Høringssvar

Følgende har afgivet høringssvar:

1. 41concepts
2. Advokatrådet
3. ATP
4. Banedanmark
5. Beskæftigelsesministeriet
6. Bitbureauets
7. CHPCOM Projektet
8. Civilstyrelsen
9. Danmarks Rederiforening
10. Dansk Byggeri
11. Dansk Erhverv
12. DANSK IT
13. Danske Handicaporganisationer (DH)
14. Danske Regioner
15. Datatilsynet
16. Den Uafhængige Politiklagemyndighed
17. DI ITEK
18. Digitalimik Sullissinermut Aqutsisoqarfik
19. Domstolsstyrelsen
20. E-boks
21. Erhvervs- og Vækstministeriet
22. Finans & Leasing
23. Finansrådet
24. Finanstilsynet
25. Forbrugerrådet TÆNK
26. Foreningen for Dansk Internet Handel (FDIH)
27. Forsikring og Pension
28. Forsvarsministeriet
29. Henrik Schack
30. Håndværksrådet
31. Institut for Menneskerettigheder
32. IT-Branchen
33. IT-Politisk Forening
34. Justitsministeriet
35. Kommercielle Linux-interessenter I Danmark (KLID)
36. Kommunernes Landsforening (KL)
37. Konkurrence- og Forbrugerstyrelsen
38. Kulturministeriet
39. Landbrug & Fødevarer og Videncentret for Landbrug
40. Lars Ole Belhage, Bjarne C. Jacobsen og Lars Roark
41. Michael Møller
42. Miljøministeriet
43. Ministeriet for Børn, Ligestilling, Integration og Sociale Forhold
44. NaturErhvervstyrelsen
45. Niels Kleberg
46. Nimish Gautam
47. Odense Kommune
48. Peercraft ApS
49. PFA Pension
50. Projekt UDENFOR
51. Region Syddanmark
52. Rigspolitiet
53. Rådet for Digital Sikkerhed
54. Rådet for Socialt Udsatte
55. SAND
56. SKAT
57. Sorø Kommune
58. Theis F. Hinz
59. Trafikstyrelsen
60. Uddannelses- og Forskningsministeriet
61. Udlændingestyrelsen
62. Undervisningsministeriet
63. Ældre Sagen

41concepts Aps,
Rørholmsgade 22, 4th
1352 København K.

15. Juni 2014

Høringsvar vedr. næste generation af den nationale identifikations- og digital signaturinfrastruktur (NemID)

1. Fremtidige forretningsmæssige behov overordnet

Den nye NemId skal udgøre en åben platform og ikke være et lukket produkt. Platformen skal indeholde åbne platformuafhængige snitflader (Web API'er), som software fra virksomheder, foreninger og tekniske privatpersoner kan koble sig op imod. Det skal muliggøre konkurrence, innovation, universel integration og nem mulighed for små lokale tilpasninger efter behov i de enkelte virksomheder, foreninger og lign.

2. Funktionalitet og anvendelse

Den nye NemId skal indeholde 2 niveauer af sikkerhed, som bl.a. skal mulig-gøre øge brugervenlighed:

A. Læse operation på godkendt enhed. F.eks. tilgå e-post[1] og sine informationer på borger.dk på sin private telefon uden brug af nøglekort. Dette niveau er uden 2-faktor sikkerhed, men med en simpel applikations-specifik adgangsbeskyttelse el. evt. uden kode, som i en App på en låst mobil, hvor brugeren i forvejen skal låse mobilen op med kode for at tilgå App'en. Kræver en tidligere niveau-B godkendelse for at fungere.
B. Godkende, skrive under, autorisere el. deautorisere personligt udstyr som telefoner, tablets og lign. til at læse på. Vil altid kræve 2-faktor sikkerhed, men præcist hvordan det sker er applikations-specifik.

3. Behov fo brugervenlighed.

Systemet skal være meget, meget mere brugervenligt end det er i dag. Men det opnås ikke ved, at designe ét statisk (frontend) produkt med ét på forhånd bestemt antal krav. Der skal mere til for at NemID ren faktisk bliver nemt at bruge både nu og i fremtiden.

I stedet skal der designes en åben platform (se pkt. 1) med 2-niveauer af sikkerhed (se pkt. 2). På dette grundlag kan forskellige leverandører, så konkurrere om det bedste - herunder mest brugervenlige - produkt. Konkurrence, innovation og brugernes frie valg vil sikre den bedst

[1] Undertegnede kender ingen, der gider at læse deres e-post regelmæssigt, fordi det er for besværligt. En ikke så brugervenlig NemID er en væsentlig årsag. Manglende udbud og konkurrence på frontend Apps til ePost er en anden vigtig årsag. F.eks. mangler Apps helt til brug for virksomheder til at læse deres post.

mulig brugervenlighed i den færdige løsning. Den åbne platform vil også give bedste mulighed for god brugervenlighed også i fremtiden, når brugsmønstre ændre sig.

4. Teknik og infrastruktur.

Som nævnt i pkt. 1 skal den nye NemId udgøre en åben platform og ikke være et lukket produkt. En platform, som software fra forskellige leverandører og privatpersoner kan koble sig op imod. En åben platform hvor sikkerhed baserer sig på velprøvede og sikre dele som kryptering, SSL m.m. og ikke myter om "security by obscurity", der også tilfældigvis samtidigt passer i visse leverandøres kram om at undgå ubehagelig konkurrence ved at lukke alt til.

Som nævnt i pkt. 2 skal platformen understøtte adgange på flere niveauer, hvilket kræver forskellige autorisering op mod servere.

A. Kan ske ved en tidligere downloadet token/nøgle, som er givet (evt. tidsbegrænset) via en tidligere Niveau B godkendelse + evt. password med mindre adgangen er sikret på anden vis (f.eks. er det unødvendigt med password i applikationen, hvis brugeren har åbnet sin telefon ved fingeraftryk el. personligt password).
B. Sker via password + engangskode som i dag eller ved Biometri, som nyeste mobiltelefoner m.m. er begyndt at understøtte. Begge metoder skal understøttes af et fleksibelt API. Således vil eID og eSignering også være adskilt.

Arkitektturen i softwaren i platformen skal være modulopdelt med åbne snitflader imellem moduler, således at enkelte moduler kan skiftes ud og evt. leveres af forskellige leverandører. Det vil også mindske risiko for NemID projektet og åbne op for at flere leverandører kan deltage. Bemærk dog, at det er vigtigt, at der stilles store krav til testability(!!) i arkitekturen, designet og koden (herunder testabiliy ind i snitfladers design, logging o.s.v.), så man ikke ender i et SOA-helvede med systemer fra 7 forskellige leverandører, der ikke kan snakke sammen og man kan ikke umiddelbart finde ud af hvorfor (noget jeg ved der tit sker i det offentlige når der er flere forskellige systemer og leverandører)

Sammen med den udviklede platform skal et offentligt tilgængeligt Software Development Kit (SDK) med eksempler på frontend løsninger frigives, som understøtter førende mobilplatforme, tablets og computere. Central kode kan med fordel skrives i "C", som understøttes af alle platforme… Mange ved det ikke, men man kan faktisk skrive sin forretningslogik (f.eks. krypteringsdelen) i "C" og hermed understøtte alt, herunder Windows mobile Apps, iOS Apps til iPhone/IPads, Android native apps, Mac OS X, Windows, Linux og så videre…. Bemærk dog at man desværre ikke kan skrive alt i "C" på nogle af platformene, så f.eks. GUI'en skal skrives specifikt til de fleste platforme – men GUI'en er heller ikke en del af SDK'erne.

