER

Ingen bemærkninger til dette punkt.

3.2.1 Styrke af akkreditiver

Nets
<p>3.2.1 Styrke af Akkreditiv</p> <p>Kommentar: Idet man har fjernet bestemmelsen om ”At det elektroniske identifikationsmiddel gør brug af en faktor” har man formentlig utilsigtet skærpet NSIS i forhold til eIDAS. Nu kan det fortolkes som om NSIS kræver adgangskontrol for at anvende den ene faktor. Kan fortolkes som at en nøgleviser skal have en lokal adgangskontrol. Dette er vel ikke hensigten med at fjerne bestemmelsen om at der skal benyttes mindst en faktor.</p> <p>NSIS v 2.0</p> <p>3.2.1 Styrke af Akkreditiv</p> <p>Lav: 1)</p> <p>”Akkreditivet er udformet således, at udstederen tager rimelige skridt til at kontrollere, at det kun er den Person, som de tilhører, der har kontrol over og er i besiddelse af det.”</p> <p>I forhold til:</p> <p>Commission Implementing Regulation (EU) 2015/1502 of 8. September 2015</p> <p>2.2.1. Electronic identification means characteristics and design</p> <p>Low:</p> <ol style="list-style-type: none">1. The electronic identification means utilises at least one authentication factor.2. The electronic identification means is designed so that the issuer takes reasonable steps to check that it is used only under the control or possession of the person to whom it belongs.
<p>Svar:</p> <p>Det nævnte krav er genindført.</p>

Finans Danmark
<p>Afsnit 3.2.1 indeholder følgende beskrivelse af sikringsniveau ”betydelige” i forbindelse med styrke af Akkreditiv: ”Akkreditivet er udformet således, at det med betydelig sikkerhed kan antages, at det kun kan bruges, når det er den Person, som det tilhører, der har kontrol over eller er i besiddelse af det.”</p> <p>Finans Danmark foreslår, at ordet ’kan’ i linje 2 udgår af beskrivelsen for at sikre overensstemmelse med den engelske version af Kommissionens</p>

gennemførelsesforordning 2015/1502 i henhold til eIDAS forordningen (herefter Kommissionens gennemførelsesforordning). Beskrivelsen er herefter følgende: ”Akkreditivet er udformet således, at det med betydelig sikkerhed kan antages, at det kun bruges, når det er den Person, som det tilhører, der har kontrol over eller er i besiddelse af det.”

Finans Danmark herudover foreslår, at beskrivelsen suppleres med et yderligere krav: ”Akkreditivet gør brug af mindst to autentifikationsfaktorer fra forskellige kategorier” Finans Danmarks forslag lægger sig ligeledes op ad formuleringen i Kommissionens gennemførelsesforordning. Finans Danmark finder samtidig, at det i terminologien (afsnit 1.5) under beskrivelsen af ”Akkreditiv” bør fremgå klart, at et akkreditiv kan være en kombination af 2 akkreditiver.

Således kan et password og en nøgleviser hver for sig være et akkreditiv, men også kombinationen af password og nøgleviser er et akkreditiv. Sidstnævnte akkreditiv (kombinationen) opfylder kravet om at ”gøre brug af mindst to autentifikationsfaktorer fra forskellige kategorier”, jf. Kommissionens gennemførelsesforordning. Samtidig undgås uklarheder om, hvorvidt en nøgleviser skal beskyttes med en PIN-kode. Ifølge gennemførelsesforordningen er en nøgleviser uden PIN-kode ikke i sig selv et akkreditiv på sikringsniveau ”betydelig”, men akkreditivet, der er en kombination af et password og samme nøgleviser, ligger på sikringsniveau ”betydelig”.

Med ovenstående forslag undgås misforståelser, og formuleringerne understøtter det behov for større fleksibilitet, som er identificeret i forbindelse med arbejdet med valide identiteter i den offentlige sektor og arbejdet med at anskaffe MitID.

Svar:

Bemærkningen er imødekommet - både hvad angår kravet om to faktorer og definitionen af Elektronisk Identifikationsmiddel.

Nets

Kommentar: Uden yderligere vejledning synes den danske tekst at kræve, at en anden bruger, som får fat i en brugers akkreditiv, ikke må være i stand til at bruge det. Dette kan hverken TOTP eller U2F tokens opfylde. Umiddelbart synes dette kun at kunne opfyldes af akkreditiver, som i sig selv omfatter flere faktorer. Dette krav var gældende i den tidligere version af NSIS v 1.01 hvor det ”samlede” elektroniske identifikationsmiddel skulle gøre brug af mindst to faktorer”. Kravet om de to faktorer er nu flyttet til afsnit 3.3.1.

NSIS v 2.0

3.2.1 Styrke af Akkreditiv

Betydelig 2): ” Akkreditivet er udformet således, at det med betydelig sikkerhed kan antages, at det kun kan bruges, når det er den Person, som

det tilhører, der har kontrol over, eller er i besiddelse af det.”

I forhold til:

Commission Implementing Regulation (EU) 2015/1502 of 8. September 2015

2.2.1. Electronic identification means characteristics and design

1. The electronic identification means utilises at least two authentication factors from different categories.
2. The electronic identification means is designed so that it can be assumed to be used only if under the control or possession of the person to whom it belongs.

Svar:

NSIS er opdateret således at bemærkningen er imødekommet, jf. tidligere svar.

FR1

Side 15: ”2) Akkreditivet er udformet således, at det med betydelig sikkerhed kan antages, at det kun kan bruges, når det er den Person, som det tilhører, der har kontrol over eller er i besiddelse af det.”

Denne formulering er ikke hensigtsmæssig, da den kan give anledning til flere misforståelser. Det er ikke sådan at mit password eller min nøgleviser kun kan bruges, når de er i min kontrol. Hvis nogen får fat i den ene eller den anden (eller begge), så kan denne uvedkommende jo bruge dem.

Man bør gå tilbage til den tekst, der er i dokumentet [LoA]. Der findes følgende definition af sikringsniveau 'Betydelig':

1. Det elektroniske identifikationsmiddel gør brug af mindst to autentifikationsfaktorer fra forskellige kategorier.
2. Det elektroniske identifikationsmiddel er udformet således, at det kan antages, at det kun kan bruges, når det er den person, som det tilhører, der har kontrol over og er i besiddelse af det.

