DemTech/DIGST/Report 1 (dansk)

DemTech Group

DemTech
Democracy, Technology & Trust

DemTech Group
Denmark
CVR: 35527052

Review
Fase 3 Scenarie analyse: oplæg til beslutninger

Carsten Schürmann, David Basin
Februar 2015

DemTech/DIGST/Report 1
(dansk)
Januar 2015

Review
Fase 3 Scenarie analyse: oplæg til beslutninger

Carsten Schürmann, David Basin
DemTech Group
Ribegade 19 st th
DK - 2100 Copenhagen
Denmark

Inholdsfortegnelse

1 Ledelsesresumé

Vi har i foreliggende rapport analyseret tre scenarier for den næste generation af NemID, som er udarbejdet af Rambøll Consulting Management og Implement Consulting Group for Digitaliseringsstyrelsen. De tre scenarier er blevet analyseret fra forskellige interessenters perspektiver; brugernes (fx borgerne og ansatte i virksomheder og offentlige institutioner), beslutningstagernes, de juridiske myndigheders, leverandørernes og administratorernes. Rapporten fokuserer på, i hvilken grad det i de tre scenarier er muligt at opfylde de vigtigste krav til den næste generation af NemID, herunder funktionelle krav, sikkerhed og brugervenlighed.

De tre scenarier viser en progressiv forbedring af NemID, hvad angår brugervenlighed, fleksibilitet og sikkerhed. Det første scenarie er en udvidet udgave af det nuværende NemID og vurderes ikke at imødekomme fremtidige behov hos borgere, virksomheder og offentlige institutioner i tilstrækkelig grad. Derimod indeholder scenarie 2 og scenarie 3 en række væsentlige forbedringer. Ikke desto mindre indeholder denne analyse en række udfordringer, som vi har klassificeret som enten større eller mindre alt efter i, hvilken grad de påvirker projektet.

Større udfordringer: Disse er enten alvorlige problemer eller mangler, som gør det vanskeligt at analysere og forudse konsekvenserne af systemdesignet. Det er altgørende, at der bliver taget stilling til disse udfordringer, før kravspecifikationerne til i den kommende generation af NemID bliver udarbejdede for at undgå efterfølgende korrektioner, som formodentlig vil medføre store udgifter.

Mindre udfordringer: Disse er mindre alvorlige udfordringer, som omfatter punkter, der er blevet overset eller områder, hvor der er oplagte muligheder for forbedringer. Disse udfordringer bør tages i betragtning inden færdiggørelsen af kravspecifikationerne.

Følgende er eksempler på de større udfordringer, som er identificeret i rapporten:

Manglende information: De tre scenarier skelner mellem autentifikation og autorisation, dvs. NemID i forhold til andre infrastrukturer som fx NemLog-in. Denne skelnen giver logisk mening og beskrivelser af både NemID og NemLog-in bør indgå i de tre scenarier. Det er nødvendigt, fordi formuleringen af attributter i forbindelse med autentifikation (fx identitet, virksomhedernes rolle og andre legitimationsoplysninger) er altafgørende.

Det er ligeledes vigtigt at overveje, hvilke andre kontekstuelle oplysninger (om fx autentifikationsprocedurens kapacitet), som er til tilgængelige. Dette bør afklares i forbindelse med analyser af kravene til systemet. En forståelse af samspillet mellem autentifikation og autorisation er fx også nødvendig for bestemmelser i forhold til, hvordan nøgler og privilegier skal kunne tilbagekaldes eller hvordan NemLog-in-rettighederne administreres internt i virksomheder.

Uden yderligere detaljer om autorisation og rettighedsinformations-tjenesterne er det ikke muligt at vurdere, hvorvidt signaturene i fremtidens NemID kan accepteres som bindende. Det afhænger bl.a. de mekanismer, som skal sikre en hensigtsmæssig tilbagekaldelse af rettigheder og nøgler. Det er heller ikke muligt at vurdere, hvordan systemdesignet påvirker brugervenligheden, omkostningerne og interoperationaliteten etc.