Løsningen skal endeligt ikke basere sig på Java[2] el. Javascript på klienten som er tungt, besværligt, kræver for meget datatrafik og hverken er fleksibelt, sikkert, robust nok el. understøtter de brugervenlige anvendelser, der skal til. I stedet bruges SSL, kryptering, forms og andre standard-teknologier samt native Apps via SDK'er.

[2] Java hører hjemme på serven, hvor det fungere godt - ikke på klienten.

5. Samspil med interessenter

I den åbne platform med åbne API'er, fri konkurrence og hermed stor innovation vil de fleste frontend løsninger (og hermed leverandører) udskiftes af borgere ud fra deres frie valg. På backend'en vil der være brug for 1+ stabile leverandører til driften.

6. Fremtidig forretningsmodel

Som nævnt i ovenstående er der brug for en model baseret på fri konkurrence på alle frontend systemer og flere løbende leverandører. Efter sigende har man i UK noget af det samme, men vist ikke helt så åbent.

7. Andre bemærkninger

Tak for muligheden for at give input. Jeg kan kontaktes for yderligere information og afklaringer.

Mvh

Morten Christensen, M.Sc, CEO i 41concepts, tlf. 40 10 92 38, mmc@41concepts.com

Advokatrådet

ADVOKAT SAMFUNDET

Digitaliseringsstyrelsen
Landgreven 4
Postboks 2193
1017 København K

kis@digst.dk

KRONPRINSESSEGADE 28
1306 KØBENHAVN K
TLF. 33 96 97 98
FAX 33 36 97 50

DATO: 2. juli 2014
SAGSNR.: 2014 - 1580
ID NR.: 300677

Høring- over næste generation af den nationale identifikations- og digital signaturinfrastruktur (NemID)

Ved e-mail af 28-05-2014 har Digitaliseringsstyrelsen anmodet om Advokatrådets bemærkninger til ovennævnte.

Advokatrådet finder ikke grundlag for at udtale sig i sagen.

Med venlig hilsen

Torben Jensen

Til Digitaliseringsstyrelsen

26. juni 2014

Høringssvar – Høring om næste generation af den nationale identifikations- og digital signaturinfrastruktur (NemID)

Hermed fremsendes ATP's bemærkninger til 'Høring om næste generation af den nationale identifikations- og digital signaturinfrastruktur (NemID)'.

NemID er en forretningskritisk komponent for ATP's løsninger og har en afgørende betydning for, at ATP kan drive en effektiv digital kundeservice. Generelt har der været god tilfredshed med den eksisterende NemID og en høj volumen af transaktioner.[1] Der er dog visse erfaringer fra den nuværende løsning, som ATP ønsker at adressere under de enkelte høringstemaer.

Fremtidige forretningsmæssige behov

ATP har i erfaringsopsamlingen identificeret barrierer for fuld digital kommunikation med borgere, der opholder sig i udlandet og udenlandske virksomheder der modtager ydelser i forbindelse med anvendelsen af den nuværende NemID løsning.[2] Anvendelse af digital post er knyttet sammen med anvendelsen af den nuværende NemID-løsning. Som situationen ser ud i dag har ca. 55 pct. af borgerne nævnt ovenfor ikke et dansk pas og kan derfor ikke få tildelt NemID. Hertil kommer, at de resterende 45 pct., som har et dansk pas og ikke i forvejen har NemID, kun kan få en sådan udstedt ved fysisk fremmøde på en dansk repræsentation i udlandet, for at sikre autenciteten af den person NemID udstedes til. Samme udfordring har udenlandske og grønlandske virksomheder, der skal søge om danske ydelser. Et eksempel er NemRefusion, hvor sagen skal håndteres manuelt, da virksomheden ikke kan få tildelt en medarbejdersignatur uden et dansk CVR-nummer.

ATP skal endelig gøre opmærksom på, at der er en juridisk barriere for at udbrede *obligatorisk* anvendelsen af NemID. Hvis man vil gøre nationale forhold/lovgivning gældende uden for Danmarks grænser, kan det have virkning som indirekte diskrimination, ikke mindst hvis der i tilgift er ekstra omkostninger ved det for borgeren.

[1] I 2013 var der ca. 2,4 mio. "log ind" vedr. Udbetaling Danmark og 1,8 mio. "log ind" vedrørende Pension og Sikring. Alt i alt ca. 4,2 mio. "log ind" i 2013.
2 ATP har i ordningerne ATP-livslang pension 16.500 borgere i udlandet der modtager ydelser, Familieydelser har ca. 10.000 og International Pension og Social Sikring (IPOS) har 48.000. I alt sender ATP ca. 150.000 breve om året til disse modtagere, og tallet er stigende.

Behov for brugervenlighed

ATP har identificeret et behov for en brugervenlig løsning til fuldmagter (både mellem personer og til firmaer, f.eks. revisorer). ATP foreslår, at alle relevante målgrupper inddrages i de indledende brugeranalyser, så deres forskelligartede behov afdækkes. Den nuværende løsning har en høj kompleksitet på virksomhedssiden, og det giver udfordringer for mindre virksomheder. Det drejer sig specifikt om:

- Tildeling af rettigheder – ønske om mere enkle tilmeldinger for fx enkeltmandsvirksomheder og mindre virksomheder, hvor der gives rettighed til en samlet pakke, som dækker de flestes behov. Der er behov for nemmere adgang til dybe links til siden, hvor rettigheder tildeles og bedre hjælpe-vejledninger med guides og lign. For større virksomheder har løsningen mange fine muligheder, og det er et stort skridt at kunne selvadministrere og tilslutte nye løsninger.
- Fremsøgning af brugeradministrator har tidligere været svært - det bør kun være ét klik væk.
- Begreberne er komplekse og blandes sammen – f.eks. når der skal udpeges rettighed, vises privilegium med en uforståelig tekst. Her burde der i stedet vises teksten for rettigheden: Fx: ”Ret til at tilgå AUB”.
- Det skal fortsat være muligt for administratorer at begrænse brugernes adgang til SE-numre i brugerrettighedsstyrings-systemet.

Samspil med interessenter

Hovedbudskabet i erfaringsopsamlingen vedr. samspil med interessenter på support er:

- Behov for en mere forpligtende driftshåndbog med NemID/NemLog-in og de øvrige offentlige komponenter (fx tilsvarende den ATP har med borger.dk). F.eks. nødprocedurer, når NemID ikke virker, da NemID er indgangen til alle offentlige løsninger.
- Øget fokus på support i forhold til iværksættelser og fejlhåndtering.
- Udfordringer med IT leverandører og tilslutning af ordninger i det nuværende setup.

Fremtidig forretningsmodel

ATP har identificeret følgende behov i den fremtidige forretningsmodel:

- Deadlines for fx NemLog-in blev udskudt flere gange inden lancering – det gav usikkerhed hos de involverede og problemstillinger med ressourcer.
- Efter lancering af NemLog-in manglede adgang til nyt testmiljø og viden om, hvordan dette benyttes. Der er behov for at have test-CPR-numre, som kan bruges i forbindelse med test af NemID.
- Der har været udtrykt behov for udarbejdelse af en kommunikationsplan tidligt i projektet herunder vejledninger og uddannelsesmateriale på NemLog-in. Fremadrettet vil dette være et oplagt område at sætte ind således, at tilstrækkeligt vejledningsmateriale/guides foreligger i god tid inden lancering.

banedanmark

Notat 27.06.2014

Offentlig høring om næste generation af den nationale identifikations- og digital signaturinfrastruktur(NemID)

Hermed Banedanmarks bemærkninger til høringen indenfor de angivne temaer:

1. Fremtidige forretningsmæssige behov, for henholdsvis virksomheder, offentlige sektor og borgere i Danmark og udlandet samt eventuelle juridiske forhold.