Altså:

- a) Et Akkreditiv, som kun har 1 faktor kan ikke i sig selv kan ligge på niveau 'betydelig'.
- b) Krav nummer 2 er en dårlig oversættelse fra engelsk, idet ordet 'kan' er

<p>kommet med ved en fejltagelse, hvilket giver en anden betydning.</p> <p>Følgende tekst foreslås:</p> <p>Akkreditivet kræver mindst 2 autentifikationsfaktorer og er udformet, så det kan antages kun at blive brugt under ejers kontrol.</p>
<p>Svar:</p> <p>NSIS er opdateret således at bemærkningen er imødekommet, jf. tidligere svar.</p>
<p>KOMBIT</p>
<p>Side 15</p> <ul style="list-style-type: none"> - ”Akkreditivet er udformet således, at det med betydelig sikkerhed kan antages, at det kun kan bruges, når det er den Person, som det tilhører, der har kontrol over eller er i besiddelse af det”. Med denne formulering udelukkes brug af passwords, som jo kan bruges af enhver, der er i besiddelse af dem.
<p>Svar:</p> <p>Det er nu præciseret, at kravet går på det samlede Elektroniske Identifikationsmiddel og formuleringen er justeret. Passwords kan dog fortsat ikke stå alene på niveau Betydelig.</p>

3.2.2 Levering og aktivering

<p>Finans Danmark</p>
<p>Afsnit 3.2.2 indeholder følgende beskrivelse af krav til levering for sikringsniveau ”betydelig”: ”Akkreditivet leveres efter udstedelse via en mekanisme, som gør det muligt med betydelig sikkerhed at antage, at det kun udleveres til den Person, som det tilhører.”</p> <p>Finans Danmark finder, at kravet bør tydeliggøres. Såfremt udstedelsen af akkreditiver sker online, så skal det være et krav, at bruger (mindst) anvender et allerede aktivt akkreditiv på sikringsniveau ”betydelig” (dvs. 2-faktor) eller, at der anvendes tilsvarende kontroller. Finans Danmark foreslår, at følgende definition overvejes: ”Akkreditivet bringes under brugerens fulde kontrol via sikker mekanisme baseret på den forudgående verifikation af identitet (jf. 3.1.2 eller 3.1.3) eller andre tilsvarende kontroller. Mekanismen skal involvere mindst 2 uafhængige elementer, som begge medvirker til at sikre, at rette vedkommende får kontrol over akkreditivet.”</p>
<p>Svar:</p>

Digitaliseringsstyrelsen foreslår i stedet, at vejledningen evt. udbygges med eksempler, således at der fortsat er metodefrihed i forhold til, hvordan kravet opfyldes.

Den nævnte formulering er blevet afstemt med den tilsvarende bestemmelse i eIDAS.

FR1

Side 16: ”2) Akkreditivet leveres efter udstedelse via en mekanisme, som gør det muligt med betydelig sikkerhed at antage, at det kun udleveres til den Person, som det tilhører.”

En nærmest cirkulær definition, som svarer til:

”Sikringsniveau er ’Betydelig’, hvis man med ’betydelig’ sikkerhed kan antage at rette person har modtaget akkreditivet.”

Den meget omhyggelige verifikation af identitet, der beskrives i 3.1.2 bør være direkte forbundet med tildelingen af akkreditivet (autentifikator). Ellers er hele denne omhyggelig verifikation nærmest spildt.

Følgende tekst foreslås derfor:

”Akkreditivet bringes under brugerens fulde kontrol via sikker mekanisme baseret på den forudgående verifikation af identitet (se 3.1.2 eller 3.1.3) eller tilsvarende kontroller. Mekanismen skal kræve mindst 2 elementer, som begge bekræfter, at akkreditivet gives til rette vedkommende.”

Svar:

Den nævnte formulering i NSIS er afstemt med den tilsvarende bestemmelse i eIDAS.

Digitaliseringsstyrelsen foreslår i stedet, at vejledningen evt. udbygges med eksempler, således at der fortsat er metodefrihed i forhold til, hvordan kravet opfyldes.

KL

s. 16 afs: 3.2.2. levering og aktivering:

"...en mekanisme der gør det muligt at antage, at det kun udleveres til den tilsigtede person."

Vejledningen beskriver ikke hvordan "...en mekanisme gør det muligt at antage, at det kun udleveres til den rigtige person." kunne se ud. En vejledning/eksempel ville være passende.

Svar:

Digitaliseringsstyrelsen overvejer at opdatere vejledningen til NSIS.

Viborg Kommune

Ét af de elementer/krav i standarden, som mange Kommuner i øjeblikket er i gang med at afklare er, hvordan vi skal efterleve kravet om MultiFaktor Autentifikation. I forbindelse med MFA kravet er der et område i standarden, som vi ikke syntes er så klart beskrevet. Mange af os kikker på de digitale løsninger til multifaktor, hvor vi kan bruge en eksisterende personlig device som MFA komponent. Dette sker typisk via en App på en smartphone, tablet eller Windows pc. Nogle Kommuner overvejer også at anvende et personligt certifikat på en personlig pc og vil anvende dette certifikat som MFA komponent.

I begge scenarier er det afgørende hvilke krav vi skal leve op til i relation til "koble" MFA "device" til brugeren. I afsnit 3.2.2 der omhandler "Levering og aktivering" står der under sikkerhedsniveauet Betydelig:

"Akkreditivet leveres efter udstedelse via en mekanisme, som gør det muligt med betydelig sikkerhed at antage, at det kun udleveres til den Person, som det tilhører."

I vejledningen til standarden er der ikke omtalt scenarier med registrering af MFA device. Spørgsmålet er derfor hvor langt vi skal gå for at sikre entydig kobling mellem bruger og MFA device? Nogle af de nyere device baserede MFA løsninger på markedet som f.eks. Signaturgruppens SoloID løsning og den kommende OS2faktor løsning tager udgangspunkt i at en kobling mellem bruger og device kun kan ske via en NemID verifikation. Dvs. at brugeren skal identificere sig med NemID én gang, når et nyt device tages i brug som MFA device. Det er en god og sikker løsning, og i tråd med kravene omkring udlevering i afsnit 3.2.2 - men kan det gøres på andre måder? F.eks. ved at et device manuelt "tages" til brugeren af en it-servicedesk i forbindelse med udlevering. Eller hvis man bruger en SMS baseret 2-faktor løsning, og stoler på brugerkatalogets telefonbog, og via den godkender mobiltelefoner som MFA enhed på baggrund af mobilnummeret?

Et input kunne derfor være at vejledningen til standarden bliver lidt skarpere på

hvad der forventes i denne sammenhæng. Et af de udfordringer vi stadig møder i Kommunerne er nemlig, at nogle brugere IKKE vil bruge deres private NemID i arbejdsmæssig sammenhæng. Det er mig bekendt uklart om vi kan forlange dette, selv om dette jo er et lidt andet scenarie end det som datatilsynet tidligere har udtalt sig om i relation til brug af privat NemID til autentifikation i arbejdsmæssig sammenhæng (hvilket vi godt må tilbyde, men ikke kræver).

Svar:

Konkrete use cases passer dårligt ind i selve standarden, da denne skal være generisk. Digitaliseringsstyrelsen vil overveje at opdatere vejledningen med de nævnte eksempler.

3.2.3 Suspendering, spærring og genaktivering

FR1

Side 16: ... hvis der er tale om et Akkreditiv tilknyttet en juridisk person og virksomheden ophører eller går konkurs.”