Produktion og håndtering af private nøgler: De nøgler, som bliver brugt til at signere digitalt, bliver genereret af en tredje part og er derfor ikke udelukkende kontrolleret af den enkelte bruger. Dette rejser en række spørgsmål om nøglernes egnethed i forhold til de juridisk bindende digitale signaturer.

Utilstrækkelige eller manglende krav: Privacy er et bredt område, som der kun tages stilling til i begrænset omfang i scenarie 3, som beskriver en maskering af personlige attributter. Flere af de standardiserede krav på dette område indgår ikke i scenariet. Fx vil det være muligt for en leverandør eller tjenesteudbyder at overvåge brugernes transaktioner samt at identificere, hvilke personer og virksomheder en given bruger interagerer med.

Potentielle sikkerhedsproblemer: Det nuværende NemID har flere svagheder i forhold til sikkerhed, fx i forhold til de såkaldte man-in-the-middle-attacks og angreb på kompromitterede klientsystemer, hvor kriminelle kan autentificere sig som brugere af forskellige services, ligesom de også vil kunne signere dokumenter som brugere. Uden konkrete tiltag i protokollerne på dette område, er det sandsynligt, at den fremtidige generation af NemID også vil blive sårbar overfor sådanne og lignende angreb. Hvis ikke man bruger Hardware Security Modules (HSM's), risikerer man endvidere også angreb på specifikke brugere samt kompromittering af brugernes privatnøgler.

Vi vil gerne understrege vores bekymringer i forhold til sikkerheden i den næste generation af NemID. Generelt er følgende nødvendigt i forhold til at kunne argumentere for sikkerheden i et system:

(1) En præcis beskrivelse af, hvilke sikkerhedsmæssige udfordringer, som systemet skal kunne modstå.

(2) En specificering af, hvilke former for modstandere (eller potentielle trusler), som systemet bør beskyttes imod. Det kan fx være om et givent system skal kunne modstå interne eller eksterne angreb, om det skal kunne modstå forsøg på at kompromittere et klientsystem (fx man-in-the–browser-attacks eller aflæsning af nøglerfiler på en harddisk) eller hvorvidt en potentiel modstander (the adversary) vil være i stand til at lave en kryptoanalyse af svage nøgler etc.

Vi finder ikke ovenstående punkter tilstrækkeligt beskrevet i de modtagne dokumenter. Endvidere savner vi også:

(3) En rationel og udførlig begrundelse for, hvorfor systemets sikkerhedsmæssige egenskaber er tilstrækkelige i forhold til den forventede trussel.

I de gennemgåede dokumenter, bliver der i de tre scenarier sporadisk refereret til forskellige former for sikkerhedsløsninger. Med vekslende detaljeringsgrad bliver der eksemplificeret for at vise, at de komponenter, som skal udgøre infrastrukturen i fremtidens NemID, er modstandsdygtige, og at de vil fungere under angreb. I denne sammenhæng er beskrivelserne i de tre scenarier ikke fyldestgørende, og det anbefales, at der fremadrettet tages stilling til manglerne i de tre ovenstående punkter.

I alle tre scenarier er det et eksplicit mål at involvere forskellige tjenesteudbydere, identitetsgaranter og brokers. Vi vil gerne understrege, at det i denne forbindelse er nødvendigt at udarbejde præcise kravspecifikationer. En underspecifikation vil fx øge risikoen for, at én tjenesteudbyder vil kunne inkorporere elementer, som tjenesteudbyderen selv har designet, i den nye version af NemID. Dette vil efterfølgende kunne gøre det vanskeligt for andre udbydere at konkurrere, bl.a. fordi de vil blive nødt til at implementere tjenesteudbyderens protokoller. Derfor bør alle versioner være interoperationelle, hvorved man også vil imødekomme fremtidige rettighedsspørgsmål (fx intellectual property). Disse udfordringer imødekommes bedst ved udarbejde de nødvendige specifikationer forud for udbudsprocessen.