Der er for nærværende ikke forretningsmæssige behov for yderligere anvendelse af NemID. Det nuværende behov er som følger:

Banedanmark anvender medarbejdersignatur til følgende:

- NEM Konto
- NEM Refusion
- Udbetaling Danmark
- CVR
- SKAT
- Virk.dk
- FerieKonto
- ATP
- Høringsportalen

De nuværende funktioner anses som dækkende.

2. Funktionalitet og anvendelse, herunder eksempelvis niveaudelt sikkerhed, lokal administration af autorisation, single sign-on mv.

- Muligheden for single sign-on vil være en lettelse i det daglige i forbindelse med de funktioner, der anvendes i stort omfang. Der er ikke konstateret behov for større niveaudeling.

3. Behov for brugervenlighed, herunder forskellige brugeres aktiviteter fra bestilling til anvendelse og eventuel spærring mv.

- Installationen er i dag acceptabel, men det er vigtigt at have fokus på ikke at gøre denne funktion mere omstændelig.

- Ud fra en administrationsmæssig (LRA) synsvinkel bør en fremtidig løsning være væsentligt mere enkel, mere overskuelig, mere gennemskuelig samt en kende mere brugervenlig, så brugerne kan følge et enkelt og selvinstruerende arbejdsflow.

- I daglig anvendelse opfattes konceptet som let tilgængeligt. Enkelheden i denne del bør fastholdes.

- Det skal være nemt og enkelt gennem hele forløbet, både ved installation og i daglig anvendelse.

4. Teknik og infrastruktur, herunder eksempelvis adskillelse af eID og eSignering, single sign-on, sammenhængende IT-arkitektur, sikkerhed mv.

- Man bør så vidt muligt ikke basere sig på proprietære systemer, produkter eller funktionalitet
- Infrastrukturen bør opbygges således, at "single point of failure" minimeres
- Konsekvenserne ved DDOS-angreb skal minimeres

5. Samspil med interessenter, herunder tjenesteudbydere, administrative procedurer, sikkerhedsprocedurer mv.

- Ingen bemærkninger

6. Fremtidig forretningsmodel, herunder leverandørstyring, support, betalingsstruktur, en model med flere leverandører mv.

- Ingen bemærkninger

De er velkommen til at vende tilbage, hvis dette giver anledning til yderligere spørgsmål.

Med venlig hilsen
Carsten Stenstrøm
Informationssikkerhedschef
cstr@bane.dk
+45 4188 1976

Høringssvar

Vedr. Offentlig høring om næste generation af den nationale identifikations- og digital signaturinfrastruktur (NemID)

Afsender	Beskæftigelsesministeriet
Dato	24. juni 2014

Kære Morten

Beskæftigelsesministeriet har ingen bemærkninger til det udsendte høringsmateriale.

Med venlig hilsen

Carsten Richter Jensen
Specialkonsulent

E-mail: crj@bm.dk
Direkte tlf.: 72 20 51 65
Besøgsadresse: Holmens Kanal 22

Beskæftigelsesministeriet
Ved Stranden 8 - 1061 København K
Tlf.: +45 7220 5000
Fax: +45 3314 3108
Sikker e-mail: bm@bm.dk
Hjemmeside: www.bm.dk

| The Ministry of Employment
| Ved Stranden 8 - 1061 København K
| Tlf.: +45 7220 5000
| Fax: +45 3314 3108
| Secure e-mail: bm@bm.dk
| Website: www.bm.dk

bitbureauet

Helgesensgade 7, st
2100 København Ø

Telefon: 89 88 06 78
Email: post@bitbureaet.dk

Dato: 27. juni 2014

Digitaliseringsstyrelsen
Att: Morten Jørsum

via email: kis@digst.dk

Høringssvar vedrørende næste generation af den nationale identifikations- og digital signaturinfrastruktur (NemID)

Når Digitaliseringsstyrelsen står på tærsklen til at skulle påbegynde arbejdet med den næste generation af NemID, er det måske også værd at kigge tilbage på nuværende løsning:

Løsning blev lanceret i 1. juli 2010, hvilket var kun 6 dage efter lanceringen af iPhone, … version 4. Alligevel skulle der gå 4 år præcist, før NemID så småt blev understøttet på mobile platforme i denne uge.

Bankerne, som medejere af løsningen, indså hurtigt behovet for at tilbyde kunderne adgang via smartphones. Så de løste selv problematikken ved at tilbyde mobile apps, der via særlige adgange kunne benytte sig af papkortet til validering af transaktioner.

Men det offentlige var hægtet af. Arkitekturen for interaktion med OCES-nøglerne i DanID's varetægt er så kompleks, at selv i dag er det noget af en opgave at få til at køre på en mobiltelefon. Og der var slet ikke tænkt på at løsningen skulle noget andet end at servicere en Java-applet på en PC.

Et godt design starter med et godt fundament. Vi håber med følgende forslag til en kommende NemID, at kunne inspirere til hvordan man kunne skabe et sådan.

Åben process

Vi er meget glade for at blive inviteret til at afgive dette høringssvar. Og vi vil gerne være med endnu længere hen i processen. Faktisk mener vi at det er essentielt at processen og specifikationen bliver så åben så mulig.

Vi vil gerne være med.

Opsplitning af funktionalitet

NemID er i dag en blæksprutte. For det første er der tale om to løsninger i en, OCES-baseret PKI på den ene side og login til netbanker på den anden. Skønt der er overlappende funktionalitet, er det to meget forskellige behov hver af løsningerne har. For bankerne handler det om at minimere økonomiske tab, hvor for OCES-baseret PKI handler det om at sikre identiteter.

For det andet er der et meget asymmetrisk forhold til hvad løsningen kan, i forhold til hvad den anvendes til. Visse funktionaliteter bruges sandsynligvis meget mere end andre. Med en NemID-applet kan man i dag fx underskrive PDF-dokumenter, skønt denne funktionalitet i praksis ganske sjældent bliver brugt af den almindelige borger. Derimod bliver NemID hyppigt anvendt til at logge ind på e-boks.dk eller borger.dk.

Vi finder det derfor naturligt at bygge den kommende NemID op af flere mindre løsninger, efter filosofien: *do one thing, do it well.* Dette kunne fx betyde at man stadig brugte papkort til SSO, men at underskrifter krævede et hardware token med OCES-nøgler.

Dermed kan man også reducere bankerenes adgang til kun at dække en af de mindre løsninger, således at deres behov bliver tilgodeset uden at det er hele NemID som skal leve op til disse.

Flere behov – flere udbydere

Vi kan ikke forvente at alle borgere og virksomheder har samme behov. Derfor vil det være naturligt at der ville kunne være flere udbydere af NemID som kunne tilpasse løsninger til bestemte målgrupper. Dermed kunne udviklingen foregå i konkurrence med andre løsninger.

I den forbindelse er det måske vigtigt at fastsætte krav til udbydere på baggrund af den løsning de tilbyder. Som eksempel: at en udbyder som udelukkende tilbyder en løsning der minder om NemID på hardware, ikke nødvendigvis behøver at have samme krav til oppetid som en løsning der minder om den "almindelige" NemID (da det ikke er nødvendigt at involvere udbyderen i transaktioner).