Betyder det at en RA-funktion (for virksomheder) til stadighed må holde sig orienteret om hvorvidt en virksomhed, der har fået et akkreditiv, ophører eller går konkurs og i så fald spærre dette akkreditiv? Og hvis spærring ikke finder sted med det samme, er det så ansvarspådragende?

Svar:

Kravet går på udstederen af det Elektroniske Identifikationsmiddel og ikke RA-funktionen. Ofte vil det være hensigtsmæssigt at overvåge konkurser etc. via en automatisk mekanisme, der straks kan foranledige spærring det Elektroniske Identifikationsmiddel, når relevante hændelser indtræffer.

Nets

Kommentar: Der er indført en ny bestemmelse i NSIS v 2.0 punkt 5, som giver god mening, men det er en skærpelse i forhold til eIDAS, som ikke har denne bestemmelse.

NSIS v 2.0

Lav 5) ”Der gives en kvittering for spærring til ejeren af Akkreditivet, hvis det er muligt.”

I forhold til:

Commission Implementing Regulation (EU) 2015/1502 of 8. September 2015

2.2.2. Issuance, delivery and activation

Low: After issuance, the electronic identification means is delivered via a mechanism by which it can be assumed to reach only the intended person.

Svar:

Formuleringen er en tilsigtet præcisering – kravet om kvittering for spærring fremgår i øvrigt også af de nuværende OCES certifikatpolitikker.

3.2.4 Fornyelse og erstatning

Ingen bemærkninger til dette punkt.

3.3 ANVENDELSE OG AUTENTIFIKATION

Ingen bemærkninger til dette punkt.

3.3.1 Autentifikationsmekanismer

FR1

Side 17: ”1) Frigivelsen af personidentifikationsdata...”

Udtrykket ’Frigivelsen af personidentifikationsdata’ virker lidt forkert. Ved en autentifikation beviser en bruger vha sin/e autentifikator(er), at han ejer en bestemt brugerID. Til brugerID’en er knyttet personidentifikationsdata, der udpeger brugeren som person. TU, som har ønsket autentifikationen kan i hvert fald få den autentificerede brugerID, og formentlig også nogen personidentifikationsdata, men ikke nødvendigvis alle. Det er almindelig kendt at ikke alle TU’er kan få cpr.nr. for bruger

Svar:

Formuleringen stammer fra eIDAS og bevares derfor.

FR1
Side 17: "... øget basal Angrebskapacitet ..."
Betydningen af et sådant udtryk bør fremgå af definition eller kunne læses i særlig appendix.
Svar: I beskrivelsen af begrebet 'Angrebskapacitet' henvises til ISO15408. Digitaliseringsstyrelsen overvejer at opdatere vejledningen med yderligere beskrivelser.

FR1
Side 17-18: "...gætte, lytte sig til, gengive eller manipulere kommunikationen og på den måde omgå autentifikationsmekanismen."
Indsæt "eller" i stedet for "og".
Svar: Meningen med sætningen er 'og' – i øvrigt er formuleringen den samme i eIDAS, hvorfor den bevares.

FR1
Side 18: "... moderat Angrebskapacitet ..."
Definition bør være med i dokumentet
Svar: I beskrivelsen af begrebet 'Angrebskapacitet' henvises til ISO15408. Digitaliseringsstyrelsen overvejer at opdatere vejledningen med yderligere beskrivelser.

FR1
Side 18: "... høj Angrebskapacitet ..." ."
Definition bør være med i dokumentet
Svar: I beskrivelsen af begrebet 'Angrebskapacitet' henvises til ISO15408. Digitaliseringsstyrelsen overvejer at opdatere vejledningen med yderligere beskrivelser.

KOMBIT
Side 18 "7) Mindst ét af de anvendte Akkreditiver skal opfylde kravene til niveau 'Høj' angivet i afsnit 3.2.1." Det bør præciseres i hvilket omfang kategorierne "Lav" og "Betydelig" i forhold til alle akkreditiver skal være på samme niveau som autentifikationsmekanismen.
Svar: Bemærkningen er indarbejdet i form af opdateringen af definitionen af begrebet "Elektronisk Identifikationsmiddel".

KOMBIT
Side 18 - "8) Hvis flere Autentifikationsfaktorer stammer fra samme enhed, så skal faktorerne være udformet, så kompromittering af én faktor ikke bevirker, at andre faktorer på enheden kompromitteres." Det bør præciseres, om ordet "enhed" her er synonymt med akkreditiv, herunder om betingelsen ikke altid er gældende for multifaktoraутentifikation.
Svar: Her menes en fysisk enhed, der udgør en besiddelsesfaktor – altså noget som brugeren er i besiddelse af jf. definitionen af Autentifikationsfaktor. Efter nærmere overvejelse er det besluttet at fjerne kravet fra NSIS.

KOMBIT
<p>Afsnit 3.3.1</p> <ul style="list-style-type: none"> - Autentifikationsmekanismer. Det foreslås, at det præciseres og der gives nogle konkrete eksempler på hvilket sikringsniveau der skal anvendes alt efter hvilke typer af persondata (jf GDPR) der behandles, Fx håndteringen af Art 6 data skal som minimum sikres som NSIS niveau Lav og Art 9 og 10 data skal som minimum sikres som NSIS niveau Betydelig. Men disse kan ændre sig alt efter risikoanalysens udfald. <p>Svar:</p> <p>Digitaliseringsstyrelsen henleder opmærksomheden på flg. passus i NSIS:</p> <p><i>Ansvaret for vurdering af krav til Sikringsniveau og risikoniveau for den enkelte forretningstjeneste ligger hos den enkelte myndighed/udbyder, som er dataansvarlig for de data, som udstilles og kan tilgås via tjenesten. Der kan i denne forbindelse henvises til publikationen [TU-LoA], som indeholder vejledning til tjenesteudbydere om risikovurdering, der kan guide til fastlæggelse af behov for Sikringsniveau.</i></p> <p>Den ønskede vejledning er således separat fra NSIS, og der henvises til vejledningen for tjenesteudbydere refereret i ovennævnte.</p>

Nets
<p>3.3.1 Autentifikationsmekanismer</p> <p>Kommentar: Bestemmelsen om at ét af akkreditiverne skal opfylde kravene til Høj (se nedenfor) synes ikke at have støtte i hverken eIDAS Forordningen, PSD2 eller NIST.</p> <p>Kravet vil diskvalificere akkreditiver som ellers i kombination med andre akkrediter giver et stærkt sikkerhedsniveau.</p> <p>Hvis man fx ser på en løsning som FIDO U2F, hvor brugeren anvender et password og efterfølgende bekræfter identiteten med et U2F token, vil dette identifikationsmiddel kunne opfylde NSIS 1.01 "Høj" imens det tilsyneladende kun kan opfylde NSIS 2.0 "Betydelig". Dette skyldes det nye krav 3.3.1 punkt 7) samt at hverken password eller U2F alene kan opfylde kravene til NSIS 2.0 afsnit 3.2.1 "Høj" (endsige "betydelig") i de nuværende formuleringer.</p> <p>Dette er bekymrende, da denne standard er en af de eneste, som understøtter verifisering af impersonation resistance, som krævet af NIST på AAL 3. I forordningens tekst vil password plus U2F token også kunne være sikringsniveau</p>

høj, så vi må formode at andre europæiske lande placerer det således.