Vi anbefaler, at Digitaliseringsstyrelsen behandler de større udfordringer og overvejer de mindre i forbindelse med udarbejdelsen af kravspecifikationerne forud for et efterfølgende udbud. Vi har i det følgende udarbejdet nogle retningslinjer i vores anbefalinger, som, vi håber, kan være til nytte i denne proces.

2 Baggrund og formål

Grundlaget for vores analyse af de tre scenarier for den næste generation af NemID er disse dokumenter, som blev modtaget d. 12. januar, 2015:

- Næste generation af NemID, Fase 3 Scenarie analyse: oplæg til beslutninger [1].
- Bilag 1: Afdækning af relevant funktionalitet i den eksisterende NemID for næste generation NemID.
- Bilag 2: Til scenarie 2 – Virksomhedsområdet.

Dokumentet, som vedrører fase 3, samt Bilag 2 er blevet udarbejdet af Rambøll Consulting Management og Implement Consulting Group. Bilag 1 er udarbejdet af Digitaliseringsstyrelsen. Dokumentet, som vedrører Fase 3, har til hensigt at fungere som beslutningsgrundlag og må derfor betragtes som helt centralt i forhold til udarbejdelsen af de kravspecifikationer, som vil blive væsentlige i forhold til den fremtidige indkøbsproces. Dokumenterne beskriver de tre scenarier på basis af input fra interessenter og høringsvar, som styregruppen har indsamlet.

Det er vigtigt at understrege, at vi i denne analyse ikke har til hensigt at udarbejde selve kravspecifikationerne, systemdesignet (design documents) eller en forundersøgelse (feasibility study). Vi har heller ikke undersøgt, hvordan den næste generation af NemID vil interagere med fremtidige generationer og andre services som fx NemLog-in, ligesom vi heller ikke har beskæftiget os med de økonomiske aspekter.

3 Scenarie 1

3.1 Overblik

Dette scenarie er en mindre revision og udvidelse i forhold til det nuværende NemID: De private nøgler opbevares centralt på leverandørernes servere. I scenariet bliver kun 2 factor-autentifikation understøttet via passwords og et standard challenge response scheme. Det understøtter fortsat NemID borger og NemID medarbejdersignatur (dvs. både borgere og virksomheder). Den mindre udvidelse består i at muliggøre brugen af Hardware Security Modules (HSM's) og forbedringer i forhold til systemets brugerinterface.

3.2 Udfordringer

Det fremgår af dokumentet (1), at scenariet ikke imødekommer mange af interessenternes ønsker, og at dette scenarie derfor ikke bør tages op til yderligere overvejelse. Vi bakker dette synspunkt op.

3.2.1 Større udfordringer

De samme nøgler bruges til signering og autentifikation: Hver bruger er i besiddelse af et nøglepar (bestående af én offentlig og én privat nøgle). Den private nøgle bliver brugt i forbindelse med både signering og autentifikation. Det er dårlig sikkerhedspraksis. De forskellige nøgler bør brugt til forskellige formål og specielt bør nøglen, som bliver brugt til autentifikation, holdes adskilt fra nøglen, som bliver brugt til at signere med. Hvis den samme nøgle kan bruges til signering og autentifikation, er det muligt for en modstander (adversary) at udnytte dette til at narre en bruger til uforvarende at signere data eller dokumenter. Yderligere oplysninger om disse risici og best practices for Key Management findes i kapitel 5 (litteraturhenvisningen), *Recommendation for key management - part 1 (revision 3)* [2].

Anbefalinger: I forbindelse med signering og autentifikation bør der bruges separate nøgler. Scenarie 1 understøtter ikke denne separation, hvilket i sig selv er et stærkt argument for, hvorfor der ikke bør arbejdes videre med dette forslag som en løsning til den kommende generation NemID.