Med venlig hilsen,

Christian Panton

25. juni 2014

Høringssvar fra CHPCOM-projektet om næste generation af den nationale identifikations- og digital signaturinfrastruktur (NemID)

CHPCOM-projektet takker for muligheden for at komme med bemærkninger i forhold til næste generation af den nationale identifikations- og digital signaturinfrastruktur (NemID).

CHPCOM projektet implementer standarder for sikker kommunikation indenfor energisektoren. Dette er en kritisk forudsætning for at vi i Danmark fortsat kan have en stabil el-forsyning i takt med at sektoren automatiseres yderligere og størstedelen af vores energi vil komme fra vedvarende energikilder.

Arbejdet i CHPCOM projektet sker med afsæt i regeringens Smart Grid strategi og EU's mandater om standardisering i forbindelse med Smart Grid.
Det er et fælles brancheprojekt med 20 partnere, heriblandt Dansk Energi, Dansk Fjernvarme, Foreningen Danske Kraftvarmeværker, Energinet.dk og EURISCO. CHPCOM er støttet af ForskEL til at fremme de internationale smartgrid relaterede datakommunikationsstandarder, specifikt omkring IEC61850, i den danske energisektor.

I etableringen af en sikker kommunikationsinfrastruktur indenfor energisektoren benyttes der eksisterende infrastruktur i så høj grad det er muligt, men der forudses også behov for etablering af ny/udbygning af eksisterende infrastruktur.

CHPCOM-projektet er derfor interesseret i en fortsat dialog om mulige synergier i mellem den nationale identifikations- og digital signaturinfrastruktur og it- og kommunikationsinfrastruktur indenfor energisektoren.

For eksempel, til sikring af kommunikationen i mellem forskellige aktører indenfor energisektoren er der behov for udstedelse af certifikater til sikring af kommunikationen fra maskine-til-maskine og fra person-til-maskine.

Dette er et område der ikke ligger naturligt indenfor det område som NemID hidtil har adresseret, nemlig at levere et brugercertifikat, der kan benyttes af danske borgere.

Uanset om det måtte give mening at inkludere maskine-til-maskine-certifikater i den kommende OCES3-infrastruktur bør certifikatpolitikkerne i denne infrastruktur understøtte samspil med andre certifikatinfrastrukturer, som fx en specifik

certifikatinfrastruktur til forsyningssektoren hvor det primært er kommunikation fra maskine-til-maskine, der skal sikres.

Et sådant samspil kan være at administratorer, der skal bestille maskine-til-maskine-certifikater kan autenticitetssikres ved hjælp af et NemID medarbejder-certifikat. På denne måde kan udgifter til etablering af en separat løsning til udstedelse af akkreditiver til administratorer undgås.

Dette vurderes dog i dag ikke at være muligt på grund af følgende afsnit 5.10 og 5.11 i DanIDs tjenesteudbyderaftale:

5.10 Certifikater fra DanID må ikke bruges til at generere eller signere Certifikater for andre eller i øvrigt danne grundlag for identifikation overfor tredjemand.

5.11 Tjenesteudbyder er indforstået med, at DanID's ydelser ikke må videreføres eller benyttes til at gennemstille Bruger til anden Tjenesteudbyder, hvorved denne Tjenesteudbyder får mulighed for at benytte den forudgående autentifikation foretaget med brug af NemID med mindre andet aftales. Aftale om gennemstilling forudsætter, at den Tjenesteudbyder, der gennemstilles til også har indgået en Tjenesteudbyderaftale med DanID, og at der afregnes transaktionsvederlag pr. Bruger. Ved en anden Tjenesteudbyder forstås en virksomhed, institution, organisation med et CVR-nummer, der er forskelligt fra det, som denne Aftale vedrører.

De ovennævnte begrænsninger vurderes også at blokere for mere privacy-venlige løsninger, som vil kunne bygges med afsæt i NemIDs solide infrastruktur.

Uanset om der arbejdes videre med en multi-leverandør model for næste generation af NemID eller en der ligner den nuværende model med blot én leverandør af NemID anbefaler CHPCOM-projektet at der ikke blokeres for at kunne danne afledte nøgler på basis af et NemID certifikat.

Nu såvel som i takt med at CHPCOM-projektet konkretiserer behovene for sikker it- og kommunikationsinfrastruktur indenfor energisektoren indgår projektet meget gerne i yderligere dialog med Digitaliseringsstyrelsen om behov og ønsker vedrørende den fremtidige identifikations- og digital signaturinfrastruktur.

Med venlig hilsen
På vegne af CHPCOM projektet

Brian Storm Graversen
Work Package Lead
CHPCOM WP5 Sikkerhed

Høringssvar

Vedr. Offentlig høring om næste generation af den nationale identifikations- og digital signaturinfrastruktur (NemID)

Afsender	Civilstyrelsen
Dato	27. juni 2014

Kære Morten

Vedhæftet finder du kopi af høringssvar fra Rigspolitiet, Domstolsstyrelsen, Kriminalforsorgen, Udlændingestyrelsen og Datatilsynet.

Det bemærkes, at hverken Den Uafhængige Politiklagemyndighed eller Civilstyrelsen har haft bemærkninger.

Med venlig hilsen

Morten Chjeffer Rasmussen
Fuldmægtig

JUSTITSMINISTERIET
Budget- og Planlægningskontoret
Slotsholmsgade 10
1216 København K
Tlf. direkte: 7226 8437
Tlf.: 7226 8400
www.justitsministeriet.dk
jm@jm.dk

Høringssvar

Vedr. Offentlig høring om næste generation af den nationale identifikations- og digital signaturinfrastruktur (NemID)

Afsender	Danmarks Rederiforening
Dato	27. juni 2014

Til Digitaliseringsstyrelsen

Danmarks Rederiforening har ikke umiddelbart bemærkninger til de listede høringstemaer, men vil med interesse følge udviklingen af næste generation af identifikations- og digital signaturinfrastruktur, når rammen for en ny løsning er mere konkret.

Med venlig hilsen / Kind regards
Stinne Taiger Ivø
Kontorchef/Head of Division, Lawyer, PhD
Danmarks Rederiforening / Danish Shipowners' Association
Amaliegade 33
DK-1256 Copenhagen K
Tel.: +45 33 11 40 88 / Direct: +45 33 48 92 85
Mobile: +45 51 50 15 85
E-mail: sti@shipowners.dk
www.shipowners.dk

Høringssvar

Vedr. Offentlig høring om næste generation af den nationale identifikations- og digital signaturinfrastruktur (NemID)

Afsender	Dansk Byggeri
Dato	30. juni 2014

Offentlig høring om næste generation af NemID

Dansk Byggeri takker for muligheden for at afgive høringsvar. Vedlagt findes vores svar.

For Dansk Byggeri er det væsentligt, at en fremtidig løsning til brug i virksomheder/erhvervsmæssige sammenhænge er baseret på høj grad af brugervenlig til gavn især for små og mellemstore virksomheder. Det betyder, at bestilling, anvendelse, vedligeholdelse opdatering og ændringer skal kunne håndteres enkelt og forståeligt, således at brugere i små og mellemstore virksomheder foranlediges til at anvende løsninger, der opfylder krav til sikkerhed, juridiske aspekter mv.

Den fremtidige løsning skal hermed kunne håndtere de forskellige roller i virksomhedens administration – herunder som ejer/indehaver eller som ansat medarbejder med forskellige funktioner i forhold til virksomhedens administration og løbende drift med relation til også branchemæssige administrative krav.

Det er endvidere vigtigt, at den fremtidige løsning er orienteret mod de tekniske muligheder – herunder den stigenede digitalisering og de effektiviseringer, der kunne opstå i denne sammenhæng – også mod lanceringen ultimo 2017 og efterfølgende..

