

Høringsnotat

15. december 2016

Behandling af indkomne høringssvar i forbindelse med den officielle høring af National Standard for Identiteters Sikringsniveau (NSIS) version 0.97

Høringsparternes besvarelser er i dette høringsnotat 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 ikke medtaget, men opsummeres i nedenstående korte afsnit:

Der er generelt blevet taget godt imod NSIS. Det fremgår af størstedelen af høringssvarene, at NSIS har en berettigelse, og at der generelt er fokus på, at tillid til identiteter er essentielt i et digitaliseret samfund som det danske. Flere har efterspurgt en national standard for identiteters sikringsniveau, hvor kravene er knap så åbne for fortolkning og henviser fx til NIST. Digitaliseringsstyrelsen har dog fastholdt den mere åbne beskrivelse, der i større grad tilgodeser innovation og ikke mindst er teknologineutral. Digitaliseringsstyrelsen udgiver en vejledning til NSIS i januar 2017.

Endvidere er der udtrykt ønsker til en mere 1:1-kravsætning i forhold til den refererede implementerende retsakt 2015/1502. Digitaliseringsstyrelsen har som udgangspunkt taget afsæt i disse krav, men har i flere tilfælde enten skærpet kravene i NSIS eller specificeret kravene tilpasset danske forhold. Det skal i øvrigt bemærkes, at det alene er medlemslande, der kan anmelde en eller flere eID ordninger jf. kravene i eIDAS-forordningens artikel 8.

God læselyst.

Indhold

1.1 Forord.....	4
1.2 Introduktion.....	4
1.3 Formål og scope	4
1.4 Eksempler på Identitetstjenester og niveauer.....	5
1.5 Terminologi	5
2. LIVSCYKLUS FOR EID'ER.....	6
3. NORMATIVE KRAV	7
3.1 REGISTRERINGSPROCESSEN	7
3.1.1 Ansøgning	7
3.1.2 Verifikation af identiteter.....	7
3.2 UDSTEDELSE OG HÅNDTERING AF EID.....	13
3.2.1 Styrke af eID	13
3.2.2 Levering og aktivering.....	17
3.2.3 Suspendering, spærring og genaktivering	18
3.2.4 Fornyelse og udskiftning	20
3.3 ANVENDELSE OG AUTENTIFIKATION.....	22
3.3.1 Autentifikationsmekanismer	22
3.4 ORGANISATORISKE- OG TVÆRGÅENDE KRAV	24
3.4.1 Generelle krav	24
3.4.2 Oplysningspligt	25
3.4.3 Informationssikkerhedsledelse	26
3.4.4 Dokumentation og registerføring.....	26
3.4.5 Faciliteter og personale	26

3.4.6 Tekniske kontroller	28
3.4.7 Anmeldelse og revision.....	29
4. ELEKTRONISKE IDENTIFIKATIONSMIDLER ASSOCIERET TIL JURIDISKE PERSONER	32
4.1 UDSTEDELSE AF ELEKTRONISKE IDENTIFIKATIONSMIDLER.....	32
4.2 BINDING (ASSOCIERING) MELLEM ELEKTRONISKE IDENTIFIKATIONSMIDLER FOR FYSISKE OG JURIDISKE PERSONER	35
5. KRAV TIL BROKERLØSNINGER	37
6. GOVERNANCE.....	43
6.1 EJERSKAB OG VEDLIGEHOLDELSE AF STANDARDEN.....	43
6.2 OPHØR OG FRATAGELSE.....	43
6.3 ANSVAR OG FORSIKRING.....	43
6.4 OMKOSTNINGER	44
6.5 DELING AF SIKKERHEDSHÆNDELSER.....	44
7. REFERENCER.....	45
8. HØRTE PARTER.....	46

1.1 Forord

Ingen bemærkninger til dette punkt.

1.2 Introduktion

Ingen bemærkninger til dette punkt.

1.3 Formål og scope

Datatilsynet

Kommentar:

”For offentlige myndigheder vil afdækning af risikoniveau ofte ligge i naturlig forlængelse af forpligtelserne, som dataansvarlig i henhold til den gældende regulering af personoplysning og sikkerhedsbekendtgørelsen udstedt i medfør heraf. Datatilsynet fører tilsyn med overholdelse af den gældende regulering af personoplysninger.”

Datatilsynet bemærker i den forbindelse, at det ikke kun er offentlige myndigheder, som har forpligtelser i henhold til den til enhver tid gældende databeskyttelseslovgivning.

Desuden bør det overvejes, om det er hensigtsmæssigt med en direkte henvisning til sikkerhedsbekendtgørelsen idet den kommende databeskyttelsesforordning finder anvendelse fra den 25. maj 2018.

På den baggrund foreslår Datatilsynet, at afsnittet i stedet for får følgende formulering:

”For virksomheder mv. og myndigheder, som behandler personoplysninger, vil afdækning af risikoniveau ofte ligge i naturlig forlængelse af forpligtelserne i henhold til den til enhver tid gældende regulering af behandling af personoplysninger.”

Svar:

Forslaget er indarbejdet i standarden.

Sundhedsdatastyrelsen

Kommentar:

Den gennemførelsesretsakt, som definerer niveauerne under eIDAS-forordningen. Det kunne være nyttigt med en litteraturreference til denne.

Svar:

Forslaget er indarbejdet i standarden.

1.4 Eksempler på Identitetstjenester og niveauer

Datatilsynet

Kommentar:

”I dag har vi med NemID og OCES-standard en fastlagt sikringsniveau (som modsvarer niveau 3).”

Datatilsynet må umiddelbart stille spørgsmålstegn ved, om den eksisterende NemID løsning generelt kan siges at opfylde NSIS-niveauet 3/”Betydelig”.

Tilsynet bemærker i den forbindelse, at Digitaliseringsstyrelsen selv (på side 5 i høringsbrevet) har anført, at vurderingen kan afhænge af den konkrete implementering, og har omtalt et eksempel på en NemID-løsning, som kun kan kategoriseres på niveau 2 i NSIS.

Datatilsynet skal foreslå, at formuleringen ”som modsvarer niveau 3” fjernes eller blødes op.

Svar:

Forslaget er indarbejdet i standarden, og teksten indeholder nu ikke længere angivelse af kobling til et sikringsniveau.

1.5 Terminologi

Peercraft

Kommentar:

Betegnelsen ”angrebspotentiale” bør medtages under kapitel 1.5 (”Terminologi”) med reference til ISO/IEC 18045 samt konteksten jf. ISO 29115, som derfor også bør medtages som referencer under kap. 7. Betegnelsen bør anvendes konsekvent (pt. anvendes ”angrebspotentiale” i kap. 3.2.1, mens der i kap. 3.3.1 (niv. 2-4) anvendes ”angrebsskapacitet”).

Svar:

Forslaget er indarbejdet i standardens tekst.

NETS

Kommentar:

Definition af identifikation stemmer ikke med EU 910/2014 forordningens definition. Definitionen bør specificeres i overensstemmelse med EU

forordningens definition.

eID er ikke defineret i terminologilisten. Det vil være befordrende for at undgå misforståelser, hvis denne definition medtages. Tilføj definition af eID.

Elektronisk identifikationsmiddel er ikke helt konsistent med definitionen eIDAS (EU) 910/2014 der præciserer at et identifikationsmiddel indeholder personidentifikationsdata. Det bør afklares om ikke der skal være konsistens mellem eIDAS og NSIS på dette punkt.

Definition af Personidentifikationsdata mangler i NSIS. Definition bør medtages, for at undgå misforståelser i fortolkningen heraf.

Definitionen af Sikringsniveau indeholder ikke registreringsprocessen, men kun udstedelse og anvendelse af identifikationsmidler. Inkluder registreringsprocessen i definitionen.

Definitionen på dynamisk autentifikation er uklar og ikke konsistent brugt i NSIS standarden.

Svar:

Forslagene er indarbejdet i standardens tekst.

2. LIVSCYKLUS FOR EID'ER

NETS

Kommentar:

Der er uoverensstemmelse mellem figur 1 og de efterfølgende processer specificeret i afsnit 3. Figur 1 bør understøtte de efterfølgende afsnit, således at en kasse på figuren beskrives i et afsnit. Som standarden er nu, er det kun tilfældet for registrering (på figur 1) og afsnit 3.1.

Nederst på side 8 mangler både aktivering og suspension (midlertidig spærring) at blive nævnt. Disse områder bør tilføjes.

Figuren benytter begreber, som ikke er konsistent med resten af dokumentet. Figuren bør tilpasses begreberne i standarden eller medtages i et vejledningsdokument.

Figuren tjener ikke noget specielt formål i standarden. Figuren bør slettes/ flyttes til vejledning.

Svar:

Forslagene er indarbejdet i standardens tekst. Figur 2 udgår fra standarden og flyttes til vejledningen.

3. NORMATIVE KRAV

Sundhedsdatastyrelsen

Kommentar:

Anvendelse af begreber som ”overvejende sandsynlighed” og ”højest usandsynligt” åbner mulighed for fortolkning. Disse krav bør præciseres, gerne med udgangspunkt i NIST Electronic Authentication Guideline.

Svar:

Forslaget er ikke indarbejdet i standardens tekst. Standarden ønskes teknologineutral og resultatbaseret, hvilket betyder, at der stilles krav til udfaldet, men den tillader, at disse kan indfries på flere måder.