Avancerede elektroniske signaturer: Vi mener, at de foreliggende dokumenter bør indeholde overvejelser af alternativer til nuværende løsning med centralt opbevarede nøgler på tjenesteudbydernes(fx Nets) servere, fordi man i sådanne overvejelser vil skulle forholde sig til den tiltagne digitalisering af services i Europa samt det fremtidige online-trusler.

Et af alternativerne til den nuværende løsning er at sikre, at den enkelte borgers offentlige/private nøglepar bliver genereret på brugernes egne kryptografiske hardware og at private nøgler aldrig adskilles fra denne hardware.

Kontrollen af nøglerne er et gennemgående problem i alle tre scenarier, hvor central opbevaring af nøgler og nøglefiler er muligt. Vi er bekymrede i forhold til, at der i beskrivelsen af de tre scenarier ikke bliver taget stilling til i hvilken udstrækning, det er sandsynligt, at det nye NemID vil være foreneligt med fremtidige EU-direktiver. Hvis det nye NemID ikke lever op til fremtidige EU-direktiver kan det blive nødvendigt at redesigne NemID, hvilket vil betyde øgede udgifter, og det kan have en negativ effekt for danske virksomheder, som handler på det europæiske marked.

Anbefaling: Når kravene for den næste generation af NemID skal udarbejdes, bør det genovervejes, hvor de private nøgler, som skal bruges til signering, skal genereres og opbevares, og hvorvidt en central opbevaringsløsning er den bedste løsning. Bemærk venligst at vores bekymring kun vedrører nøgler, som bruges til signering. For nøgler til autentifikation er dette ikke nødvendigt i samme omfang og her er andre (og mindre sikre) løsninger mulige, deriblandt central opbevaring, opbevaring i nøglefiler og opbevaring på tjenesteudbydernes servere.

4 Scenarie 2

4.1 Overblik

I scenarie 1 og 2 bliver de private nøgler genereret af og opbevaret på identitetsgarantens server. Forskellen mellem de to scenarier er, at der i scenarie 2 er forskel mellem de nøgler, som skal bruges til autentifikation og signering. Hver borger får to private nøgler, som begge opbevares på identitetsgarantens server. Det er en forbedring i forhold til scenarie 1, fordi det forhindrer tilfælde, hvor der på ulovlig vis bliver signeret på en brugers vegne.

I scenarie 2 præsenteres forskellige sikkerhedsniveauer, især 1-factor autentifikationen, som giver borgerne nemmere adgang og dermed en bedre brugeroplevelse. Det beskrevne design vil gøre det muligt for andre serviceudbydere (specielt bankerne) at genbruge specifikke NemID-funktioner og at tilbyde tillægsservices så som konto-kig.

Sidst introduceres der i scenarie 2 et nyt komponent til NemID's infrastruktur; rettighedsinformationstjenesterne. Her kan NemID borger blive konfigureret til at erstatte NemID medarbejdersignatur, hvilket vil forbedre brugeroplevelsen og nogle områder af administrationen i forhold til scenarie 1.

4.2 Udfordringer

I forhold til scenarie 1, løser scenarie 2 problemet med at bruge de samme nøgler til autentifikation og signering. En af udfordringerne i forhold til scenarie 1, nemlig kravene til de digitale signaturer, gælder imidlertid også i forhold til scenarie 2. I nedenstående beskriver vi de yderligere udfordringer:

4.2.1 Større udfordringer

Administration af rettigheder: I Scenarie 2 (og scenarie 3) samt bilag 2 introduceres rettighedsinformationstjenesterne, som inkluderer delegation, i den næste generation af NemID. Dette er nødvendigt, for når forretnings-mæssige og personlige nøgler blandes, og der kun udstedes et nøglepar per borger, skal systemet vide, i hvilken egenskab en borger/medarbejder bruger NemID for at kunne administrere rettighederne hensigtsmæssigt. Spørgsmålet er, hvilken effekt rettighedsinformationstjenesterne vil have ikke bare på NemID, men også på andre systemer, i særdeleshed NemLog-in.