Dansk Byggeri forventer endvidere at en national digital identifikations- og signaturinfrastruktur vil kunne anvendes (oprettelse, drift, support og løbende vedligeholdelse) af virksomheder uden omkostninger for virksomhederne.

Vi er naturligvis til rådighed for uddybning af ovennævnte.

Venlig hilsen
Jørn Jensen
Udviklingschef
Kursus&Udvikling
Tlf. direkte: 72 16 01 33 · Mobil: 40 13 22 03

DANSK ERHVERV
BØRSEN
DK-1217 KØBENHAVN K
WWW.DANSKERHVERV.DK

T. +45 3374 6000
F. +45 3374 6080
–
INFO@DANSKERHVERV.DK

Digitaliseringsstyrelsen
Att.: Morten Jørsum

kis@digst.dk

27. juni 2014

Offentlig høring om næste generation af den nationale identifikations- og digital signaturinfrastruktur (NemID)

Generelle bemærkninger

NemID har uden tvivl være med til bane vejen for digitalisering af Danmark. Dels fordi løsningen for de fleste er nemmere at bruge end den digitale signatur, NemID afløste. Dels i kraft af det bagvedliggende samarbejde mellem den offentlige og privat sektor. Brugervenlige løsninger og offentligt/privat samarbejde er vejen frem, ikke mindst i takt med at digital kommunikation bliver obligatorisk.

En nyt NemID skal sætte nye ambitiøse mål som kan retfærdiggøre en gentækning og et nyt udbud af konceptet. De tre år frem til at kontrakten på den nuværende NemID udløber er lang tid i teknologiår - og hvad der umiddelbart kan opfattes som en fjern tendens i dag, kan være meget nærværende til den tid. Et eksempel er den øgede mobilitet, som har været drøftet som tendens i årevis, men hvor der først er fundet finansiering til lancering af en mobil variant af NemID medio 2014.

Dansk Erhverv hilser det derfor velkomment, at Digitaliseringsstyrelsen indleder arbejdet på et nyt beslutningsgrundlag med en bred høring. Arbejdet bør til stadighed indtænke kommunikation og bred forankring i en verden, hvor det digitale for længst er blevet mainstream – og Dansk Erhverv forventer derfor også, at dette blot er første af flere gange, offentligheden inddrages i sagen.

Specifikke bemærkninger

Dansk Erhverv har følgende bemærkninger til de syv temaer fra Digitaliseringsstyrelsen.

1. Fremtidige forretningsmæssige behov, for henholdsvis virksomheder, offentlige sektor og borgere i Danmark og udlandet samt eventuelle juridiske forhold.

Fremtidens vigtigste infrastruktur er digital og går via internettet. På grund af internettets åbne og globale natur vil mange diskussioner om standarder mv. være globale diskussioner. Den teknologiske udvikling betyder, at visionen om et indre marked i EU rykker tættere på virkeligheden. Internettet går på tværs af landegrænser, og så længe man har en bredbåndsforbindelse, kan man

/JSA
jsa@danskerhverv.dk

i princippet etablere virksomhed og samarbejde over landegrænser, ligesom man har mulighed for at tilbyde sine produkter til et stort europæisk marked. Dansk Erhverv ønsker en langt højere grad af fællesmarkedstænkning og harmonisering på disse områder.

Ikke mindst virksomheder har behov for løsninger, der fungerer gnidningsfrit på tværs af nationale systemer. EU har stort fokus på at realisere potentialerne i det digitale indre marked. En del af dette er øget samarbejde og bevægelighed på tværs af unionen. Dansk Erhverv opfordrer derfor til at sikre, at en kommende NemID er ajour og foreneligt med udviklingen af tilsvarende systemer i resten af unionen.

Fuldmagtsløsninger bør indarbejdes på tværs af løsninger, så en borger kan give en medborger en begrænses fuldmagt – fx afgrænset i tid eller til bestemte selvbetjeningsløsninger. Det stiller ikke kun krav til udformningen af selve NemID, men også til alle de myndigheder der integrerer løsninger med NemID.

2. Funktionalitet og anvendelse, herunder eksempelvis niveaudelt sikkerhed, lokal administration af autorisation, single sign-on mv.
Et springende punkt ved overgangen til NemID var den centrale opbevaring af nøglefiler. Papkortet (og senere den digitale "nøgleviser") er en pragmatisk løsnings, der tilgodeser brugervenlighed. Fremadrettet bør NemID kunne tilbydes, så brugeren (borgere, organisationen, virksomheden) har mulighed for selv at opbevare nøglefilen. For centralt placerede nøgler er der selvsagt behov for højeste sikkerhed med brug af robuste teknologier og procedurer.

Virksomhedsforum (enklereregler.dk) behandler løbende udfordringer om samspillet mellem virksomheder og den offentlige sektor, og har haft flere drøftelser med relation til NemID. Flere af de behandlede forslag har ikke (eller kun delvist) kunne gennemføres inden for rammerne af det eksisterende NemID. Disse emner kan med fordel tages op til fornyet overvejelse.

Eksempelvis har man i dag een NemID (eet papkort) pr. person og CVR-nummer. Det betyder, en person, der driver tre virksomheder i dag skal bruge tre forskellige NemID-nøglekort til sine virksomheder, samt et i rollen om borger. Her ville det være hensigtsmæssigt, at man med én og samme identitet kan administrere flere virksomheder (flere CVR-numre og roller). Se virksomhedsforum, forslag 239.

3. Behov for brugervenlighed, herunder forskellige brugeres aktiviteter fra bestilling til anvendelse og eventuel spærring mv.
Hidtidige erfaringer har vist, at man nærmest kun kan undervurdere betydningen af brugervenlighed og genkendelighed på tværs af løsninger. Brugerne af NemID er også brugere af store kommercielle tjenester, som investerer massivt i brugervenlighed som konkurrenceparameter eller præmis for overhovedet at have en rolle på markedet. Brugerne tager derfor høje forventninger til brugervenlighed med sig med største selvfølgelighed, når de møder offentlige løsninger.

Implementeringen af Digital Post til erhverv pr. 1. november 2013 viste, at der stadig er plads til forbedringer ift. udvikling og brugervenlighed, og at der skal afsættes betydelige ressourcer til opmærksomhedsskabende aktiviteter og support ved implementering (se Virksomhedsforum, forslag 237). Fx finder flere enmandsvirksomheder det kontraintuitivt at skulle udstede en "medarbejdersignatur" til sig selv (se Virksomhedsforum, forslag 240).

4. Teknik og infrastruktur, herunder eksempelvis adskillelse af eID og eSignering, single sign-on, sammenhængende IT-arkitektur, sikkerhed mv.

I dag er NemID "nøglen til alting" med samme sikkerhed i alle løsninger. I takt med at mere og mere kommunikation foregår digitalt – ikke bare mellem virksomheder og det offentlige, men mellem borgere, virksomheder og myndigheder på tværs – stiger behovet for forskellige grader af sikkerhed, alt efter hvilken selvbetjeningsløsning eller kommunikation der er tale om. En fremtidigt NemID bør derfor designes til at levere sikkerhed fra "niveau lukket kuvert" til "niveau Fort Knox".