3.1 REGISTRERINGSPROCESSEN

Ingen bemærkninger til dette punkt.

3.1.1 Ansøgning

Ingen bemærkninger til dette punkt.

3.1.2 Verifikation af identiteter

Datatilsynet

Kommentar:

Sammenligning af NSIS punkt 3.1.2 (Verifikation af identitet (fysiske personer)), niveauet 3/”Betydelig” med eIDAS-gennemførelsesforordningens punkt 2.1.2. (Godtgørelse og kontrol af identitet (fysiske personer)), niveauet ”Betydelig”:

NSIS:

”Der bør være kontroller, som med langt overvejende sandsynlighed forhindrer anvendelse af stjålne eller tabte dokumenter tilhørende andre personer”

eIDAS:

”der er taget skridt til at nedbringe risikoen for, at den pågældende persons identitet ikke er den, den påstås at være, under hensyntagen til risikoen for at beviset kan være blevet tabt, stjålet, suspenderet, tilbagekaldt eller være udløbet.”

Forskellene fremstår her dels som åbenlyse forskelle mellem de anvendte formuleringer dels i, at teksten i NSIS er formuleret som en anbefaling (bør),

mens den i eIDAS er formuleret som et krav. Beskrivelsen i eIDAS er desuden mere omfattende i forhold til, hvad kontrollerne skal beskytte imod. Datatilsynet skal for god ordens skyld understrege, at tilsynet IKKE med dette høringssvar har foretaget en vurdering af, om en løsning, der lever op til NSIS, også vil kunne anerkendes på det tilsvarende niveau under eIDAS. De konstaterede forskelle giver imidlertid Datatilsynet anledning til at tvivle på, om der reelt kan siges at være den sammenhæng, som beskrives i standardens afsnit 1.2.

Svar:

Forslaget om tilføjelse af ”suspenderet” og ”tilbagekaldt” er tilføjet til standardens tekst.

IDA

Kommentar:

Det er vigtigt, at NSIS formår både at sikre et højt sikkerhedsniveau og samtidig kunne favne nye digitale muligheder, der vil gøre det lettere og dermed mere attraktivt at benytte de digitale muligheder. Digitaliseringsstyrelsen opfordres derfor til at genoverveje kravet under pkt. 3.1.2, sikringsniveau 4, om at personligt fremmøde er en forudsætning, da der i dag er teknologier, som vil kunne være en brugbar erstatning for personligt fremmøde, der af mange vil opfattes som tids- og ressourcekrævende.

Her tænkes bl.a. på forskellige biometriske muligheder som fingeraftryk eller irisscanninger.

Standarden bør give mulighed for, at disse teknologier vil kunne benyttes efterhånden, som de vinder udbredelse. Der kunne derfor med fordel være en definition af, hvad der forstås ved ”fysisk match mellem ansøgeren og den præsenterede dokumentation”, som nye digitale muligheder kunne måles op imod.

Svar:

Forslaget er indarbejdet i standardens tekst således, at der nu er formuleret i kravet om personligt fremmøde, at en ækvivalent mekanisme med samme sikkerhedsniveau også tillades.

Signaturgruppen

Kommentar:

Det ser ud til at NSIS bestemmelserne er forsimplet voldsomt i forhold til bestemmelserne i LoA Guidance, særligt for niveau højt, hvor der grundlæggende udpeges fysisk fremmøde i NSIS imens LoA Guidance rummer flere nuancer.

Det bør vurderes om NSIS skal følge LoA tættere på dette område.

Desuden kan det vurderes, om kravet om fysisk fremmøde bør præciseres i forhold til hvilke kvalifikationer de personer man møder frem hos skal besidde, og hvilke kontroller og revisioner registreringen omfattes af.

For eID associeret til juridiske personer kan det f.eks. overvejes, om lokale medarbejdere kan udføre fysisk identifikation og under hvilke vilkår.

Svar:

NSIS er skrevet til danske forhold, hvor der bl.a. er stor tillid til de nationale autoritative registre. LoA og LoA guidance skal rumme alle medlemslandenes nuancer og er derfor formuleret herefter. Den danske pendant til LoA guidance, vejledningen til national standard for identiteters sikringsniveauer udgives i januar 2017.

I forhold forslaget om beskrivelse af krav til personalet, der skal håndtere personligt fremmøde og verifikation af dokumenter, er der tilføjet krav om uddannelse til standardens tekst.

I forhold til forslaget om eID associeret til juridiske personer, og overvejelse om hvorvidt lokale medarbejdere kan udføre fysisk identifikation mv., behandles dette i vejledningen til standarden.

Sundhedsdatastyrelsen

Kommentar:

"Ansøgeren vurderes med overvejende sandsynlighed at være i besiddelse af almindeligt anerkendt dokumentation for sin identitet. Dette kan være sygesikringskort, pas, kørekort, dåbsattest, forskudsopgørelse eller elektronisk ID". Begrebet "overvejende sandsynlighed" åbner mulighed for fortolkning og bør konkretiseres.

5) Der bør være kontroller, som med langt overvejende sandsynlighed forhindrer anvendelse af stjålne eller tabte dokumenter tilhørende andre personer. Begrebet "overvejende sandsynlighed" åbner mulighed for fortolkning og bør konkretiseres.

7) Ansøgeren skal besidde viden, som kun forventes at være kendt af en legitim ansøger (kontrolspørgsmål). Eksempler på sådanne kontrolspørgsmål kunne give en bedre forståelse af kravet.

Svar:

Forslagene er ikke indarbejdet i standardens tekst, men behandles i vejledningen til standarden, der udgives i januar 2017.

Danske Regioner

Kommentar:

Det kan blive en udfordring for myndigheder, der ønsker at indrullere udenlandske medarbejdere, at myndighederne skal kunne verificere andre landes registre eller udstedte pas eller lignende. Der bør søges fælles/nationale løsninger for dette, fx ved at have specielt uddannede enheder (i udvalgte kommuner eller i hver region) der kan varetage denne verifikation. Bemærk, at regionerne ansætter sundhedspersoner fra en lang række lande, også medarbejdere, der ikke kommer fra EU medlemsstater.

Svar:

Regeringen har i den seneste finanslovsaftale for 2017 besluttet, at der skal etableres en national ID-enhed, som skal fungere som et centralt ekspertorgan, der blandt andet kan rådgive andre myndigheder og sikre udveksling af erfaringer blandt relevante myndigheder.

ATP

Kommentar:

ATP ønsker en mere ensartet proces i forbindelse med udstedelse af CPR-nr. for personer født i udlandet. Der ønskes registreringer af identifikationsdata, således at fx CPR, Udlændingestyrelsen registrerer de alternative ID, der er anvendt i identitetsprocessen. De alternative ID skal registreres og videreformidles, når andre myndigheder skal have data på personen.

En tilsvarende proces bør også tilvejebringes for udenlandske virksomheder.

Svar

Dette forslag vurderes at ligge uden for rammerne af standarden, og er ikke indarbejdet. Der henvises til digitaliseringsstrategiens initiativ 7.3 Digitale identiteter og rettighedsstyring, hvor en arbejdsgruppe arbejder med valide identiteter, herunder drøftelser om såkaldte administrative personnumre uden bopælsregistrering.

Peercraft

Kommentar:

I tabellen under kapitel 3.1.2 er der som punkt 6 angivet: Ansøgeren eksisterer i autoritative registre (fx CPR) og er ikke død.

Det bør overvejes at udvide dette krav med “eller forsvundet” (d.v.s. CPR status kode 70) da CPR ellers mister sin autoritative status og den forsvundne person – eller en anden, der har overtaget vedkommendes identitet eventuelt vil kunne angive forskellige adresser til forskellige eIDtjenesteudbydere.

Alternativt foreslås det at Digitaliseringsstyrelsen sammen med andre relevante myndigheder udarbejder en separat vejledning for eID håndtering af personer som er forsvundne (status kode 70), uden bopæl (status kode 20) eller registreret med “høj vejkode” (status kode 03), således at almindeligt hjemløse personer tilgodeses bedst muligt.

Svar:

Dette forslag er delvist indarbejdet i standardens tekst. ”Forsvundet” er indarbejdet i kravet. Den nederste del af forslaget om håndtering af statuskoder for personer, der er forsvundne, uden bopæl eller hjemløse mv., behandles i vejledningen til standarden.

KL/KOMBIT

Kommentar:

Punkt 7 (kontrolspørgsmål) bliver lidt tricky at implementere i kommunen (tænker det typisk er ved ansættelsestidspunktet at det bliver registreret). Det man skal overveje er hvordan man håndtere allerede oprettede brugere, så de ikke skal re-enrolles

Svar:

Som med forslagene om bindingen mellem naturlige personer og juridiske behandles dette i vejledningen til standarden.

NETS

Kommentar:

Punkt 2) og 3) under ”2. Lav” kunne med fordel slås sammen til et punkt ”Det er verificeret, at ansøgeren er i besiddelse af ægte og gyldig almindeligt anerkendt dokumentation for sin identitet. Det kan være...”

Svar:

Forslaget indarbejdes ikke i standardens tekst. Digitaliseringsstyrelsen vurderer, at punkt 2 og 3 holdes adskilt.