Rettighedsinformationstjenesterne giver virksomheder og forvaltninger mulighed for at definere og kontrollere en given brugers privilegier, således at den enkelte bruger kan gennemføre tiltag på deres vegne. I den forbindelse skal man være opmærksom på, at validiteten af en signatur ikke blot afhænger af, hvorvidt en given bruger vil kunne signere et dokument, men også af i hvilken udstrækning det er juridisk dokumenterbart, at det er den givne bruger, som har signeret dokumentet og at vedkommende er autoriseret til at signere det. Blandt de fagfolk, som arbejder med access control, er sådanne management-løsninger blevet studeret intensivt, og der er blevet udviklet mange løsningsmodeller på området. Generelt er der en tendens til, at der i forhold til disse løsninger synes at være afvejning mellem fleksibiliteten og kapaciteten på den ene side og brugervenligheden på anden. Hvor svært er det fx at specificere og vedligeholde retningslinjerne for autorisationen? Hvis man skal bedømme tilstrækkeligheden af en given løsning, kræver det, at egenskaberne er præciserede. Dette er ikke tilfældet i scenarie 2, B.

Vi vil gerne understrege, at rettighedsinformationstjenesterne er afgørende for sikkerheden i den næste generation af NemID. Det er også meget vigtigt, at designet er brugervenligt, især fordi de brugere, som er ansvarlige for at administrere rettighederne ikke kan forventes at have udpræget erfaring på dette område. Endvidere bemærker vi, at designet af den næste generation af NemID og NemLog-in må hænge sammen. Interaktionen mellem de to systemer er subtil og ændringer ét sted vil let medføre problemer i forhold til tidligere design.

Anbefaling: Kravene til rettighedsinformationstjenesterne kan ikke udarbejdes isoleret, fordi de påvirker kravene til andre komponenter, designet og implementeringen af disse, administrationen og brugeroplevelsen. De skal derfor udvikles sammen med scenarierne.

Trusselsanalyse (adversary model): Fraværet af en trusselsanalyse gør det vanskeligt at evaluere sikkerheden i scenarie 2. Vi kan kun gætte på, at en ny og mere strømlinet generation af NemID vil være attraktivt for tjenesteudbydere, hvilket kan skabe opmærksomhed blandt it-kriminelle. Det er også oplagt, at 1-faktor-autentificeringen kan føre til flere tilfælde af identitetstyveri.

Anbefaling: En trusselsanalyse, som kan indgå i overvejelser vedr. sikkerhed, bør udarbejdes.

4.2.2 Mindre udfordringer

Tilgængelighed: I dette scenarie beskrives en distribueret arkitektur for NemID, som består af brokere og identitetsgaranter (se detaljer i (1) kapitel

8). Afhængigt af hvordan systemet implementeres, kan brugernes tilgængelighed øges, fordi antallet af brokere betyder, at der er mange udbydere til de samme services. Tilgængeligheden kan også blive reduceret, hvis en tjenesteudbyder kun bruger en enkelt broker – og hvis denne ene broker fejler, vil det have negative konsekvenser for tjenesteudbyderen. Derfor afhænger meget af, hvordan systemet bliver designet. Dokumentet indeholder ingen forslag til eller diskussioner om, hvordan man vil kunne sikre en hensigtsmæssig tilgængelighed.

Anbefaling: Kravene til systemets design bør indeholde en beskrivelse af de foranstaltninger, som skal sikre tilgængelighed. Denne beskrivelse bør omfatte, hvilke rammer man vil opstille i forhold til identitetsgaranter, brokere (fx i forhold til mirroring, redundans, load balancing) og tjenesteudbydere (fx at der skal være en backup-broker, hvis den primære broker ikke leverer).