Tendenser der kan synes fjerne i dag, kan blive dagligdag for borgerne og forretningskritisk for virksomheder og offentlige myndigheder på kort tid. Få snakkede om smartphones og det mobile internet i 2007, men det har som bekendt for længst fået sit folkelige gennembrud, hvor det fremstår utidssvarende, at offentlige it-løsninger ikke for længst har fulgt med. En kommende NemID skal derfor kunne benyttes på tværs af platforme – hardware såvel som software. Der bør så vidt muligt anvendes åbne standarder, der også fremadrettet understøtter (også kommende) platforme, kommunikation med endnu ukendte tjenester, eller systemer i andre lande. Det kunne for eksempel blive relevant inden for sundhedsteknologier (Quantified Self) og "the internet of things".

I medieomtaler af identitetstyveri har der ind i mellem hersket uklarhed og sket sammenblanding af identitetstyveri og svindel med betalingskort, lige som der er set regulatoriske tiltag omkring CPR med tvivlsom effekt. Diskussionen om en kommende NemID kan forhåbentlig være medvirkende til at rydde op i misforståelser– fx misopfattelsen af CPR-nummeret som en slags kodeord, eller tanken om, at NemID skulle være løsningen på alt, herunder også ved almindelig handel. Se Dansk Erhvervs "Løsningsforslag til kampen mod identitetstyveri".

5. Samspil med interessenter, herunder tjenesteudbydere, administrative procedurer, sikkerhedsprocedurer mv.

NemID har været ramt at nogle uheldige driftsforstyrrelser. I takt med at brugen og afhængigheden stiger, har disse uregelmæssigheder bevæget sig fra at være irritationsmomenter til at udgøre reelle problemer. Een ting er kontrakter og bodsbestemmelser; noget andet er daglig praksis. Derfor bør beslutningsgrundlaget for den kommende NemID indeholde overvejelser om nødløsninger ved de driftsforstyrrelser, som selvfølgelig ikke må ske, men som ikke desto mindre forekommer i den praktiske virkelighed.

6. Fremtidig forretningsmodel, herunder leverandørstyring, support, betalingsstruktur, en model med flere leverandører mv.

Der ligger udfordringer i spørgsmålet om, hvorvidt en kommende NemID skal udbydes af en eller flere leverandører. På den ene side står ønsket om konkurrenceudsættelse med flere leverandører (pris, innovation), og på den anden side behovet for at sikre tilstrækkelig volumen til at der kan drives en rentabel forretning på en kommende NemID, som holdes ajour ift. sikkerhed og nye funktioner. Uanset fremtidens brug af NemID er løsningen afgrænset til omkring fem millioner danskere, hvad enten de er i rollen som borgere, organisationer eller virksomheder. I lighed med IT-Branchen vil Dansk Erhverv derfor opfordre til, at man undersøger eksempelvis engelske erfaringer med en flerleverandørløsning.

7. Andre bemærkninger

-

Med venlig hilsen

Janus Sandsgaard
Chefkonsulent

27.juni 2014

Til Digitaliseringsstyrelsen
Att. Morten Jørsum

kis@digst.dk

Vedr. Offentlig høring om næste generation af den nationale identifikations- og digital signaturinfrastruktur (NemID)

Digitaliseringsstyrelsen har den 28. maj 2014 iværksat en høring med henblik på at indhente input til næste generation af den nationale identifikations- og digital signaturinfrastruktur (NemID).

DANSK IT har en række observationer vedrørende den nuværende NemID-løsning. Disse indgår sammen med en række anbefalinger i høringssvaret nedenfor.

En helt indledende bemærkning er, at det vil være nødvendigt at gøre det ganske klart, hvorfor der er behov for en afløser for NemID. Trods begyndervanskeligheder og visse kritikpunkter er NemID ved at blive bredt accepteret og forstået af det offentlige, virksomheder og ikke mindst befolkningen, så de ændringer, der måtte blive introduceret, skal kunne opfattes som klare forbedringer bredt i befolkningen for at modvirke en generel modstand mod den digitale udvikling.

Et væsentligt spørgsmål – som vi dog ikke tager endelig stilling til i dette høringssvar – er, hvorvidt der skal skabes et marked med flere udbydere af den næste generation af den nationale identifikations- og digital signaturinfrastruktur, eller om der alene skal være én (offentlig) udbyder. Det er på den ene side et spørgsmål om at sikre en samfundsmæssig kontrol over den essentielle infrastruktur og på den anden side sikre en markedsbaseret udvikling, der fremmer innovation og sikrer konkurrence om at levere tidssvarende løsninger, der til stadighed modsvarer borgernes, erhvervslivets og den offentlige sektors behov. Basalt set handler det om at lægge det rigtige snit i forhold til hvilken del af infrastrukturen, der skal være centralt kontrolleret, og hvilke dele, der kan underlægges konkurrence. Det er under alle omstændigheder en diskussion, som DANSK IT opfordrer Digitaliseringsstyrelsen til at give stor opmærksomhed i det videre arbejde.

1. Fremtidige forretningsmæssige behov

Traditionelt har cpr-nummeret været anvendt som et middel til unik identifikation – og i visse tilfælde også autentifikation – af en borger/bruger. Udviklingen de senere år og de mange sager, hvor cpr-numre enten er lækket eller misbrugt, understreger behovet for udvikling af en sikkerhedsmæssig robust og holdbar løsning, der unikt identificerer den enkelte borger. Løsningen bør som default indeholde forskellige sikkerhedsniveauer og privatlivsbeskyttelse og samtidig være enkel at bruge.

DANSK IT anbefaler at orientere sig på europæisk plan for at vurdere, om Danmark bør forholde sig til løsninger og trends der og som minimum sikre kompatibilitet med andres europæiske identitetssystemer.

Mulighed for delvis eller trinvis anonymitet: Der er situationer, hvor det kan være ønskværdigt at være delvist anonym; fx kan der være funktioner, hvor det kun er få oplysninger om brugeren, som er nødvendige for at blive tilladt adgang til en bestemt funktion. Ved de fleste ehandels-transaktioner vil der for eksempel alene være behov for at sikre valide adresseinformationer.

2. Funktionalitet og anvendelse

Borgerne bliver mere og mere mobile, og forventer en større og større grad af personalisering. Det betyder for det første, at en kommende udgave af NemID funktionelt skal være markant lettere at anvende, når den skal bruges på farten.

Derudover bør der opbygges en form for trappe eller trinvis inddeling af autentifikationen, således at man med få login-oplysninger kan tilgå almindelige personlige oplysninger – og at det først er når særligt personfølsomme oplysninger skal præsenteres, eller der skal foretages væsentlige transaktioner, man skal bruge højeste sikkerhedsniveau. Altså mulighed for differentierede sikkerhedsniveauer og privatlivsbeskyttelse. Det bør fremgå, hvilket sikkerhedsniveau der er valgt for en specifik kommunikation. Der bør i videst muligt omfang gives brugeren mulighed for selv at vælge sikkerhedsniveau, hvis det kan sikres, at der sker et oplyst valg på basis af en afvejning af sikkerhed kontra bekvemmelighed.

Det skal desuden være nemt at anvende løsningen på nye typer af enheder, hvad enten det måtte være fremtidens intelligente køleskabe, støvsugere, tv, telemedicinsk udstyr etc.

Interfacet skal være nemt at forstå, så brugeren nemt kan overskue hvad han giver væk af information.

Der bør være andre to-faktor autentifikationsmekanismer end nøglekort og password.

Borgerens digitale identitet bør tilhøre borgeren på samme måde som et pas til traditionel identifikation. Det vil sige, at man bør kunne autentificere sig over for en tredjepart og eventuelt få etableret afledte identiteter uden at dette bliver registreret hos udstederen og uden at der kan opkræves gebyr herfor – i særdeleshed gebyrer for brug af afledte identiteter.

NemID til medarbejderbrug bør håndteres som tilknyttede roller (attributter) for personen. Det vil gøre brugen lettere for personer med mange roller.