Under sikringsniveau betydelig listes, at det skal valideres at ”ansøgeren eksisterer i autoritative registre og ikke er død.” Men hvad med hvis brugeren er umyndiggjort? Overvej tilføjelse om umyndiggjorte.

Svar:

Forslaget er indarbejdet i standardens tekst, der nu rummer en tilføjelse vedrørende umyndiggjorte.

Der anvendes i ”3. Betydelig” (og andre steder) betegnelsen ”anerkendt”. DIGST bør specificere, hvem denne anerkendelse skal være foretaget af. Eksempler på disse ønskes.

Svar:

Forslaget behandles i vejledningen til standarden.

Der anvendes i ”3. Betydelig” betegnelsen ”autoritative registre”. DIGST bør specificere, hvem der fastlægger om et register er autoritativt. Eksempler på disse ønskes.

Svar:

Forslaget behandles i vejledningen til standarden.

Det fremgår, at ”Ansøgeren skal besidde viden, som kun forventes at være kendt af en legitim ansøger (kontrolspørgsmål)”, men denne betingelse vil aldrig være strengt opfyldt, eftersom denne viden også må være tilgængelig for dem, som skal kontrollere viden. I stedet for ”Som kun forventes at være kendt” kunne man med fordel anvende formuleringen ”Som ikke forventes alment kendt”.

Svar:

Forslaget er indarbejdet i standardens tekst.

Det fremgår, at ”Hvor ansøgeren ikke er besiddelse af dette, kan de samme identifikationsprocesser som benyttes ved udstedelse af pas og kørekort anvendes.” Er disse processer standardiseret på tværs af EU? Hvis ikke, vil det så være processerne i det land, hvor ansøger er statsborger, som skal anvendes?

Svar:

Processerne er ikke standardiseret på tværs af EU. Standarden henviser til/beskriver de processer, der er gældende i Danmark for udstedelse af pas eller kørekort.

Det fremgår, at ”Generelt er det tilladt at basere identifikation på autentifikation med et gyldigt eID på mindst samme sikringsniveau, såfremt de nødvendige oplysninger tilvejebringes gennem denne autentifikation.” Hvad menes med ”nødvendige oplysninger”?

Svar:

Her menes personidentifikationsdata.

Det fremgår, at ”Niveau 3 kan også opnås gennem elektronisk ansøgning over internettet, hvilket dog vil stille særlige krav til muligheden for verifikation i offentlige registre.” 1) Er dette krav udover dem, som fremgår af tabellen? – hvis ja, hvad er disse krav?, 2) Her benyttes betegnelsen ”offentlige”, men i tabellen ”autoritative” – hvad er forskellen/definitionen? Præciseringer ønskes.

Svar:

Her menes autoritative registre. Afsnittet er efterfølgende flyttet til vejledningen til standarden.

Ansøgeren skal besidde viden som kun forventes at være kendt af en legitim ansøger (kontrolspørgsmål). Dette krav findes ikke i eIDAS gennemførelsesforordning (EU) 2015/1502. Kan det være i strid med EU regler?

Svar:

Det er tilladt at stille større krav end forordningens. I Danmark har det vist sig nødvendigt at stille disse kontrolspørgsmål.

3.2 UDSTEDELSE OG HÅNDTERING AF EID

Ingen bemærkninger til dette punkt.

3.2.1 Styrke af eID

Signaturgruppen

Kommentar:

For niveau lav har NSIS disse bestemmelser:

- 2) Det elektroniske identifikationsmiddel er designet, så det er personligt (delte kodeord ikke tilladt).
- 3) Udstederen tager rimelige skridt til at kontrollere, at det kun er den person, som det tilhører, der har kontrol over og er i besiddelse af det.”

De tilsvarende bestemmelser i LoA Guidance er lidt anderledes formuleret: ”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.”

Det bør vurderes, om NSIS bør følge LoA Guidance formuleringen tættere, f.eks. med en formulering som ” Udstederen tager rimelige skridt for at kontrollere, at det kun bruges, når det er under ejerens kontrol eller besiddelse”?

For niveau betydelig har NSIS denne bestemmelse: ”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.”

Den tilhørende engelske formulering i LoA Guidance er: ”The electronic identification means is designed so that it can be assumed to be used only if under the control of the subject to whom it belongs.”

Det ser ud til, at kravet i NSIS bestemmelsen for niveau betydeligt er øget i forhold til LoA med et krav om at brugeren skal være ”I besiddelse af det”. Det bør overvejes at følge LoA bestemmelsen, som synes bredere.

For niveau High har NSIS bestemmelsen: ”Det elektroniske identifikationsmiddel skal være beskyttet mod kopiering og manipulering samt angribere med højt angrebspotentialer.”

Den tilhørende engelske tekst i LoA Guidance er: ”The electronic identification means protects against duplication and tampering against attackers with high attack potential.”

Den engelske tekst indikerer at løsningen skal beskytte mod kopiering og manipulering ”udført af” angribere med højt angrebspotentialer, imens den danske tekst synes at kræve beskyttelse mod alle typer angreb fra angribere med højt angrebspotentialer.

Det foreslås, at NSIS bestemmelserne bringes i overensstemmelse med LoA Guidances’ bestemmelser, således at Danmark rammer de europæiske krav præcist på dette afgørende vigtige område af standarden.

Svar:

Der er tale om en fejl i angivelsen af kravet, hvor ”og” er blevet forvekslet med ”eller”, og dette er nu rettet til, så det følger forordningens krav. Det er således indarbejdet i standardens tekst.

Forslaget om omformulering af kravet til niveau ”Høj” punkt 7 er indarbejdet i standardens tekst, så den nu følger forordningen.

Rådet for digital sikkerhed

Kommentar:

"(fx match af billede og underskrift). Dette forudsætter personligt fremmøde. " Konkret synes udkastet med krav om eksempelvis ”fysisk fremmøde” ikke at tage højde for den digitale udvikling på dette område. Den teknologiske udvikling giver allerede i dag mange andre muligheder for at fastslå en persons identitet end gennem personligt fremmøde. Det bør sikres, at denne formulering ikke er til hinder herfor.

Svar:

Forslaget er indarbejdet i standardens tekst.

Sundhedsdatastyrelsen

Kommentar:

4. Høj

4) Det elektroniske identifikationsmiddel er udformet således, at den person, som det tilhører, kan beskytte det sikkert mod, at andre bruger det. Det fremgår ikke tydeligt, hvordan dette niveau adskiller sig fra ” 3. Betydelig”

Styrken af den enkelte autentifikationsfaktor bør nøje vurderes – herunder fx entropien af kodeord eller kryptografiske samt tilhørende kontroller. Disse krav bør være konkret specificeret, som de f.eks. er det i NIST standarden? Formålet med en standard er at sikre ensartethed. Ved at overlade dette til den enkeltes vurdering, opnår man det modsatte.

Svar:

Begge dele af forslaget behandles i vejledningen til standarden og indarbejdes dermed ikke direkte i standardens tekst.

Danske Regioner

Kommentar:

I sikringsniveau 2, punkt 2

o Her menes der vel delte identiteter, altså ”fællesbrugere”, hvor flere fysiske personer kender identiteten og adgang til denne elektroniske identifikationsmidler?

Svar:

Forslaget er indarbejdet, og standardens tekst er blevet præciseret i henhold til dette.

- Eksempler på akkreditiver i teksten efter tabellen

o Giv også gerne nogle eksempler på, hvad der ikke opnår hhv. niveau 3 og 4, så det bliver mere klart, hvilke karakteristika sikringsniveauerne skal have.

Svar:

Forslaget er ikke indarbejdet i standardens tekst, men behandles i vejledningen til standarden.

NETS

Kommentar:

Der mangler et ord i sætningen efter kryptografiske, ”- herunder fx entropien af kodeord eller kryptografiske samt tilhørende kontroller”. ”- herunder fx entropien af kodeord eller kryptografiske mekanismer? samt tilhørende kontroller”

Svar:

Her menes kryptografiske nøgler. Dette er tilføjet til standardens tekst.

Det fremgår, at ”Udstederen tager rimelige skridt til at kontrollere, at det kun er den person, som det tilhører, der har kontrol over og er i besiddelse af det.” Det er vanskeligt at kontrollere, om personen frivilligt har overdraget sit e-ID. Vil en sådan kontrol være påkrævet for sikringsniveau 2? Hvis ja, hvordan skulle denne kontrol eksempelvis foretages? Det skal præciseres, at det er i udleveringsprocessen der tænkes på.

Svar:

Der tænkes i denne kontekst ikke på frivillig overdragelse. Dette er ikke formålet med kravet.

Det fremgår, at ”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”. Kun faktorer i kategorien ”noget brugeren er” er ikke-overdragelige. Er der således krav om dette for at opnå sikringsniveau 3? Vejledning ønskes.

Svar:

Dette forslag er ikke tilføjet til standardens tekst, men i stedet behandlet i vejledningen til standarden.

Udstederen tager rimelige skridt til at kontrollere, at det kun er den person, som det tilhører, der har kontrol over og er i besiddelse af det. I ”Guidance for the application of the levels of assurance which support the eIDAS Regulation” bliver der specificeret, at dette krav kun kan kontrolleres af udstederen og henviser til afsnittet om udstedelse, levering og aktivering hvor det præciseres, at det er kun i fremsendelsesprocessen at dette kan kontrolleres. Det er vanskeligt generelt set, at overholde kravet om at det kun er den person som identifikationsmidlet tilhører der også til enhver tid har kontrol med det. Dette krav bør ligeledes flyttes til udstedelse og aktivering hvor det giver mere mening. Der er behov for en vejledning til at underbygge og klargøre forståelsen af dette krav.