NSIS v 2.0

3.3.1 Autentifikationsmekanismer

Høj Punkt 7) ” Mindst ét af de anvendte Akkreditiver skal opfylde kravene til niveau 'Høj' angivet i afsnit 3.2.1.”

I forhold til:

Commission Implementing Regulation (EU) 2015/1502 of 8. September 2015
2.3.1. Authentication mechanism

Level substantial, plus: The authentication mechanism implements security controls for the verification of the electronic identification means, so that it is highly unlikely that activities such as guessing, eavesdropping, replay or manipulation of communication by an attacker with high attack potential can subvert the authentication mechanisms.

Kommentar: Bestemmelsen i punkt 8) nedenfor er en skærpelse i forhold til eIDAS Forordningens tekst. Denne bestemmelse findes ikke der. Det ville være gavnligt med eksempler i vejledningen.

NSIS v 2.0:

Høj Punkt 8) ”Hvis flere Autentifikationsfaktorer stammer fra samme enhed, så skal faktorerne være udformet, så kompromittering af én faktor ikke bevirker, at andre faktorer på enheden kompromitteres.”

Svar

Bestemmelsen i NSIS er justeret, således at den er mere i overensstemmelse med eIDAS, og kravet om to faktorer går nu på det samlede Elektroniske Identifikationsmiddel, hvilket vurderes at imødekomme ovennævnte bekymringer.

4. ORGANISATORISKE- OG TVÆRGÅENDE KRAV

Ingen bemærkninger til dette punkt.

4.1.1 Generelle krav

KOMBIT

Side 19

- ”Organisationer, som leverer ID-tjenester, er ansvarlige for opfyldelse af forpligtelser, som er overdraget til tredjepart.” Det bør præciseres, hvad der nærmere forstås ved begrebet "overdraget". Endvidere bør det præciseres, om der, hvis en leverandør af en ID-tjeneste stoler på en ID-tjeneste hos en anden part (fx fordi de indgår i en føderation) – om førstnævnte dermed har overdraget forpligtelser til sidstnævnte, som førstnævnte derfor er ansvarlig for.

Svar:

Der er tale om sidstnævnte – altså overdragelse af forpligtelser til tredjepart.

NSIS medfører ikke forpligtelser for modpartens tjenester ved indgåelse i føderation – se i øvrigt kapitel 6 i NSIS for regulering af føderation. Dette overvejes uddybet i vejledningen.

Nets

4.1.1 Generelle krav

Kommentar: eIDAS forordningen samt anden relevant lovgivning virker meget åben. En præcisering kunne være gavnlig.

Lav 2) ”Organisationer skal for så vidt angår ID-tjenesten til enhver tid kunne dokumentere overholdelse af gældende lov herunder den gældende regulering af databeskyttelse, forvaltningsloven (hvis offentlig myndighed), [eIDAS] forordningen samt anden relevant lovgivning.”

Svar

Der ønskes ikke nogen begrænsning på denne bestemmelse, hvorfor formuleringen bevares, så den inkluderer fremtidige lovgivningsmæssige tiltag.

KOMBIT

Afsnit 4.1.1

- Det foreslås, at begrebet termineringsplan præciseres og uddybes

Svar:

Dette overvejes udbygget i vejledningen.

4.1.2 Oplysningspligt

Ingen bemærkninger til dette punkt.

4.1.3 Informationssikkerhedsledelse

Finans Danmark
<p>Afsnit 4.1.3 indeholder følgende beskrivelse af sikringsniveau ”betydelig” i forbindelse med informationssikkerhedsledelse:</p> <p>”Ledelsessystemet skal være i overensstemmelse med kravene i [ISO 27001] standarden. Der skal foreligge en beredskabsplan, som dækker alle væsentlige områder.” Det er Finans Danmarks opfattelse, at formuleringen ligger meget tæt på krav forsikringsniveau ”høj”, hvorefter ”organisationen skal være certificeret efter [ISO 27001] standarden eller på en tilsvarende måde kunne dokumentere efterlevelsen af krav til informationsledelse.”</p> <p>Finans Danmark efterspørger derfor vejledning om, hvordan kravene til de to sikringsniveauer adskiller sig fra hinanden. Det er vigtig for Finans Danmark, at det kan læses direkte ud af standarden, hvordan kravene adskiller sig fra hinanden. I forlængelse heraf foreslår Finans Danmark, at begrebet ”kravene” erstattes med ”principperne” i beskrivelsen af sikringsniveau ”betydelig”.</p>
<p>Svar:</p> <p>Bemærkningen er imødekommet.</p>

KOMBIT
<p>Afsnit 4.1.3: Informationssikkerhedsledelse: Betydelig 2) Ledelsessystemet skal være i overensstemmelse med kravene i [ISO 27001] standarden. Bør ændres til at Ledelsessystemet skal leve op til kravene i [ISO 27.001] standarden</p>
<p>Svar:</p> <p>Det er præciseret (jf. forrige svar) at det er principperne i ISO 27001, som skal efterleves på niveau Betydelig.</p>

KL
<p>s. 20 afs. informationssikkerhedsledelse</p> <p>Under sikringsniveau "høj" anføres det, at "Organisationen skal være certificeret efter ISO 27.001standarden eller på tilsvarende måde kunne dokumentere efterlevelsen af krav til informationssikkerhedsledelse"</p> <p>KL foreslår tilføjesen "... i henhold til virksomhedens risikovurdering".</p>
<p>Svar:</p> <p>Digitaliseringsstyrelsen mener ikke, at dokumentationen kan være i henhold til virksomhedens risikovurdering, da dette ville efterlade et for stort fortolkningsrum. På niveau Høj skal der foreligge en certificering eller noget, som giver en tilsvarende dokumentation for efterlevelsen.</p>

FR1
<p>Side 20: ”2) Ledelsessystemet skal være i overensstemmelse med kravene i [ISO 27001] standarden.”</p> <p>Skriv: Ledelsessystemet skal være i overensstemmelse med principperne i [ISO 27001] standarden.</p>
<p>Svar:</p> <p>Bemærkningen er imødekommet.</p>

4.1.4 Dokumentation og registerføring

Ingen bemærkninger til dette punkt.

4.1.5 Faciliteter og personale

KOMBIT
<p>Afsnit 4.1.5</p> <ul style="list-style-type: none">- Faciliteter og personale. 1) Der skal findes procedurer, som sikrer, at personale og underleverandører er tilstrækkeligt uddannede, kvalificerede, erfarne og har de færdigheder, der er behov for, når de skal udfylde deres

roller. Teksten bør præciseres og suppleres med eksempler. Fx ved brug af underleverandører skal udbyder af informationstjenester have kontrakt på, at underleverandøren opfylder de samme krav som udbyder har.
Svar: Dette hører til i vejledningen og ikke i standarden. Digitaliseringsstyrelsen vil overveje at opdatere vejledningen.