Kryptografiske muligheder: Der er mange forskellige måder, hvorpå man vil kunne bruge kryptografi i forhold til autentifikation og signering. I forhold til autentifikationen er det muligt at bruge symmetrisk og asymmetrisk kryptografi. Mht. asymmetrisk kryptografi er der forskellige muligheder for implementering, fx RSA og elliptiske kurver. Hvis nøglerne bliver opbevaret centralt, vil antallet af tillidsskabende faktorer måske kunne reduceres ved brug af teknikker som fx keysharing. Der bliver ikke taget stilling til sådanne muligheder. Andre muligheder bliver kun overfladisk og inkonsekvent behandlet. Fx bliver Yubikey bliver nævnt i scenarie 3. Yubikey bruger symmetrisk kryptografi, som ellers ikke er yderligere beskrevet. Samlet set vurderer vi, at de tekniske deltaljer er utilstrækkelige i betragtning af formålet med dokumentet.

Anbefaling: Der mangler et rationale i forhold til understøttelsen af kryptografiske muligheder og de tilhørende kryptografiske protokoller bør blive specificeret i efterfølgende dokumenter om systemdesignet (design documents).

5 Scenarie 3

5.1 Overblik

Scenarie 3 indeholder – ud over tre elementer, som allerede er blevet præsenteret i scenarie 2 – et element, som gør det muligt at begrænse tjenesteudbydernes adgang til personlige informationer, alt afhængig af, hvem tjenesteudbyderen er og til hvilket formål tjenesteudbyderen skal bruge informationerne. Dette element er udviklet for at beskytte borgernes privatliv i videst muligt omfang med det in mente, at ikke alle personlige oplysninger vil kunne være hemmelige.

Det andet nye element muliggør tilføjelse af login-faktorer, fx HSM's deriblandt Yubico Security Key. I scenariet anslås det, at der er et stigende behov for sådanne muligheder, specielt hos større virksomheder, som er afhængige af en høj sikkerhed i infrastrukturen. Og ja; hvis den korrekte hardware er understøttet, kan det højne hele sikkerheden i NemID's infrastruktur. Hvis alle borgere havde en HSM konfigureret med deres egne respektive private nøgler til autentifikation og signering, vil det forbedre sikkerheden i NemID.

Det tredje element, som er særegent for scenarie 3 omhandler ikke det tekniske design, men handler om måder, hvorpå servicen vil kunne optimeres i forhold til ressourcer, økonomiske rammer etc.

5.2 Udfordringer

5.2.1 Større udfordringer

Beskyttelse af personlige oplysninger: Privacy er et komplekst begreb, som der i Scenarie 3 kun bliver taget overfladisk stilling til. Vi forventer, at de involverede parter (borgere, politikere, virksomheder og andre interessenter) generelt er bekymrede i forhold til beskyttelse af personlige oplysninger om, hvem de interagerer med og hvordan de interagerer med andre. Fx skal borgerne gerne kunne bruge forskellige services uden at andre parter, herunder identitetsgaranterne, får viden derom, ligesom tjenesteudbyderne gerne vil have, at oplysninger om, hvem deres kunder er, ikke deles med andre parter.

Der er en tendens til, at privacy betragtes som et snævert spørgsmål om at maskere specifikke brugerattributter. Her bør det holdes for øje, at identitetsgaranten (fx Nets) kan observere og relatere transaktioner og

derved indhente informationer, som fortæller meget om NemID-brugernes adfærd. Det samme er tilfældet for andre parter, fx ISP's (Internet Service Providers).

Andre udfordringer i forhold til beskyttelse af personlige oplysninger bliver slet ikke beskrevet. Formodentlig logger identitetsgaranterne, brokerne og tjenesteudbyderne de transaktioner, som de behandler. Hvordan bliver disse oplysninger beskyttet, og hvornår bliver de slettet? Hvilke mekanismer vil man bruge for at beskytte personfølsomme oplysninger i forhold til logning og i forhold til at sikre, at loven bliver håndhævet?