Svar:

Forslaget er ikke indarbejdet i standardens tekst, men behandles i vejledningen til standarden.

3.2.2 Levering og aktivering

Signaturgruppen

Kommentar:

NSIS sætter samme krav til niveau lav som til niveau betydeligt, imens LoA guidance opererer med et ekstra krav for niveau betydeligt, samt en detaljeret guidance om forskellen i forhold til niveau lav. Det bør overvejes at føre NSIS tættere på LoA Guidance bestemmelserne.

Svar;

Forslaget er tilføjet til standardens tekst, så kravene er i overensstemmelse med den implementerende retsakt 2015/1502.

Danske Regioner

Kommentar:

I sikringsniveau 2, punkt 1, ”fx postforsendelse”

o i et liberaliseret postsystem kan enhver type postforsendelse vel ikke anvendes? Eksemplet bør evt. skærpes, så det fremgår, at en del af sikkerheden her beror på overholdelse af postloven. Bemærk endvidere at i større virksomheder åbnes post ofte af administrativt personale, for at afgøre hvem posten er til, så i forbindelse med medarbejdere er ”postforsendelse” ikke altid et tilstrækkeligt virkemiddel, til at sikre, at kun medarbejderen har adgang til forsendelsen. Endelig skal det nævnes, at postforsendelse giver problemer i forhold til såkaldt ”straksudstedelse” af digital identitet, hvilket er nødvendigt i regionerne.

o Overvej evt. helt at fjerne ”fx postforsendelse” og overlade det til guidancedokumentet at vejlede og beskrive eksempler.

Svar:

Forslaget er indarbejdet i standardens tekst. Vejledningen til standarden behandler behovet for eksempler.

NETS

Kommentar:

Udleveringen skal beskyttes mod angreb, hvor elektronisk identifikationsmidler stjæles under transport samt insider angreb i udleveringsfunktionen hos udstederen ved fx at benytte to uafhængige forsendelseskanaler eller funktionsadskillelse. Dette krav findes ikke i eIDAS gennemførelsesfordning (EU) 2015/1502. Kan det være i strid med EU regler?

Svar:

Forslaget er ikke indarbejdet i standardens tekst. Der må gerne være strengere krav eller krav tilpasset danske forhold.

3.2.3 Suspendering, spærring og genaktivering

Signaturgruppen

Kommentar:

Det bør overvejes, om eID udstederen også har pligt til selvstændigt at spærre en eID i beskrevne situationer, som det kendes fra MOCES CP afsnit 7.3.6.

Svar:

Forslaget er indarbejdet i standardens tekst.

Sundhedsdatastyrelsen

Kommentar:

3) Reaktivering skal kun finde sted, hvis de samme sikringskrav som forud for suspenderingen eller reaktiveringen fortsat er opfyldt. Det er ikke tydeligt, hvilke sikringskrav der henvises til.

Svar:

Kravet er omformuleret og præciseret.

Danske Regioner

Kommentar:

I sikringsniveau 2, punkt 2

Der savnes noget motivation. Det må handle om, at det ikke må være muligt at spærre eID'er som et slags "denial og service" angreb? Kom gerne med et eksempel.

Svar:

Forslaget er indarbejdet i vejledningen til standarden.

- I sikringsniveau 3, punkt 4

o "Hjemmeside" virker for løsningsspecifikt. Beskriv evt. i stedet, at teknologien skal rette sig mod alle brugere, have høj opetid og tilgængelighed osv. så også fremtidens grænseflader kan være omfattet af standarden.

Svar:

Forslaget er indarbejdet i standardens tekst.

KL/KOMBIT

Kommentar:

"indenfor få sekunder" – Hvad menes der præcis her. Kravet er lidt uklart. Er der spærring inden man kommer ind på en selvbetjeningsside hvor man kan spærre sin adgang er der gået mere end "få sekunder"? Måske det krav skal tunes lidt?

Svar:

Forslaget er indarbejdet i standardens tekst. "få sekunder" er fjernet fra kravet.

NETS

Kommentar:

Afsnittet nævner krav til brugerens mulighed for at spærre sit eID. Men hvad med eID udbyderens forpligtelse til at spærre, hvis eksempelvis udbyderen får mistanke eller bliver bekendt med at eID'et er kompromitteret. Overvej at indføre afsnit om eID udbyders forpligtelse til at spærre eID.

Svar:

Forslaget er indarbejdet i standardens tekst jf. ovennævnte forslag om det samme, stillet af Signaturgruppen.

Suspenderings-og spærrefunktionen bør være tilgængelig via en hjemmeside døgnet rundt – fraregnet minimale service vinduer. Dette krav findes ikke i eIDAS gennemførelsesforordning (EU) 2015/1502. Kan det være i strid med EU regler?

Svar:

Forslaget er ikke indarbejdet i standardens tekst. Der må gerne være strengere krav eller krav tilpasset danske forhold.

3.2.4 Fornyelse og udskiftning

Signaturgruppen

Kommentar:

NSIS har bestemmelsen: "Ovenstående krav sigter mod fornyelse i forbindelse med udløb af et elektronisk identifikationsmiddel. Sker fornyelsen inden for eID'ets udløbsperiode (fx fordi brugeren har mistet det oprindelige eID, eller dette er kompromitteret), kan re-identifikation evt. udelades op til niveau Betydelig, hvis der er stærke kontroller som sikrer, at eID'et udstedes til samme bruger."

Bestemmelsen synes vanskelig at læse og forstå. Signaturgruppen går ud fra, at

intentionen er, at et endnu gyldigt eID kan anvendes som autentifikation i forbindelse med udstedelse af et andet eID med længere gyldighedsperiode. Men hvad er intentionen med udeladelsen af re-identifikation for brugere, som har mistet eller kompromitteret eID?

Det bør vurderes om dette afsnit kan formuleres tydeligere.

Svar:

Dette forslag behandles i vejledningen til standarden.

Danske Regioner

Kommentar:

I sikringsniveau 4, punkt 2

o Der er ingen vejledning eller specifikation af, hvor lang tid der skal gå mellem fornyelse i hvert niveau. Der savnes noget mere håndfast.

Svar:

Dette er ikke indarbejdet i standardens tekst, men behandles i vejledningen til standarden.

o Begrebet ”identitetsdata” omtales, men er ikke yderligere specificeret. Regionerne formoder, at ”identitetsdata” er de data, som knyttes sammen med den digitale identitet ved oprettelse/fornyelse. I en løsning med privat e-ID og tilknyttet CVR nummer, er denne relation da inden for begrebet ”identitetsdata”?

Svar:

Forslaget er indarbejdet i standardens tekst. Identitetsdata er ændret til personidentifikationsdata, og der er endvidere tilføjet en beskrivelse af begrebet i 1.5 Terminologi.

KL/KOMBIT

Kommentar:

Kravet om at man skal bruge samme identifikationsproces som ved oprindelige udstedelse er forståelig, men det er ikke super praktisk for kommunerne når en bruger har glemt sit kodeord, så skal de gennem den helt store proces for at få et nyt.

Svar:

Det fremgår af teksten i 3.2.4 Fornyelse og udskiftning, at såfremt der er stærke kontroller, der sikrer, at eID'et udstedes til samme bruger, kan re-identifikation udelades op til niveau "betydeligt" – fx så en bruger ikke skal starte helt forfra, hvis der er tale om et glemt kodeord.

3.3 ANVENDELSE OG AUTENTIFIKATION

Ingen bemærkninger til dette punkt.

3.3.1 Autentifikationsmekanismer

Sundhedsdatastyrelsen

Kommentar:

4) Autentifikationsprocessen skal være dynamisk (dvs. det præsenterede bevis skal være unikt per autentifikationsproces). Dette bør præciseres, f.eks. ved at angive entropien af nonce osv.

Svar:

Forslaget indarbejdes ikke i standardens tekst, men behandles i vejledningen til standarden.

5) Autentifikationsmekanismen implementerer sikkerhedskontroller til at efterprøve det elektroniske identifikations-middel, således at det er højest usandsynligt, at det er muligt for en angriber med en moderat angrebskapacitet at gætte, lytte sig til, gengive eller manipulere kommunikationen og på den måde omgå autentifikationsmekanismen. Begreberne "højest usandsynligt" "moderat angrebskapacitet" er for uspecifikke, og afsnittet bør konkretiseres, og gerne angive eksempler, som letter forståelsen.

Svar:

Forslaget er ikke indarbejdet i standarden, som er resultatbaseret. Eksempler behandles generelt i vejledningen til standarden.

Danske Regioner

Kommentar:

- Sikringsniveau 3, punkt 4
 - o Fodnote. For at sikre at læseren ser dette som et eksempel på opfyldelse, bør der i stedet for ”vil normalt” stå ”vil for eksempel normalt”.

Svar:

Fodnoten er udgået i forbindelse med omskrivning af kravet, der henviste til noten.

NETS

Kommentar:

Man bør sikre at definitionen er konsistent med eIDAS forordningens. ‘dynamic authentication’ means an electronic process using cryptography or other techniques to provide a means of creating on demand an electronic proof that the subject is in control or in possession of the identification data and which changes with each authentication between the subject and the system verifying the subject's identity”.