KOMBIT
Side 21 - ”7) Betroede adgange (herunder administratoradgange) i produktionssystemer skal sikres og overvåges.” Det bør præciseres, hvad der nærmere ligger i ”sikres”.
Svar: Dette hører til i vejledningen og ikke i standarden. Digitaliseringsstyrelsen vil overveje at opdatere vejledningen.

4.1.6 Tekniske kontroller

Ingen bemærkninger til dette punkt.

4.1.7 Anmeldelse og revision

Danske Regioner
I afsnit 4.1.7 angives en række kontroller. Det undrer lidt, at der ikke er nævnt retrospektive kontroller som log-overvågning og lov-audits – evt. stikprøver. Er der en forklaring på det?
Svar: Digitaliseringsstyrelsen går ud fra, at der menes afsnit 4.1.6 om kontroller og ikke afsnit 4.1.7. Formålet med 4.1.6 er ikke at nævne alle kontroller, men blot nogle få udvalgte, idet krav om ISMS og efterlevelse af ISO 27001 eller tilsvarende forventes at give et passende basisniveau af kontroller.

KOMBIT
Afsnit 4.1.7
<ul style="list-style-type: none"> - Anmeldelse og revision: Præciser gerne, om det forventes, at samtlige kommuner skal registrere deres IdPer her.
<p>Svar:</p> <p>Anmeldelse under NSIS er frivilligt, så det er op til den enkelte kommune at afgøre. Digitaliseringsstyrelsen kan dog oplyse, at såfremt man ønsker at føderere en lokal IdP med den kommende NemLog-in3 løsning, så vil en betingelse være, at den lokale IdP er anmeldt under NSIS på et givet sikringsniveau og overholder de tilhørende krav.</p>

5. ELEKTRONISKE IDENTIFIKATIONSMIDLER ASSOCIERET TIL JURIDISKE PERSONER

Ingen bemærkninger til dette punkt.

5.1 UDSTEDELSE AF AKKREDITIVER

Ingen bemærkninger til dette punkt.

5.2 BINDING (ASSOCIERING) MELLEM AKKREDITIVER FOR FYSISKE OG JURIDISKE PERSONER

Lakeside
<p>Ad 5.2) Lakeside havde i høringen til NSIS 1.0 forslået processer for at undgå misbrug fra registrerings-enhedens side:</p> <p><i>Der savnes krav der kan forhindre/ besværliggøre misbrug fra en ondsindet registrerings-enhed/ identity-proofer, som fx udstedelsen af et eID til en fysisk person uden tilknytning til den juridiske person med henblik på at kunne misbruge den fysiske persons rettigheder/fuldmagter. Det foreslås at der på niveau 3 stilles krav om:</i></p> <p><i>a. Dokumentation af registreringsprocessen og 'forbindelsesprocessen' med ekstern revision (og ikke kun i forbindelse med straksudstedelse)</i></p> <p><i>b. Notifikation af den fysiske person ved udstedelse eller 'forbindelse' af et eID (fx. via brev til bopælsadressen eller via besked i e-boks).</i></p> <p>Eksempelvis er truslen i den nuværende NemID infrastruktur meget reel, idet en ondsindet LRA kan udstede en medarbejdersignatur til en person, der slet ikke er ansat i virksomheden, uden at personen bliver bekendt med det.</p>

Derved kan angriberen efterfølgende let misbruge de privilegier, der knytter sig direkte til personen (fx en lægelig autorisation, som er bundet op på personen og ikke på en ansættelse).

Der forslås således igen, at processerne for ”Binding (associering) mellem Akkreditiver for fysiske og juridiske personer” styrkes jf. ovenstående.

Svar:

Det fremgår af punkt 9), at procedurer til grund for etableringen af forbindelsen er underlagt revision.

Der er endvidere tilføjet et nyt krav om, at den fysiske person notificeres ved etablering af en forbindelse.

6. KRAV TIL IDENTITETSBROKERE

Datatilsynet

6. End to end kryptering af security tokens

Datatilsynet har bemærket, at der lægges op til en end to end kryptering af security tokens, når disse indeholder følsomme oplysninger.

Det ses ikke entydigt i beskrivelsen, hvordan ”end to end” defineres, hvilket bør præciseres.

Herudover begrænses anvendelsen til ”følsomme personoplysninger”. Det er tilsynets opfattelse, at det bør overvejes at præcisere anvendelsen af kryptering.

Datatilsynet har tidligere i år tilkendegivet, at det for transmission af data, normalt vil gælde, at de såkaldte ”fortrolige” personoplysninger også skal krypteres under transmission, og at det beror på den konkrete risikovurdering om dette skal ske ”end to end”. Datatilsynet skal på den baggrund henstille til, at der foretages en sådan vurdering.

Svar:

End-to-end kryptering betyder, at token krypteres på applikationslaget og ikke blot beskyttes af transportkryptering som fx TLS. Dette overvejes at blive præciseret i vejledningen til NSIS.

Formuleringen omkring kryptering i NSIS er endvidere udvidet til også at omfatte fortrolige oplysninger.

Finans Danmark
<p>Afsnit 6 indeholder følgende beskrivelse af krav til sikringsniveau ”lav” for Identitetsbrokere (2. krav, 2. pkt.): ”Sikringsniveauet i en token opgøres som mindsteværdien af Sikringsniveauet for Autentifikationen, brokerens eget Sikringsniveau (FAL) samt Sikringsniveauerne for evt. Identitetsbrokere, der er benyttet som underleverandører i den konkrete Autentifikation (dvs. LoA i token er minimum af IAL, AAL og FAL).”</p> <p>Finans Danmark finder ikke, at det at sætte LoA som lig med minimum af IAL, AAL og FAL er egnet til at give udtryk for graden af tillid, der kan have til en autentificering. Det skyldes, at den sikkerhed, der skal være omkring tildeling af akkreditiv til bruger, ikke indgår heri.</p> <p>Såfremt det er tiltænkt, at AAL skal omfatte denne sikkerhed, fremgår dette på nuværende tidspunkt ikke af beskrivelsen af AAL i afsnit 3.3.1 (Autentifikationsmekanismer). AAL er alene defineret ved tabellen i afsnit 3.3.1. Finans Danmark finder på den baggrund, at der er behov for at dette skrives ind afsnit 3.3.1, ligesom justeringerne også bør reflekteres i afsnit 3.2 (udstedelse og håndtering af akkreditiver).</p>
<p>Svar:</p> <p>Begreberne AAL og IAL er præciseret således at fremstår klarere, hvilke krav der hører til i vurderingen af disse.</p>

FR1
<p>Side 26: ”... Sikringsniveauet i et token opgøres som mindsteværdien af Sikringsniveauet for Autentifikationen, brokerens eget Sikringsniveau (FAL) samt Sikringsniveauerne for evt. Identitetsbrokere, der er benyttet som underleverandører i den konkrete Autentifikation (dvs. LoA i token er minimum af IAL, AAL og FAL).”</p> <p>LoA= minimum af IAL, AAL og FAL er ikke egnet til at give udtryk for graden af tillid, der kan have til en autentificering. Dette skyldes at sikkerhed omkring tildeling af autentifikatorer ikke indgår.</p> <p>Man er formentlig nødt til at lade flere tabeller indgå.</p>
<p>Svar:</p> <p>Begreberne AAL og IAL er præciseret således at fremstår klarere, hvilke krav der hører til i vurderingen af disse.</p>

FR1

Side 26: ”... og det skal være muligt for brugeren at logge ud af alle sessioner på én gang (single logout).”