3. Behov for brugervenlighed

Det er vigtigt at den kommende løsning understøtter brugere med særlige behov, fx i forbindelse med handicap, uanset om det er en borger eller en offentligt ansat medarbejder.

I den forbindelse må der også tages hensyn til problemstillinger omkring fuldmagt og delegering, hvor der eksempelvis bør være mulighed for at delegere rettigheder til begrænsede formål til familiemedlemmer eller andre. Derved kan det undgås, at personer generelt udleverer hele deres NemID-credentials til andre.

Det bør være muligt at kunne foretage en spærring online, hvis der er mistanke om misbrug.

Endvidere bør løsningen kunne stilles til rådighed for børn og unge og tilgodese deres behov for login i forbindelse med skoleplatforme, eksamener, bus- og tog-kort, bankkonti m.v.

I takt med at et bredere spektrum af tjenester må forventes at benytte en fremtidig id- og signaturløsning, bør det også fra begyndelsen gøres muligt, at personer med kortvarig tilknytning til Danmark – fx turister, expats og udvekslingstuderende – kan tilbydes adgang til løsningen på en administrativ enkel og omkostningseffektiv måde.

4. Teknik og infrastruktur

Den nye generation af Nemid bør være uafhængig af platforme og således kunne fungere på alle kendte, relevante platforme.

Adskillelse af eID og eSignering vil være at foretrække. Desuden synes det også at være sikkerhedsmæssigt hensigtsmæssig at skelne mellem den digitale identifikation og de situationer, hvor borgeren eller brugeren skal underskrive digitalt.

Systemet bør konstrueres således at (avancerede) brugere har mulighed for at få fuldkommen kontrol over deres eget nøglemateriale.

Man bør undersøge muligheden for at introducere et sikret hardware-modul, som kan vise den transaktion, man er ved at godkende/signere. Dette vil vanskeliggøre man-in-the-middle-angreb, som har vist sig at være en udfordring ved det eksisterende system.

Løsningen bør i videst muligt omfang benytte åbne standarder – blandt andet for bedre at kunne interagere med kommende teknologier og standarder.

Den nye version af NemID skal være robust over for kompromittering, således at de personlige oplysninger, som bruger afgiver ved anvendelse af NemID, ikke kan anvendes af uvedkommende. Der skal planlægges for, at løsningen kan kompromitteres på centralt hold uden tab af fortrolighed og integritet. Dette kan eksempelvis opnås ved at kryptere lagrede oplysninger og opretholde en effektiv og robust adgangskontrol.

5. Samspil med interessenter

Det bør være et krav, at en anden offentlig myndighed end Digitaliseringsstyrelsen godkender sikkerhedsdesign og implementering i den næste generation af NemID som valideringsmekanisme i forhold til offentlige systemer.

Især det private marked har behov for løsninger, der fungerer interoperabelt og brugervenligt på tværs af nationale grænser.

I forhold til organisering har "Se og Hør-sagen" senest illustreret vigtigheden af organisatoriske sikkerhedsrutiner m.v. Derfor bør der i forbindelse med driften af systemerne stilles krav, som eksempelvis indebærer, at

- samme person må ikke have adgang til mere end ét system
- hardware til hvert kritisk system skal fysisk være beskyttet og uafhængig af hardware til andre kritiske systemer
- kritiske funktioner skal involvere mindst to personer
- Digitaliseringsstyrelsen gennemfører egen kontrol med leverandørens it-sikkerhedspraksis

6. Fremtidig forretningsmodel

Ingen særlige bemærkninger til dette punkt men se det indledende afsnit om samfundsmæssig kontrol og skabelse af marked.

7. Andre bemærkninger

Det bør helt generelt holdes for øje, at den nye generation af NemID bør være så robust og pålidelig, at borgernes tillid til den offentlige, digitale infrastruktur kan bibeholdes.

Desuden bør etableringen af løsningen være baseret på en bevidsthed om, at der er en øget hastighed i udviklingen af både tjenester, services og brugsscenarier. Det er eksempelvis en konsekvens af udbredelsen af "Internet of Things" og et tilhørende behov for rettighedsstyring. Det stiller nye krav til mulighederne for løbende at tilpasse løsningen, så den understøtter udviklingen frem for at blive betragtet som en klods om benet.

Med venlig hilsen

Anders Sparre
politisk chef

Til
Digitaliseringsstyrelsen,
e-mail: kis@digst.dk

Danske Handicaporganisationer

Blekinge Boulevard 2
2630 Taastrup, Danmark
Tlf.: +45 3675 1777
Fax: +45 3675 1403
dh@handicap.dk
www.handicap.dk

Taastrup, den 27. juni 2014
Sag 6-2014-00357– Dok. 162734 SL /mol/kft

Høringssvar: Offentlig høring om næste generation af den nationale identifikations- og digital signaturinfrastruktur (NemID)

Danske Handicaporganisationer (DH) har følgende bemærkninger til tema 3, Behov for brugervenlighed:

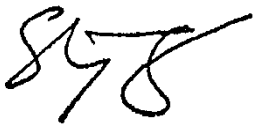
I forbindelse med næste generation af NemID er det vigtigt, at der tages højde for tilgængelighed for personer med handicap allerede fra udarbejdelsen af kravspecifikationerne. NemID skal også kunne benyttes af personer med handicap, hvoraf nogle bruger særligt tilpassede it-programmer. I udviklingsfasen skal man stille krav om tilgængelighed og henvise til de eksisterende standarder og retningslinjer. I de tilfælde, hvor der ikke findes standarder eller retningslinjer, skal behovene om tilgængelighed afdækkes ved at inddrage personer med handicap og tilgængelighedseksperter i processen. Tilgængelighed er vigtig for mange forskellige grupper af personer med handicap, heriblandt personer med fysiske, kognitive og kommunikationsmæssige handicap.

Hvor der er behov for det, skal der udvikles særlige løsninger for personer med handicap. Dette behov skal afdækkes i samarbejde med handicaporganisationerne, der skal inddrages løbende i dette arbejde. De nuværende alternative løsninger har langtfra dækket de behov, personer med handicap, der tidligere har været selvhjulpne, er stødt på. F.eks. har hardware-løsningen, der bl.a. skulle være en løsning for mennesker med handicap, vist sig ikke at være brugbar, da man allerede i forbindelse med installationen støder ind i netop de problemer, som man også møder, når man bruger et almindeligt nøglekort. Derudover fungerer denne løsning kun på de offentlige løsninger og ikke bankernes. Desuden har hardware-løsningen være forbundet med en ekstra udgift for den enkelte borger. Derfor er en mere simpel (og gratis – der skal ikke være en ekstra udgift alene fordi man har et handicap) nødvendig.
Desuden er det ikke muligt, at få et nyt login, hvis man ikke kan huske sit login. Hvis der skrives forkert tre gange, må der i stedet bestille en ny, med de omkostninger der er forbundet med dette.

Adgang til NemID for personer med handicap er afgørende for, at alle bliver inkluderet i det digitale samfund, vi alle skal være en del af med bl.a. obligatorisk digitalisering og digital post. Den nuværende NemID-løsning rummer en del udfordringer, som IT- og Telestyrelsen for nogle år siden identificerede gennem en arbejdsgruppe, nedsat til formålet. Vi vedlægger den afsluttende rapport. F.eks. bør det være muligt, at nøglekort kan modtages elektronisk, da det vil give personer med handicap mulighed for at benytte kompenserende programmer som zoom og talesyntese til at aflæse og anvende nøglekortet.
Disse udfordringer skal løses i den næste generation af NemID, så den bliver tilgængelig for alle.