Svar:

Forslaget er indarbejdet i standardens tekst, som er blevet omskrevet, så kravet er tilpasset eIDAS-forordningen.

Fodnote 4 på side 14 bør slettes da den giver frirum til fortolkning til at nonce kan vælges således at den er forudsigelig for en angriber. Dette vil ødelægge formålet med dynamisk autentifikation.

Svar:

Fodnoten er fjernet som følge af omskrivning af kravet, der ledte til fodnoten.

”Frigivelse af personidentifikationsdata”. Det er uklart hvad personidentifikationsdata er. Drejer det sig om navn og adresse eller drejer det sig om PID numre? Hvis det drejer sig om persondata kan denne frigivelse muligvis

være i strid med privacy by design som krævet i EU GDPR. Overvej at ændre formulering om personidentifikationsdata.

Svar:

Personidentifikationsdata er tilføjet til standardens tekst, afsnit 1.5, terminologi.

3.4 ORGANISATORISKE- OG TVÆRGÅENDE KRAV

Lakeside

Kommentar:

Der er uklart hvem der skal leve op til kravene i dette afsnit. I 3.4.1 står der at kravene skal overholdes af eID-tjenester, men der mangler en eksplicit angivelse af hvem der skal leve op til kravene i de andre underafsnit i 3.4 (der antages at kravene gælder eID-tjenester).

Svar:

Forslaget er indarbejdet i standardens tekst, hvor der nu er foretaget et kapitelskifte således, at det nu bør fremgå mere tydeligt, at disse krav gælder alle, der leverer en eID-tjeneste eller dele heraf.

3.4.1 Generelle krav

Signaturgruppen

Kommentar:

Det kan overvejes, om der ikke skal stilles krav til opbevaringsperiode for centrale logningsdata til afklaring af hændelser eller tvister, som det fastlægges i MOCES CP afsnit 7.4.11.

Svar:

Forslaget er ikke indarbejdet i standardens tekst, men behandles i vejledningen til standarden.

NETS

Kommentar:

Det fremgår, at ”Leverandøren skal leve op til alle krav for de tilbudte tjenester.” Hvad betyder det? For de tilbudte eID tjenester?

Svar:

Her menes; for dele af eID en livscyklus, eID-tjenesteudbyderen deltager i.

Der er i kasse ”2 lav” henvist til Forvaltningsloven – den gælder ikke for private virksomheder. Den bør udgå. Henvielse bør udgå.

Svar:

Forslaget er indarbejdet i standardens tekst, så det nu fremgår, at det gælder for offentlige myndigheder.

3.4.2 Oplysningspligt

Signaturgruppen

Kommentar:

Dette afsnit var måske et godt sted at placere eID leverandørers eventuelle oplysningspligt i forhold til specifikation af brugeres og relying parties ansvar og forudsætningerne til disse parter ageren for opnåelse af det specificerede sikringsniveau?

Svar:

Dette forslag er indarbejdet i standardens tekst, som punkt 2, under niveau ”lav”.

Peercraft

Kommentar:

Teksten bør jf. den definerede terminologi anvende: ”sine elektroniske identifikationsmidler” i stedet for ”sit eID, dele heraf eller kodeord”

Svar:

Forslaget er indarbejdet i standardens tekst.

Udover at forsætlig overdragelse af identifikationsmidler fremstår som et brud på betingelserne er det vigtigt at dette fremstår som en reel sikkerhedsvejledning af brugeren. Dette er i særlig grad nødvendigt, når løsningens sikringsniveau er baseret på tillid til RP'en og et til brugeren overladt ansvar for ved personlig stillingtagen at mitigere diverse for brugeren vanskeligt gennemskuelige former for brud på denne tillid (Ref. Punkt 1)

Svar:

Dette forslag er indarbejdet i standardens tekst, som punkt 2, under niveau ”lav”.

3.4.3 Informationssikkerhedsledelse

KL/KOMBIT

Kommentar:

Tænker at der skal være en læse-let guide til kommunerne her. Kun at pege på ISO 27001 kommer til at koste kommunerne mange penge i konsulenttimer.
-Her mangler også noget omkring compliance, hvor man kunne overveje ISO 29.100

Svar:

Forslaget er ikke indarbejdet i standardens tekst, men behandles i vejledningen til standarden.

3.4.4 Dokumentation og registerføring

Ingen bemærkninger til dette punkt.

3.4.5 Faciliteter og personale

NETS

Kommentar:

Som krav til sikringsniveau ’Høj’ er angivet at ”det skal sikres at adgang til og ophold i de centrale driftslokaler videoovervåges”. Hvorfor er dette rimelige krav ikke gældende for sikringsniveau ’Betydelig’? Man kan overveje om ikke også kravet bør eksistere på sikringsniveau ’Betydelig’.

Svar:

Forslaget er indarbejdet i standardens tekst.

IDA

Kommentar:

Der synes at være uklarhed om, hvorvidt krav til henholdsvis indhentelse af straffeattester, punkt 7) og krav til uddannelse, erfaring og sikkerhedsklassifikation, punkt 8) både gælder for ledere og medarbejdere, der

udfører betroede opgaver og for personale hos underleverandører. Det anbefales, at gøre det helt klart, at både indhentelse af straffeattester OG krav til uddannelse, erfaring og sikkerhedsklassifikation gøres gældende for begge grupper, da der er tale om to forskellige krav.

Svar:

Forslaget er indarbejdet i standardens tekst. De refererede punkter 7 og 8 er nu slået sammen og omformuleret under sikringsniveau "betydelig", som punkt 5.

Rådet for digital sikkerhed

Kommentar:

"7) Det skal kontrolleres, at ledere og medarbejdere, der udfører betroede opgaver, ikke er straffet for en forbrydelse, der gør dem uegnede til at bestride deres hverv.

8) Det skal sikres, at personale hos underleverandører opfylder samme krav til uddannelse, erfaring og sikkerhedsklassifikation som tjenestens egne medarbejdere i de funktioner, underleverandørens personale varetager. "

Der sammenblandes sikkerheds klassifikation og straffeattest – det er ikke det samme. Teksten bør omformuleres, så kravene er ensartede.

Svar:

Forslaget er indarbejdet i standardens tekst. De refererede punkter 7 og 8 er nu slået sammen og omformuleret under sikringsniveau "betydelig", som punkt 5.

Danske Regioner

Kommentar:

- Sikringsniveau 4, punkt 10 og 11

o Det er uklart for regionerne, hvor stor en del af identitets-infrastrukturen disse krav gælder for. Gør dette sig også gældende for organisationer, der leverer brokere (identity providers / SAML tokens / IDWS tokens)? Bør skærpes.

Svar:

Forslaget er indarbejdet i standardens tekst. Det fremgår nu af den indledende tekst under kapitel 4, at alle krav også gælder brokere.

Lakeside

Kommentar:

punkt 11: Reference til DS 471 mangler.

Svar:

Forslaget er indarbejdet i standarden.

3.4.6 Tekniske kontroller

Sundhedsdatastyrelsen

Kommentar:

Der mangler beskrivelse af krav til logning og sikring af logs.

Svar:

Forslaget er indarbejdet i standardens tekst, under afsnit 3.4.4.

3) Adgang til kryptografisk materiale brugt til udstedelse af akkreditiver eller autentifikation skal være begrænset til de roller og applikationer, der har et strengt nødvendigt behov for adgang, og de må aldrig gemmes i klar tekst i persistente lagringsmedier. Det fremgår ikke tydeligt, hvad der henvises til med ”de” i teksten: ”de” må aldrig gemmes i klar tekst”.

Svar:

Forslaget er indarbejdet i standardens tekst. Her menes kryptografisk materiale, og dette fremgår nu mere præcist af kravet.

6) Følsomt kryptografisk materiale anvendt til udstedelse af eID og autentifikation, som lagres vedvarende, skal beskyttes mod manipulation. Dette krav er dækket af pkt. 5.

Svar:

Forslaget er ikke indarbejdet i standardens tekst. Det refererede punkt 6, er mere vidtrækkende.

7) Der bør ikke benyttes kryptografiske algoritmer eller protokoller med kendte sårbarheder eller med utilstrækkelige nøglelængder Dette krav er dækket af pkt. 4

Svar:

Forslaget er ikke indarbejdet i standardens tekst, idet punkt 7 er mere specifikt end punkt 4, som er mere generelt.

DK-Cert

Kommentar:

Ved sikringsniveau Lav kræves det, at der findes ”rimelige tekniske kontroller, som gør det muligt at afværge trusler mod tjenesternes sikkerhed ...”
DKCERT savner en nærmere definition af, hvilket niveau af tekniske kontroller, der vil være ”rimelige”.

Svar:

Dette forslag er ikke indarbejdet i standardens tekst, men behandles i vejledningen til standarden.

Ved sikringsniveau Betydelig og Høj lyder kravet 7) Der bør ikke benyttes kryptografiske kontroller, eller protokoller med kendte sårbarheder eller med utilstrækkelige nøglelængder. Vi finder at dette er et så afgørende krav til disse sikringsniveauer, at det bløde ord ”bør” ikke kan benyttes. I stedet foreslår vi, at der skrives ”Der må ikke benyttes..”.

Svar:

Dette forslag er indarbejdet i standardens tekst.