Det anbefales, at dette sidste krav droppes. Det er en større opgave for en central enhed at skulle holde styr på dette og informere de TU'er, hvor bruger har været logget på, ligesom det er en større opgave for hver TU i hver enkelt session ifm hvert enkelt request at undersøge om der evt. skal ske logout (initieret udefra). Det er brugers opgave at logge af. Det kan let gøres ved at lukke device't eller lukke alle browser instanser eller tilsvarende. Ja, det kan bruger glemme, men han kan også glemme at lave single logout. Omkostningerne står slet ikke mål med gevinsten.

Svar:

Kravene om single logout anses som værende relevante ud fra et sikkerhedsmæssigt synspunkt - særligt når brugere deler computere. De bevares derfor.

Single logout er succesfuldt implementeret i NemLog-in-føderationen og er en standardfunktion i bl.a. SAML protokollen, og Digitaliseringsstyrelsen fastholder derfor af sikkerhedsmæssige årsager kravet.

FR1

Side 26: ”8) Anvendere af Identitetsbrokere, der tillader Autentifikation, skal i deres forespørgsel kunne fravælge Single Sign-On, hvis der fra tjenestens side er ønske om at gennemtvinge en aktiv Autentifikation (dvs. fravælge SSO).

Kan formentlig forenkles.

Svar:

Digitaliseringsstyrelsen finder sætningen klar, og den bevares derfor.

FR1

Side 26: ”10) Tokens, som indeholder følsomme personoplysninger eller transporteres via brugerens browser, skal end-to-end krypteres, således at indholdet kun er læsbart for modtageren.

Indsæt ”user agent” i stedet for ”browser”.

Hvad giver det af ekstra sikkerhed at end-end kryptere tokens, der ikke indeholder personfølsomme data? Det giver ikke større sikkerhed mod evt. uautoriseret anvendelse af den pågældende token.

Teksten hænger heller ikke sammen med vejledningen, der kun lægger op til end-end kryptering af personfølsomme data. Krav i vejledningen er endnu blødere, da der kun er krav om kryptering, hvis tokens passerer brugers browser.

Vejledning:

I mange situationer vil security tokens i sig selv ikke indeholde fortrolige eller følsomme oplysninger, og derfor kan ovennævnte mod fortroligheden være acceptabel. Hvis brugers browser er kompromitteret, vil der alligevel være sandsynlig for dataleak, når forretningstjenesten præsenterer data lige efter autentifikationen.

Hvis security tokens omvendt indeholder følsomme oplysninger (herunder følsomme personoplysninger jf. GDPR artikel 9), og der samtidig kommunikerer via brugers browser, stiller NSIS krav til end-to-end kryptering af security tokens, hvilket dækker hele vejen fra Identitetsbroker til forretningstjeneste.

Svar:

Beskrivelsen er justeret, så der i stedet står "Tokens, som indeholder fortrolige eller følsomme personoplysninger, **og** transporteres via brugers browser..."

Begrebet browser vurderes at være mere alment kendt end begrebet "user agent".

End-to-end kryptering giver større sikkerhed for, at oplysninger fra security token ikke kompromitteres - enten på brugers computer eller i yderkanten af den infrastruktur (før/efter TLS terminering) som sender/modtager tokens. Kravet læner sig op af den udbredte 'best-practice' indenfor SAML verdenen, at tokens, som transporteres via browseren, skal krypteres (se fx OIOSAML eller SAML2Int profilerne). Endelig er der i senere år set en del sårbarheder og angreb på transportprotokoller (fx POODLE angrebet), og her giver end-to-end kryptering et ekstra lag af beskyttelse.

Vejledningen bliver opdateret, så den er konsistent med ovennævnte.

FR1

Side 26-27: "... samt ved at forhindre sessionsinformation at blive tilgængelig fra script i browseren"

Må præciseres eller droppes. De scripts, der anvendes i NemID regi har jo adgang til visse former for sessionsinformation. Foreslås droppet.

Svar:

Det var ment som eksempler og i en række implementeringer kan det give god værdi at sikre, at fx sessionscookies ikke kan tilgås fra JavaScript. Beskrivelsen er justeret således, at kravet alene går på, at sessioner skal beskyttes, mens de konkrete beskyttelsesmekanismer kan evt. uddybes vejledningen til NSIS.

Lakeside

Vedrørende Krav 6 til Identitetsbrokere:

- a. Ad 8) Som det nu er beskrevet under dette punkt, dækker 'Fravalg af SSO' over at tjenesten skal kunne fremtvinge en autentifikation og ikke om et egentligt fravalg af SSO (som ville indebære, at der ikke oprettes en SSO-session i brokeren). Rigtig 'fravalg af SSO' er en egenskab, der er ønskeligt i en række sammenhæng (herunder især i forbindelse med udvikling af mobile app's hvor man vil undgå 'hængende' SSO sessioner i systembrowseren). Lakeside forslår, at punktet udvides til at dække 'rigtig' fravalg af SSO, hvor tjenester kan fravælge, at der oprettes og/eller anvendes eksisterende SSO-sessioner i brokerne.
- b. I forlængelse af ovenstående forslås formuleringen i 5) og 6) til generelt at gælde sessioner med brokere og ikke kun SSO-sessioner.
- c. Ad 5) og den tilhørende supplerende tekst fra NSIS vejledningen: Der savnes en begrebsafgrænsning for sessioner for forskellige anvendelsesscenarier. Eksempelvis er der stor forskel mellem hvordan browser-sessioner (som kunne foregå fra en offentlig PC på et bibliotek), en app-session på en borgers private mobil eller en fagsystems-session i service-integrationer på lukkede netværk benyttes og bør sikres. I gængse app-autentifikationsmønstre (baseret på OpenID Connect/OAuth2 standarden) opereres eksempelvis typisk med en initial brugerautentifikation og efterfølgende med meget langt levende sessioner, der bliver 'genoptaget'. Det kunne være hensigtsmæssigt at lade NSIS indeholde krav til, hvordan apps/tjenester kan håndtere genoptagelse af (langt levende) sessioner og stadig leve op til NSIS.
- d. Ad 15) Det er lidt uklart hvad der menes med at nøglen ikke må eksporteres 'i klar tekst.' Er hensigten ikke, at nøglen slet ikke skal kunne eksporteres?