5.2.2 Mindre udfordringer

Billigere og bedre support: I Element F anslås det, at man i den nye generation af NemID vil kunne yde billigere og bedre support. Vi ser dette som et prisværdigt ønske, men vil gerne se en bedre argumentation for, at det rent faktisk er muligt. Afhængigt af rettighedsinformationstjenesternes design kan den valgte løsning blive vanskelig at konfigurere og bruge. I mangel af flere detaljer, vil vi bemærke, at det modsatte vil kunne blive tilfældet, og at supporten vil kunne blive dyre, før den vil blive bedre.

Anbefaling: En genovervejelse af dette punkt anbefales, når der foreligger flere detaljer om løsningen til rettighedsinformationstjenesterne.

Rationale i forhold til design: I den samlede selvevaluering skrives der, at designet vil skabe større tillid til NemID. Vi er bekymrede for, at dette ikke bliver tilfældet. Den omstændighed, at brugeren skal bruge NemID, hvis vedkommende fx skal have adgang til et casino eller et andet sted, som vil tjekke, at alle gæster er over 18 år, vil formodentlig blive betragtet som en krænkelse af privatlivets fred, også selv om det bliver lovet, at det kun er oplysninger om alder, som afsløres. Som det bliver noteret i scenarie 3, vil det ydermere være muligt for en tjenesteudbyder (i dette tilfælde Casinoet) at kræve yderligere oplysninger. Med mindre der er mekanismer, som forhindre dette (fx at det bliver muligt for borgerne at specificere deres egne præferencer i forhold til beskyttelse af deres personlige oplysninger, og at de har sikkerhed for, at disse præferencer respekteres) vil dette potentielt kunne skabe mistillid hos borgerne.

6 NemID til børn

6.1 Overblik

Dette scenarie er tænkt som en parallel i forhold til de andre tre scenarier. NemID til børn er i højere grad baseret på infrastrukturerne i scenarie 2 og 3 end scenarie 1. Børn under 15 år er ikke gamle nok til selv at kunne signere, og derfor kræver det, at autentifikationen separeres fra signeringen.

6.2 Udfordringer

Udstedelse af NemID til børn: Dette scenarie er ikke overbevisende i forhold til, hvorfor NemID til børn overhovedet er nødvendigt i Danmark. Fordelene ved at børn under 15 år vil kunne autentificere sig, når de bruger offentlige services som fx biblioteker, står ikke mål med de ulemper, som er forbundet med, at de samtidig vil kunne få adgang til utallige private tjenesteudbydere (måske uden at det var intentionen). En anden bekymring handler om, at forældre, som jo er ansvarlige for deres børn handlinger, er afskåret fra disse handlinger.

Anbefaling: En mere detaljeret analyse af forretningsmodellen for NemID til børn under 15 år bør udarbejdes.

Customization og vedligeholdelse: NemID til børn under 15 år er forskelligt fra det NemID, som vil møde de øvrige borgere. Derfor er det nødvendigt at lave et modificeret system (som endnu ikke er specificeret). Denne tilføjede kompleksitet vil øge udgifterne til implementeringen, ligesom systemet også vil være dyrere og vanskeligere at vedligeholde. Systemet skal konstrueres så det automatisk træffer de nødvendige foranstaltninger, når børnene fylder 16 år, da det ellers vil blive nødvendigt med yderligere foranstaltninger til vedligeholdelse. Disse processer er ikke tilstrækkeligt beskrevet i de analyserede dokumenter.

Anbefaling: En mere detaljeret analyse af forretningsmodellen for NemID til børn under 15 år bør udarbejdes.

Litteratur

[1] Rambøll Management Consulting and Implement Consulting Group. Næste generation af nemid, fase 3 scenarie analyse: oplæg til beslutninger. Draft, January 2015.

[2] Elaine Barker, William Barker, William Burr, William Polk, and Miles Smid. Recommendation for key management - part 1 (revision 3): General. In NIST Special Publication 800-57, National Institute of Standards and Technology, 2013.