NETS

Kommentar:

Ved sikringsniveau 3- betydeligt er formuleret ”der ”bør” ikke benyttes kryptografiske algoritmer eller protokoller med kendte sårbarheder eller utilstrækkelig nøglelængde”. Kravet bør skærpes til:
”der ”må” ikke benyttes kryptografiske algoritmer eller protokoller med kendte sårbarheder eller utilstrækkelig nøglelængde”.

Svar:

Dette forslag er indarbejdet i standardens tekst.

3.4.7 Anmeldelse og revision

IDA

Kommentar:

Forslaget til NSIS udmærker sig ved et generelt højt fokus på sikkerhed. Det er derfor bekymrende, at Digitaliseringsstyrelsen alene påtager sig ansvar for at sikre, at formalia er opfyldt ved anmeldelse af en eID-ordning men ikke for, hvorvidt den anmeldte løsning faktisk lever op til det angivne sikringsniveau. Det skal her anbefales, at ansvaret for sikkerhedsniveauet for anmeldte eID-ordninger placeres hos en myndighed, der konkret gennemgår og godkender løsningens sikkerhedsniveau. En sådan certificering vil også være med til at øge tilliden til den digitale løsning.

Svar:

Forslaget indarbejdes ikke i standarden, idet det ligger uden for Digitaliseringsstyrelsen ressort og kompetenceområde at opretholde en teknisk certificeringsenhed. I forbindelse med anmeldelse på niveau ”betydelig” og ”høj” skal der indsendes omfattende og detaljeret dokumentation for, at en løsning lever op til alle krav, og dette skal være undersøgt og påtegnet uden forbehold af en uvidlig og eksternt statsautoriseret revisor, med speciale i it-revision. Revisionserklæringen er særligt udarbejdet til formålet, og det er Digitaliseringsstyrelsens opfattelse, at denne skal være garant for, at alle krav fuldt ud efterleves.

Signaturgruppen

Kommentar:

Det er ønskeligt, at en part som skal vurdere, om de bør etablere tillid til en given anmeldt løsning, har mulighed for at finde den relevante information på digitaliser.dk, samt at der gives sikre værktøjer til validering af, at det er den rigtige udsteder man etablerer tillid til. Til eksempel anviser PKI standardiseringen sikre metoder til validering af de såkaldte rodcertifikater.

Det ser ud til at NSIS kravene i afsnit 3.4.7 for niveau betydeligt, med krav om minimum årlige uafhængige eksterne revision, er højere end de tilsvarende bestemmelser i LOA afsnit 2.4.7. Imens NSIS kravene virker mere præcise, instruktive og passende for store (nationale) identitetsudbydere, kan det overvejes, om de højere danske krav kan give en skævvridning i forhold til internationale identitetsløsninger revideret efter LOA Guidance krav?

Svar:

Forslaget er ikke indarbejdet i standardens tekst. eID-løsninger under forordningen skal notificeres og gennem et omfattende peer-review. NSIS beror ikke på dette, men på anmeldte eID løsninger, der på niveau ”betydelig” eller ”høj” skal have en ekstern gennemgang af løsningen, hvor en statsautoriseret it-revisor skal vurdere om løsningen lever op til alle gældende krav. Det er dermed afgørende, at revisionserklæringen er udfærdiget på en måde, der gør it-revisoren i stand til at undersøge om alle krav er tilstrækkeligt opfyldt.

De nuværende NSIS krav til anmeldelse og revision på niveau betydelig kan muligvis gøre det for kostbart at anmelde f.eks. kommunale eller regionale identitetsudbydere med føderationsmodellen på dette niveau, hvilket kan vanskeliggøre etableringen af et troværdigt ensartet sikkerhedsniveau for denne type løsninger.

Svar:

Forslaget er ikke indarbejdet i standardens tekst. Det er afgørende for tilliden til standarden og dets anmeldte eID løsninger, at de anmeldte løsninger på niveau ”betydelig” og ”høj” er gennemgået af en uvildig, ekstern og statsautoriseret revisor med speciale inden for it-revision, for at sikre at kravene er tilstrækkeligt opfyldt.

Det kan overvejes om de tekniske referencer til sikkerhedsstandarder i LOA afsnit 2.4.7 bør citeres eller refereres i NSIS, eller hvorvidt andre mere præcise grundlag for revision kan specificeres.

Svar:

Forslaget er ikke indarbejdet i standardens tekst, men behandles i vejledningen til standarden. Dette er i øvrigt på linje med, hvordan det er behandlet i LOA guidance, der er vejledningen til den implementerende retsakt.

DI Digital

Kommentar:

For det første finder DI Digital det betænkeligt, at Digitaliseringsstyrelsen ved anmeldelse af eID-ordninger jf. pt. 3.4.7 alene påtager sig ”ansvar for at sikre, at formalia omkring opfyldelse af anmeldelse er overholdt”. Styrelsen eller en anden myndighed burde vurdere, om de anmeldte løsninger i praksis har det sikringsniveau, som anmelder angiver. Der er risiko for, at Styrelsen medvirker til at offentliggøre og dermed reelt blåstemple løsninger til et givent sikkerhedsniveau, uden at dette har hold i virkeligheden. En eID-ordning, som i praksis ikke kan efterleve det angivne niveau, kan bidrage til at underminere tilliden til standarden og de øvrige offentliggjorte eID-ordninger.

Svar:

Forslaget indarbejdes ikke i standarden, idet det ligger uden for Digitaliseringsstyrelsen ressort og kompetenceområde at opretholde en teknisk certificeringsenhed. I forbindelse med anmeldelse på niveau ”betydelig” og ”høj” skal der indsendes omfattende og detaljeret dokumentation for, at en løsning lever op til alle krav, og dette skal være undersøgt og påtegnet uden forbehold af en uvildig og eksternt statsautoriseret revisor, med speciale i it-revision. Revisionserklæringen er særligt udarbejdet til formålet, og det er Digitaliseringsstyrelsens opfattelse, at denne skal være garant for, at alle krav fuldt ud efterleves.

Lakeside

Kommentar:

Begrebet 'eID-ordning' anvendes uden forudgående forklaring.

Svar:

Forslaget er indarbejdet i standardens tekst. ”Elektronisk identifikationsordning” er tilføjet til afsnit 1.5, terminologi.

NETS

Kommentar:

Under krav nævnes ’tjenesteudbyder’. Dette begreb er ikke anvendt før. ’Tjenesteudbyder’ bør defineres.

Svar

Forslaget er indarbejdet i standardens tekst. ”Tjenesteudbyder” er ændret til ”leverandør”.

4. ELEKTRONISKE IDENTIFIKATIONSMIDLER ASSOCIERET TIL JURIDISKE PERSONER

Ingen bemærkninger til dette punkt.

4.1 UDSTEDELSE AF ELEKTRONISKE IDENTIFIKATIONSMIDLER

Signaturgruppen

Kommentar:

Den nuværende indledende tekst indeholder enkelte undtagelser og formuleringer som kan skabe lidt forvirring om, hvilke dele af kapitel 3 der egentlig gælder. For klarhedens skyld kunne hver enkelt undtagelse måske beskrives selvstændigt, for eksempel som ”i tabel xx erstattes den nuværende tekst med denne nye tekst:...”. De særligt formulerede krav i tabellens række ”Betydelig” i afsnit 4.1 bærer præg af OCES konteksten og fremstår indforståede uden yderligere beskrivelse. I stedet for beskrivelse af proces for udlevering af adgangskode kunne der være en bestemmelse om at ”den implementerede etablerings- og udleveringsproces sikrer, at det med høj sikkerhed kun er den retmæssige bruger, som efterfølgende har kontrol over og kan anvende identifikationsmidlet” inspireret af kravene i 3.2.2.

Svar:

Forslaget er indarbejdet i standardens tekst. Kravene i kapitel 3 for fysiske personer gælder også for udstedelse af eID til fysiske personer associeret til juridiske personer.

Generelt bør kapitel 3 genlæses i medarbejderkonteksten, hvor det nok bør indtænkes at organisationen og dens administratorer også pålægges ansvar og rettigheder på linje med brugeren.

For eksempel bør 3.2.3 Suspending, spærring og genaktivering omfatte organisationens ret til via en administrator at spærre en medarbejder identitet.

Svar:

Forslaget er indarbejdet i standardens tekst under afsnit 5.2, punkt 2.

Det bør også vurderes om den skelnen imellem organisationens ansvar (Certifikatindehaver) og den enkelte brugers (certifikatholder) ansvar bør opdeles, på linje med hvad der kendes fra OCES CP’erne.

Svar:

Forslaget er delvist indarbejdet i standardens tekst. Afsnittet om ansvar og forsikring samt afsnit 4.2.1 om oplysningspligt, er opdateret med krav til eID-brugerne.

Sundhedsdatastyrelsen

Kommentar:

Videregivelse af den midlertidige adgangskode sker på betryggende vis, Der mangler en beskrivelse af, hvordan det sikres, at sikringsniveauet i denne sammenhæng er på højde med brugerens samlede sikringsniveau.

Svar:

Forslaget er indarbejdet i standardens tekst. Kravene i kapitel 3 for fysiske personer gælder også for udstedelse af eID til fysiske personer associeret til juridiske personer. Hermed opnås ensartet sikkerhed.