Svar:

Ad 8) Digitaliseringsstyrelsen anerkender, at dette kan være et behov i visse konkrete implementeringer, men finder ikke det nødvendigvis skal være et krav, som skal påtvinges *alle* implementeringer. Det er således frit at implementere ekstra funktioner ud over de af NSIS kravstillede.

Ad 5) og 6) Formuleringen omkring sessioner er generaliseret i NSIS.

I forhold til Apps vil Digitaliseringsstyrelsen overveje at opdatere vejledningen, såfremt der kan identificeres best practice på området.

Ad 15) I miljøer med behov for høj opetid er der ofte behov for at klonе/eksportere nøgler fra en HSM til en anden, således at single point of failures undgås. Dette kan gøres på en sikker måde efter veldefinerede procedurer, hvor nøglen overføres i en krypteret form uden risiko for kompromittering.

KOMBIT

Kapitel 6, punkt 10 i skema

- det foreslås, at ”følsomme personoplysninger” ændres til ”almindelige fortrolige personoplysninger og følsomme personoplysninger”

Svar:

Formuleringen er justeret jf. også kommentarer fra Datatilsynet.

KOMBIT

Side 27

- ”15) Den private nøgle skal genereres i hardware og må ikke kunne eksporteres i klar tekst.” Præciser gerne, om ikke dette er en logisk følge af krav 14).

Svar:

Dette er ikke en logisk følge af krav 14) - i nogle kryptoenheder kan nøgler fx genereres uden for hardwaren og herefter importeres, hvilket ikke er tilladt jf. krav 15.

KOMBIT

Side 27

- ”Tjenester som udsteder Akkreditiver til private borgere eller personer associeret til vilkårlige virksomheder. En broker som kun håndterer en/få virksomheders eller myndigheders egne lokale brugere anses ikke som national, og derfor gælder kravet ikke for disse”. Præciser gerne definitionen på nationale tjenester. Der er et spænd mellem de tjenester,

der defineres som værende henholdsvis ikke-værende nationale tjenester. Det er fx uklart, om 98 kommuner er at betragte som "få" myndigheder.
Svar: Definitionen vedrører bred, national anvendelse i modsætning til situationen med lukkede systemer, eller når der på forhånd er indgået aftaler mellem et defineret sæt af deltagere i en føderation. Digitaliseringsstyrelsen vurderer dog, at en identitetsbroker, som har alle kommuner tilsluttet, har karakter af en national tjeneste og derfor bør leve op til kravene for disse.

Nets
Kommentar: Bør ordet "kryptografisk" indgå i sætningen? Det indgår ikke i krav 13. HSM bør skrives ud. Høj 14) "Brokerens private nøgle, der underskriver security tokens, placeres i "tamper-resistant" kryptografisk hardware (HSM), der opfylder kravene til [FIPS 140-2] level 3 eller tilsvarende.
Svar: Bemærkningen er indarbejdet.

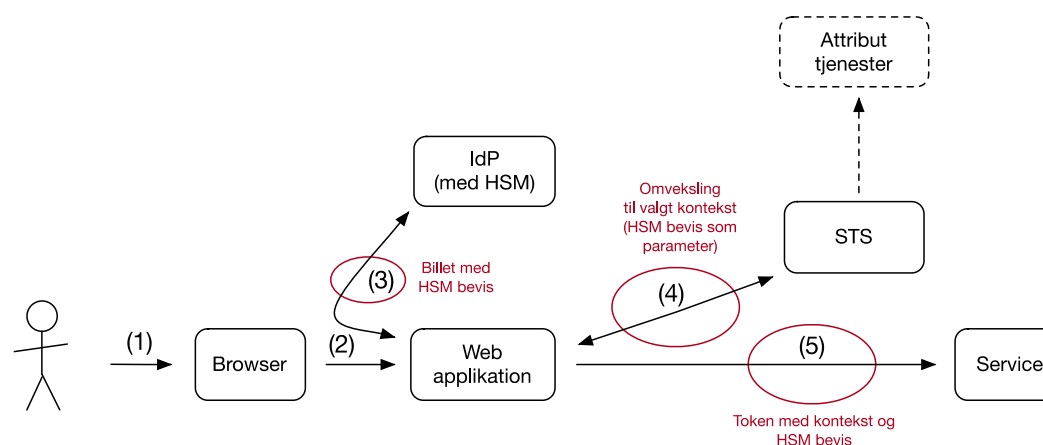
Sundhedsdatastyrelsen
NSIS stiller for niveau 3 og 4 eksplicitte krav til brokere (IdP'er og STS'er) ¹ , der viderefører en brugerauthentifikation, om at tokensigneringsnøglen skal placeres i tamper-resistant hardware (HSM). I sundhedsvæsnets målarkitektur for identitetsbaserede service-integrationer står (STS)-brokere ikke alene for videreformidling af brugerauthentifikation, men i høj grad også for videreformidling og verifikation af en mere volatil kontekst, som fx aktuel brugerrolle, valgt patient (og afledte relationer), anvendt rettighedsdelegering mm. I målarkituren er en lang række valideringer og registeropslag, som service-udbydere i dag selv varetager, således flyttet til brokerinfrastrukturen, hvilket mindsker byrden for service-udbydere, men medfører meget hyppige token omvekslinger i brokerne. For at kunne håndtere de mange token-omvekslinger, stræbes der efter at kunne

¹ Krav 13 til 15 i kapitel 6.

realisere STS omvekslinger decentralt (fx ude i regionerne) i flere parallelle STS instanser – og her er HSM baserede løsninger både dyre og skalerer dårligt.

Som alternativt til den direkte anvendelse af HSM, og eksplicit opfyldelse af NSIS kravet, overvejer sundhedsvæsenet at anvende en model, der i stedet baserer sig på HSM-baserede autentifikationsbeviser. Autentifikation- og omvekslingsfunktionalitet i brokerne adskilles, således at tokens som udstedes i forbindelse med autentifikation altid signeres med en HSM baseret nøgle. Tokens der fremkommer under efterfølgende omvekslinger kan derimod signeres med softwarebaserede nøgler. Dog under den forudsætning, at der videreføres et HSM-signeret autentifikationsbevis², der skal valideres af service-udbyderne. En kompromitteret softwarebaseret nøgle vil således ikke alene kunne benyttes til at udstede valide tokens, idet de da vil mangle det HSM-signerede autentifikationsbevis.

Modellen med videreførelse af et HSM-baseret autentifikationsbevis er i nedenstående figur illustreret for et webscenarie med autentifikationen hos en IdP (med HSM) og omveksling til et token med valgt kontekst hos en STS.



Som vi ser det, har modellen med HSM-baserede autentifikationsbeviser de samme sikkerhedsegenskaber som HSM-signerede tokens og vi foreslår derfor, at NSIS formuleringerne omkring HSM kravene blødes op (eventuel kun i NSIS vejledningen), så ækvivalente tekniske mekanismer tillades.

Svar:

Digitaliseringsstyrelsen finder, at NSIS kravene til HSM vedr. Identitetsbrokerne

² Fx tokenet der fremkom under autentifikationen eller et separat indlejret HSM-signeret bevis der udstedes i forbindelse med autentifikationen.

netop går på 'autentifikationsbeviser', og at NSIS ikke regulerer hvorvidt tokens med andre typer attributter indeholdende fx autorisationer skal signeres med en nøgle i kryptografisk hardware. Dermed forekommer der ikke umiddelbart at være konflikt mellem NSIS-kravene og det beskrevne scenarie.

Sundhedsdatastyrelsen

NSIS krav vedrørende end-to-end tokenkryptering

Under profilering af den fællesoffentlige OIO IDWS standard til sundhedsområdet som en del af 'initiativ 7.2: Fælles standarder for sikker udveksling af information' er vi stødt på en udfordring i forhold til at kunne overholde NSIS 1.0 krav nummer 10 til Identitetsbrokere: *Tokens skal end-to-end krypteres, således at indholdet kun er læsbart for modtageren.*

I udkastet til NSIS 2.0 er kravet blevet blødt op til '*Tokens, som indeholder følsomme personoplysninger eller transporteres via brugerens browser, skal end-to-end krypteres, således at indholdet kun er læsbart for modtageren.*' – men dette ændrer ikke på udfordringen.

Problemstillingen ligger i at, der under udarbejdelsen af sundhedsvæsnets IDWS webservice profil og den tilhørende værktøjsunderstøttelse har vist sig, at de internationale webservice standarder, som profilen baserer sig på, ikke definerer en model for *end-to-end* kryptering af adgangsbilletter. Ligeledes kan der med standard rammeværk³ ikke realiseres end-to-end kryptering uden at skulle foretage proprietære tilpasninger i rammeværkerne, hvilket i praksis ofte teknisk ikke kan lade sig gøre, idet rammeværkerne typisk er en fast del af driftsleverandørernes driftsplatform. Den praktiske model som benyttes til end-to-end tokenkryptering i NemLog-in STS er således ikke helt i tråd med internationale specifikationer og er blevet tilvejebragt i gennem proprietære tilpasninger af standard rammeværk (Digitaliseringsstyrelsen er allerede blevet informeret om problemstillingen).

Som kompenserende foranstaltning har profileringsprojektet opstillet en model til end-to-end kryptering af relevante del-elementer i billetten, således at personfølsomme oplysninger kan beskyttes imod uautoriseret aflæsning. Derved opnås det samme mål som NSIS sigter efter, men med en lidt anden teknisk tilgang. Samtidigt er modellen holdt indenfor internationale specifikationer, således at standard rammeværk som realiserer standarderne kan anvendes

³ Under 'standard rammeværk' forstås standard kode-biblioteker (ofte open source) som tilbyder standard funktionalitet. Konkret drejer der sig her om biblioteker, der implementer de internationale standarder SAML, WS-Security og WS-SecurityPolicy.

uforandret.

Der foreslås derfor at lade krav 10 til Identitetsbrokere fokusere på formålet (end-to-end beskyttelse af personoplysninger) og til at tillade forskellige tekniske mekanismer til at realisere kravet (som fx kryptering af følsomme del-elementer).

Svar:

Forslaget er imødekommet ved at åbne for kryptering af attributter.

7. GOVERNANCE

Ingen bemærkninger til dette punkt.

7.1 EJERSKAB OG VEDLIGEHOLDELSE AF STANDARDEN

Ingen bemærkninger til dette punkt.

7.2 OPHØR OG FRATAGELSE

Ingen bemærkninger til dette punkt.

7.3 ANSVAR OG FORSIKRING

FR1

Side 28: ” at oplysninger i udstedte Akkreditiver eller Security Tokens er forkerte på tidspunktet for udstedelsen eller manglende spærring på baggrund af gyldig anmodning.”

Skriv: forkerte pga procedurefejl nos anmelder eller broker.

Eller omvendt: anmelder /broker er ikke ansvarlig for fejl, som deres korrekt udførte procedurer ikke kan opdage.

Svar:

Digitaliseringsstyrelsen henleder opmærksomheden på, at der under bestemmelse står, "medmindre det kan godtgøres, at der ikke er handlet uagtsomt eller forsætligt.", hvilket vurderes at dække den omtalte situation.

KOMBIT
Side 28
<ul style="list-style-type: none">- ”at oplysninger i udstedte Akkreditiver eller Security Tokens er forkerte på tidspunktet for udstedelsen eller manglende spærring på baggrund af gyldig anmodning”. Det foreslås, at det præciseres, hvilken part der har ansvaret hvis en tjeneste forlader sig på et akkreditiv hos en anden part med forkerte oplysninger
Svar: Det fremgår af NSIS, at den part som udsteder et Elektronisk Identifikationsmiddel med forkerte oplysninger, kan ifalde ansvar over for den part, som forlader sig på dette.

7.4 OMKOSTNINGER

Ingen bemærkninger til dette punkt.

7.5 DELING AF SIKKERHEDSHÆNDELSER

Ingen bemærkninger til dette punkt.

8. REFERENCER

Datatilsynet
4. Henvisning til ISO 15408 Datatilsynet kan konstatere, at der i udkast til NSIS version 2.0, pkt. 8, er indsat en reference til ISO 15408. Datatilsynet foreslår, at det anføres, hvilken version der er tale om. Datatilsynet antager, at der er tale om ISO 15408-1:2009. Datatilsynet bemærker endvidere, at brugen af gradinddelingen af begrebet ”angrebsskapacitet” ikke synes overensstemmende med benyttelsen i selve ISO 15408.
Svar: Referencen er præciseret til ISO 15408-1:2009. Formuleringerne vedr. Angrebsskapacitet er direkte taget fra eIDAS, og Digitaliseringsstyrelsen kan ikke umiddelbart finde uoverensstemmelser med

standarden.

Datatilsynet

5. Henvisning til persondataloven

Datatilsynet kan konstatere, at der i udkast til NSIS version 2.0, pkt. 8, er indsat en reference til den dagældende persondatalov. Datatilsynet bemærker i den forbindelse, at persondataloven er ophævet pr. 25 maj 2018. Det bør derfor overvejes, om henvisningen bør udgå – navnlig da der ikke ses at være henvist til persondataloven andre steder i dokumenterne.

Svar:

Referencen er opdateret.

9. HØRTE PARTER

Nedenstående liste er en oversigt over de parter der har indsendt høringssvar med generelle og/eller tekstnære kommentarer.

Danske Regioner

Region Midt

Datatilsynet

Erhvervsstyrelsen

Finans Danmark

FR1

KL

KOMBIT

Lakeside

Nets

Skatteforvaltningen

Sundhedsdatastyrelsen

Viborg Kommune

Nedenstående har svaret, at der ingen kommentarer er til høringen:

Konkurrence- og Forbrugerstyrelsen