Danske Regioner

Kommentar:

Umiddelbart ser dette afsnit ikke ud til at være dækket af "LOA guidance" dokumentet. Fx er der ingen guide for, hvilken kvalitet "kvitteringen" i sikringsniveau 3 og 4 skal have.

- Sikringsniveau 3 punkt 4 bullet 2.
 - o Regionerne savner vejledning i, hvad kvitteringen skal sik-re, fx at det bliver uafviseligt, at medarbejderen/borgeren har fået udleveret sit elektroniske identifikationsmiddel.

Der savnes krav til opbevaring af kvitteringen og nogle eksempler på valide løsninger.

Svar:

Forslaget er ikke indarbejdet i standardens tekst, men behandles i vejledningen til standarden.

Lakeside

Kommentar:

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:

- a. Dokumentation af registreringsprocessen og 'forbindelsesprocessen' med ekstern revision (og ikke kun i forbindelse med straksudstedelse)

Svar:

Forslaget er indarbejdet i standardens tekst.

- b. Notifikation af den fysiske person ved udstedelse eller 'forbindelse' af et eID (fx. via brev til bopælsadressen eller via besked i e-boks).

Svar:

Forslaget er ikke indarbejdet i standardens tekst, men behandles i vejledningen til standarden.

NETS

Kommentar:

Hvem er udstederen nævnt i ”kasse 2 lav”? Det fremgår, at udstederen skal udstede en instruks for anvendelse af eID’et, som beskriver tilladt og ikke-tilladt brug. Udsteder blander sig normalt ikke i, hvad et medarbejder certifikat anvendes til, kun at det er udstedt til den pågældende identificerede person. En klarere adskillelse af rollefordeling mellem eID provider og virksomheden. Det bør tydeliggøres, at det er virksomheden, der skal sætte regler for, hvad eID’et må bruges til i arbejdsmæssig sammenhæng?

Svar:

Forslaget er indarbejdet i standardens tekst. Det er nu kapitel 3, der gælder for eID associeret til juridiske personer.

4.2 BINDING (ASSOCIERING) MELLEM ELEKTRONISKE IDENTIFIKATIONSMIDLER FOR FYSISKE OG JURIDISKE PERSONER

Signaturgruppen

Kommentar:

Det kunne med fordel beskrives yderligere, at dette afsnit omfatter krav, hvor et elektronisk identifikations-middel udstedt til, og ejet af, en (natural) fysisk person jf. kapitel 3 associeres til en juridisk person, men i øvrigt anvendes uændret. Til eksempel kunne man nævne den kommende løsning, hvor virksomhedsejer i nogle typer af virksomheder tillades at anvende sit private NemID til at repræsentere virksomheden.

Svar:

Forslaget er indarbejdet i standardens tekst.

Sundhedsdatastyrelsen

Kommentar:

4. Høj

Som Betydelig samt flg.:

1) Godtgørelse af identiteten af den fysiske person, der handler på vegne af den juridiske person, kontrolleres på sikringsniveau »betydelig« eller »høj«.

Sikringsniveauet »betydelig» skal slettes her.

Svar:

Forslaget er indarbejdet i standardens tekst.

Lakeside

Kommentar:

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:

- a. Dokumentation af registreringsprocessen og 'forbindelsesprocessen' med ekstern revision (og ikke kun i forbindelse med straksudstedelse)
- b. Notifikation af den fysiske person ved udstedelse eller 'forbindelse' af et eID (fx. via brev til bopælsadressen eller via besked i e-boks).

Under '4. Høj' i tabellen står der under punkt 1: '... kontrolleres på sikringsniveau »betydelig« eller »høj«.' Menes der ikke '... kontrolleres på sikringsniveau »høj«.?'

Svar:

Forslaget er indarbejdet i standardens tekst.

: Sætningerne 'Godtgørelse af identiteten af den fysiske person, der handler på vegne af den juridiske person, kontrolleres på sikringsniveau ... ' er lidt svært forståelige ('godtgørelse' anvendes i en ikke særlig gængs betydning). De kunne med fordel omskrives til noget i stil med 'Validering af identiteten af den fysiske person, der handler på vegne af den juridiske person, foretages på sikringsniveau ...'.

Svar:

Forslaget er indarbejdet i standardens tekst.

Peercraft

Kommentar:

Dette krav er en eksakt kopi af det tilsvarende først angivne krav til "3. Betydelig" og bør derfor slettes.

Svar:

Forslaget er indarbejdet i standardens tekst.

NETS

Kommentar:

Det fremgår, at "Forbindelsen er blevet etableret på grundlag af anerkendte procedurer." Hvem skal have foretaget denne anerkendelse? Præcisering af hvad der ligger bag "anerkendte" procedurer. Eksempler vil hjælpe på forståelsen.

Af "kasse 2 Lav 3)" og "kasse 3 betydelig 2) og 3)" fremgår det at, "Den fysiske person er ikke registreret af en autoritativ kilde, med en status der afholder den fysiske person fra at handle på vegne af den juridiske person", "Forbindelsen er blevet etableret på baggrund af anerkendte procedurer, som resultere i registrering af forbindelsen i autoritativ kilde" og "Forbindelsen er blevet kontrolleret på grundlag af oplysninger fra en autoritativ kilde" Det bør tydeliggøres, at dette er en forpligtelse, der påhviler virksomhederne.

Det bør præciseres, hvad en autoritativ kilde er i de forskellige sammenhænge.

Svar

Forslaget er ikke indarbejdet i standardens tekst, men behandles i vejledningen til standarden.

5. KRAV TIL BROKERLØSNINGER

IDA

Kommentar:

Hvis det påtænkes, at niveau 4 også skal benyttes af almindelige borgere, bør det overvejes, om ikke der skal være mulighed for Single Sign-On i de tilfælde, hvor en certificeret tjeneste videregiver en identitet til en anden tjeneste på samme eller lavere niveau. Risikoen ved at afvise brug af Single Sign-On er, at tjenesten bliver for usmidig og dermed enten ikke brugt eller at sikkerheden forsøges omgået, fordi det anses at være alt for besværligt.

Svar

Forslaget er indarbejdet i standardens tekst. Det er således valgfrit for en given tjeneste at anvende Single Sign-On.

Signaturgruppen

Kommentar:

Der bør også tages stilling til sikringsniveauer i sammenbundne løsninger, hvor man anvender en kæde af brokere. Dette er den almindelige situation i mange arkitekturer for fødererede identiteter, og gælder særligt for KOMBIT rammearkitekturen.

Der er nok behov for at specificere:

- Hvilket sikringsniveau kan opnås for en eID fra en broker, som baserer sig på en række andre brokere?

Svar

Forslaget er indarbejdet i standardens tekst.

- Hvorledes sikres logning af aktivitet på tværs af brokere, således at en transaktion kan spores fra brugeren og til tjenesteudbyderen? (KOMBIT rammearkitektur specificerer krav til logning, formater, synkronisering af tid etc.)

Svar

Forslaget er ikke indarbejdet i standardens tekst, men behandles i vejledningen til standarden.

Der er formuleret en undtagelse for kravet om HSM beskyttelse af private udstedelsesnøgler for IdP'ere, som kun servicerer egne brugere i en brugerorganisation. Umiddelbart kunne man tænke, at risikoen kun var den pågældende organisations egen, men egentligt svækkes den samlede adgangskontrol for de tjenester, der vælger at acceptere eID fra en sådan organisation, idet en stjålet privat IdP nøgle fra denne organisation ville kunne misbruges til at give bred uberettiget adgang til disse tjenester.

Det bør genovervejes, hvorledes dette stiller de data-ansvarlige for en tjenesteudbyder i forhold til at løfte ansvaret for beskyttelse af adgangen til data? Som standarden er formuleret nu, ser det endvidere ud til at eID'ere fra disse IdP'ere også vil kunne anmeldes og anvendes overfor tjenester i andre EU lande på niveau betydeligt? Her harmonerer en dansk undtagelse næppe med intentionen om et fælleseuropæisk sikringsniveau.

Svar

Forslaget er ikke indarbejdet i standardens tekst. Der stilles allerede krav om sikker opbevaring af brokerens private nøgle på niveau "lav", og en betydelig forøgelse af kravet på niveau "betydelig" vil kunne betyde, at ganske få vil anmelde en eID løsning på dette niveau.

Rådet for digital sikkerhed

Kommentar:

"9 Single Sign-On må ikke anvendes dvs., at der skal ske en fornyet (frisk) autentifikation af brugeren ved hver forespørgsel til broderen om autentifikation."
"

Dette vil givet sikre, at dette niveau ikke vil blive brugt af almindelige borgere, da det vil medføre et sandt mareridt for borgerne med gentagne logon ved hvert tjenesteskift. Det er ikke i tråd med den udvikling, der er indenfor digitalisering. Det bør være muligt, at en certificeret tjeneste videregiver en identitet til en anden tjeneste på samme eller lavere niveau.

Svar

Forslaget er indarbejdet i standardens tekst. Det er således valgfrit for en given tjeneste at anvende Single Sign-On.

Sundhedsdatastyrelsen

Kommentar:

1) Security tokens må kun udstedes umiddelbart efter forudgående, succesfuld autentifikation Security tokens må godt omveksles til andre security tokens løbende gennem en session, så det bør præciseres hvilken type security tokens, kravet vedrører.

Svar

Forslaget er indarbejdet i standardens tekst.

2) Sikringsniveau'et for den anvendte autentifikation skal indeholdes som en attribut i det udstedte token (level of assurance), således at tjenesten direkte kan aflæse dette. Det er det samlede sikringsniveau forstået som det lavest sikringsniveau for alle delområder, og ikke blot sikringsniveauet for autentifikation, der skal indgå i det udstedte token.

Svar

Forslaget er indarbejdet i standardens tekst.

6) Tokenet skal være begrænset til en specifik tjeneste (såkaldt AudienceRestriction). AudienceRestriction er et SAML begreb. Der er behov for en teknologineutral definition, så det også fremgår, hvad det betyder i andre sammenhænge.

Svar

Forslaget er indarbejdet i standardens tekst.

Danske Regioner

Kommentar:

Umiddelbart ser dette afsnit heller ikke ud til at være dækket af ”LOA guidance” dokumentet.

Svar

Korrekt. Brokere er ikke omfattet af LOA guidance.

- Regionerne savner generelt en præcis definition af ”broker” begrebet. Gælder kravene også evt. STS’er?

- Regionerne savner også nogle krav, der forhindrer replay

Svar

Forslaget er indarbejdet i standardens tekst.

- Sikringsniveau 4, punkt 9
o Regionerne savner motivation for dette punkt, og evt. op-hæng til internationale rammeværk, som ligger til grund for at fravælge muligheden for SSO

Svar

Forslaget er indarbejdet i standardens tekst.

o Regionerne savner mere præcision og scoping af dette punkt. Det kan muligvis

give mening ikke at tillade SSO mellem forskellige webbaserede tjenester på sikringsniveau 4, men det bør præciseres, at der for en given tjeneste stadig er mulighed for (efter passende systemteknisk veksling af tokens) at kontakte forskellige bagvedliggende web services inden for samme session. Med den nuværende formulering kan man godt blive i tvivl.

Svar

Forslaget er indarbejdet i standardens tekst.

o Regionerne savner krav til levetid for sessioner og evt. servicetokens udstedt inden for disse sessioner. Desuden savnes der krav til egenskaberne af sessionen, fx krav til hvor sikker systemet skal være på, at brugeren stadig er til stede ved it-applikationen mv.

Svar

Forslaget er ikke indarbejdet i standardens tekst, men behandles i vejledningen til standarden.

DK-Cert

Kommentar:

DKCERT noterer med tilfredshed, at der i krav 8) stilles krav om anvendelse af HSM til placering af brokerens private nøgle, der anvendes til signering af security tokens.

I krav 9) (sikringsniveau Høj) stilles krav om at Single Sign-On ikke må anvendes. DKCERT anerkender det sikkerhedsmæssige formål med dette krav, men finder at en afvejning af brugervenlighed og sikkerhedsniveau i tilfælde, hvor en certificeret tjeneste på niveau Høj videregiver (evt. anonymiserede) login-tokens til tjenester på lavere niveau, kan trække i retning af at der her – efter konkret vurdering - åbnes for muligheden for Single Sign-On. I modsat fald kan frygte, at tjenesten enten ikke vil blive brugt eller kontrollen vil blive forsøgt omgået.

Svar

Forslaget er indarbejdet i standardens tekst.

DI Digital

Kommentar:

For det andet ser der ikke ud til i NSIS at være lagt op til muligheden for at bruge pseudonymer. Særligt med henvisning til de krav til data protection by design og pseudonymisering som sikkerhedsmekanisme, der fremgår af persondataforordningen, synes det oplagt at benytte denne standard til at fastslå muligheden for at bruge pseudonymer. F.eks. ville det være oplagt at anvende pseudonymer i forhold til brokeren omtalt i kapitel 5, således at denne ikke ville kunne opsamle informationer om brugerne. Der findes på markedet allerede glimrende identitetsløsninger, som understøtter dette - f.eks. i form af U-Prove og IdentityMixer.

Svar:

Forslaget er indarbejdet i standardens tekst. Endvidere behandles pseudonymisering i vejledningen til standarden.

Finansrådet

Kommentar:

I udkastets afsnit 5 behandles de forventede krav til broker-løsninger, hvor det blandt andet fremgår, at det ikke på niveau høj skal være muligt at tilbyde single-sign on til brugerne. Brugernes ønsker til en digital tjenesteudbyders tilgængelighed, fleksibilitet og hastighed opvejer, når adspurgte - og i særdeleshed ved genbesøg - ofte brugerens krav til sammes sikkerhedsforanstaltninger, som eksempelvis forbundet med to-faktor log-in processer.

Svar:

Forslaget er indarbejdet i standardens tekst.

Lakeside

Kommentar:

Udover kravet omkring 'audience restriction' bør der overvejes at stille krav om kryptering af selve tokenet under aftagertjenestens nøgle på sikringsniveau 3 for at opnå end-to-end konfidentialitet (fremfor kun punkttil-punkt konfidentialitet som kravet omkring transportlagskryptering på sikringsniveau 2 sikrer).

Svar:

Forslaget er indarbejdet i standardens tekst.

Peercraft

Kommentar:

Er meningen ikke blot at der skal ske en ny frisk autentifikation af brugeren, hver gang denne vil tilgå en service, der kræver sikringsniveau 4? Hvorimod en autentifikation på niveau "4. Høj" efterfølgende uden fornyet autentifikation vil kunne give adgang til services, der kræver et lavere sikringsniveau? I så fald bør teksten ændres til: "Der skal ske en fornyet (frisk) autentifikation af brugeren ved hver forespørgsel til broderen om et token til en specifik tjeneste."

Svar:

Forslaget er indarbejdet i standardens tekst.

NETS

Kommentar:

Der refereres til NemLogin. Der bør ikke refereres til specifikke løsninger/produkter i en standard. Standarder bør være generiske. Eksempler bør flyttes over i en vejledning. Her gælder det helt konkret eksemplet om Nemlogin.

Svar:

Forslaget er ikke indarbejdet i standardens tekst. Der er tale om et eksempel, der ikke har indflydelse på kravene.

6. GOVERNANCE

Ingen bemærkninger til dette punkt.

6.1 EJERSKAB OG VEDLIGEHOLDELSE AF STANDARDEN

Ingen bemærkninger til dette punkt.

6.2 OPHØR OG FRATAGELSE

Ingen bemærkninger til dette punkt.

6.3 ANSVAR OG FORSIKRING

Signaturgruppen

Kommentar:

Det ser generelt ud til, at ansvarsbeskrivelsen er bredere end hvad der kendes for OCES og digital signatur, og den tilhørende finansielle risiko dermed vanskeligere at kvantificere i forhold til forsikringsdækning.

Svar:

Forslaget er indarbejdet i standardens tekst.

Til eksempel er CA i OCES CP afsnit 6.4 ansvarlig for ”at oplysningerne angivet i certifikatet ikke var korrekte på tidspunktet for udstedelsen af certifikatet”. I NSIS lægges der op til eID leverandørerne er ansvarlig for ”at oplysninger i eID/esignatur eller SAML token er forkerte”, hvilket særligt for SAML baserede tjenester vil medføre ekstra ansvar og økonomiske risici for eID leverandøren, idet udstedelsen af tokens almindeligvis foregår kontinuert på basis af delvis dynamiske data.

Det anbefales, at eID leverandørernes ansvar præciseres så meget som muligt, og fokuseres på forhold, hvor leverandørerne har størst mulighed for at inddæmme risici ved at implementere kvalificerede processer og drift.

Kombineret med kravet om en erhvervsansvarsforsikring i størrelsesorden 10 millioner kr. gør ansvarsforholdene det nok urealistisk at indmelde f.eks. kommunalt eller regionalt baserede ADFS baserede brokere eller føderationer på niveau betydeligt eller højt. Da det jo er meget vigtigt at NSIS følger den fælleseuropæiske standardisering, er det dog nok vanskeligt at indføre nationale undtagelser for at udbrede anvendelsesområdet.

6.4 OMKOSTNINGER

Sundhedsdatastyrelsen

Kommentar:

"Alle omkostninger til opretholdelse af kravene i standarden afholdes af eID-tjenesteyderen". Opretholdelse skal erstattes af ”overholdelse”

Svar:

Forslaget er indarbejdet i standardens tekst.

6.5 DELING AF SIKKERHEDSHÆNDELSER

NETS

Kommentar:

govCERT¹ er ikke en myndighed, men en del af forsvaret efterretningstjeneste under center for cybersikkerhed. Eksemplet bør slettes.

Svar:

Forslaget er indarbejdet i standardens tekst.

7. REFERENCER

Ingen bemærkninger til dette punkt.

8. HØRTE PARTER

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

ATP

Danske Regioner

Datatilsynet

DI Digital

DK-Cert

Finansrådet

Ingeniørforeningen, IDA

Justitsministeriet

KL/KOMBIT

København's Kommune, Økonomiforvaltningen

København's Kommune, Børne og Ungeforvaltning

Lakeside

NETS

Peercraft

Rådet for digital sikkerhed

Signaturgruppen

Skatteministeriet

Sundhedsdatastyrelsen

Styrelsen for it og læring

Trafik og Byggestyrelsen

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

Miljø- og Fødevareministeriet

Erhvervs- og Vækstministeriet

Uddannelses- og Forskningsministeriet

Forsvarsministeriet

Finanstilsynet

Sikkerhedsstyrelsen