Skulle ovenstående give anledning til spørgsmål, kan disse rettes til chefkonsulent, Monica Løland, på tlf.: 3638 8524 eller e-mail: mol@handicap.dk.

Med venlig hilsen



Stig Langvad
Formand

N O T A T

DANSKE REGIONER

16-06-2014
Sag nr. 14/413
Aleksander Bjerrum
Tel. 35 29 84 90
E-mail: alb@regioner.dk

Bilag A: Regionernes visionsoplæg for NemID

Resumé
Regionerne ser frem til et konstruktivt og effektivt samarbejde om udbudsprocessen for NemID, som især bør fokusere på lokale forretningsbehov.

Regionernes formelle indspil udgøres af nærværende visionsoplæg samt løbende deltagelse i workshops, høringer og ad hoc henvendelser. Det undersøges endvidere, om der er grundlag for indstationering i Digitaliseringsstyrelsen.

Baggrund
Regionerne har gennemført en fælles opsamling om den nuværende NemID-løsning som led i forberedelsen af udbudsprocessen. Erfaringsopsamlingen fokuserer på 1) velfungerende elementer i NemID, som bør videreføres og 2) oplagte områder til forbedring. Dette visionsoplæg udgør en uddybning af erfaringsopsamlingen samt regionernes formelle svar på den offentlige høring om næste generation af den nationale identifikations- og digital signaturinfrastruktur (NemID).

Løsning
Nedenfor opsamles regionernes indspil til udbuddet af NemID.

Velfungerende elementer i det nuværende NemID
Regionerne kvitterer for den stabile og gensidigt forpligtende offentligt/private forretningsmodel for det nuværende NemID. Forretningsmodelen bør fortsat inkludere bankerne og udbygges med eventuel inddragelse af telesektoren og forsikringsselskaberne. Endelig har også den tekniske model vist sig at være velfungerende over længere tid sideløbende med udviklingen i den nationale og lokale digitale infrastruktur.

Temaer for et kommende NemID

Det er vigtig med en overordnet diskussion af de styrende temaer for et kommende NemID, eksempelvis forholdet mellem staten som udbyder af infrastruktur og lokale virksomheder som indkøbere af services, markedsbaserede modeller samt drøftelser af sikkerhed. Helt centralt for det næste NemID er at forholde sig til at lave en struktur for en løsning, der i princippet skal virke frem til 2024 og matche forskellige tekniske formål på en gang. Endelig er det vigtigt med en drøftelse af sikkerhedsdagsordenen, især i lyset af den politiske bevågenhed på området.

Næste generation af NemID skal skaleres til at rumme store virksomheder og bør bringe brugerne tættere på "Bring Your Own Device"-konceptet, hvor NemID i et større omfang er platformsuafhængig og kan anvendelse på mobile enheder.

Leverandørkontakt og styring

- Betalingsstrukturen skal leve op til gængse standarder for gennemsigtig og økonomisk rimelig fakturering og det skal være muligt at følge håndteringen af sin henvendelse.
- Leverandøren af et kommende NemID skal forpligtes på konkrete servicemål for den tekniske løsning, herunder især oppetider, fejlhåndtering, løsningstider og lovrelaterede ændringer. Servicemålene, og opfølgningen herpå, forvaltes i samarbejdsmodel om drift og vedligehold af fællesoffentlig infrastruktur.
- Der bør i den nye model rettes et større fokus på brugervenligheden i administrationen/håndteringen af NemID. Der mangler vigtige og forbedrede elementer som statistik-modul, visnings-modul og fejlhåndterings-modul.
- Servicemål skal ses i sammenhæng med centrale opdateringer og evt. afledte lokale behov for at indkøbe hjælpeprogrammer. Fx bruger den nuværende NemID programmeringssproget Java. Den næste javaopdatering fungerer ikke på Windows XP, som mange regioner fortsat bruger. Det betyder, at regionerne må speede opgradering af anden software op.
- Den samlede løsning med al nødvendig dokumentation til udvikling, implementering og drift skal være offentliggjort og tilgængelig mindst 6 måneder før en planlagt idriftsættelse.
- Store organisationer, som regionerne, har brug for en bedre adgang til udvikling, support og service end en hotline. Hver region bør have sin formelle kontaktperson hos leverandøren med hurtig adgang samt mulighed for at påvirke udviklingen af services i forbindels med styringen og opfølgningen af leverancer.

- Den fremtidige supportorganisation bør følge 24/7/365-konceptet.
- Planlagte årlige releases samt release-notes bør tilgå alle kunder

Lokal forankring

- Et nyt NemID skal understøtte fleksibel og effektiv lokal administration af autorisation, herunder masseudstedelse og straksoprettelse. Eksempelvis er der i dag udfordringer ved vikar- og nyansættelser, hvor der er behov for straksopretning.
- Der bør være bedre muligheder for test, herunder flere testmiljøer, udvikling, kvalitetstest, staging og undervisning.
- Løsningen skal forholde sig til forskellen mellem autentificering og bemyndigelse med tanke for det store behov for at kunne håndtere flere sikkerhedsniveauer lokalt ligesom dobbelt-sikring bør undgås.
- Der bør fastholdes en sammenhæng mellem autentifikation og signatur, således at den en funktionalitet ikke kan eksistere uden den anden
- Autentifikation og bemyndigelse skal være synkroniserede, så de udløber på samme tid.
- Det skal være muligt for store virksomheder at have en superadministrator som kan opsætte administrator rettigheder for grupper af administratorer.
- Anvendelsen af NemID skal genere grundlag for ledelsesinformation. Det drejer sig eksempelvis om statistikker. Eksempelvis kan det være mulighed for at se på antallet af brugere og gruppering af brugere udefra kriterier og tid. Desuden skal det i statistiklister være muligt med højere detaljegrad på specifikke dataelementer.
- Implementeringen af NemID skal tage højde for omfanget af systemtekniske konksekvenser i lokale systemer. Dette er især med tanke på, at løsningen skal indtænkes i systemets arkitektur.
- Behov for større handlefrihed til anvendelse på forskellige platforme, herunder diverse gængse tablets og smartphones, fx IOS, Andriod, Windows Phone / Surface mv.
- Der bør findes en løsning, så udenlandske ansatte har mulighed for at benytte tjenester, der er anvendes med NemID.
- Øget mulighed for integration med andre offentlige instanser.

Teknik og infrastruktur

- Mulighed for single signon (afdækning af særligt tekniske og juridiske aspekter i ny digital signatur).
- Yderligere udbygning/mulighed for anvendelse af web-services

- Overvågning, monitorering og display af aktuel status af web-services fra leverandørens side
- Udviklingen af fremtidig NemID bør følges af et overordnet arkitektur-råd, så der sikres compliance med andre nationale/regionale systemer.
- Føderationsløsninger bør udbygges til brug for regioner og kommuner.
- Der bør arbejdes på en yderligere understøttelse af føderationsløsningen i NSP. Adgang til relevante statslige systemer og fællesregionale systemer skal flyttes til adgang via NSP.

Afhængigheder (juridiske mv.)

- Der skal laves centrale retningslinjer, for hvornår der skal bruges medarbejder-, funktions- eller virksomhedssignatur.

DATATILSYNET

Digitaliseringsstyrelsen
Landgreven 4
Postboks 2193
1017 København K

Sendt til: kis@digst.dk

25. juni 2014

Datatilsynet
Borgergade 28, 5.
1300 København K

CVR-nr. 11-88-37-29

Telefon 3319 3200
Fax 3319 3218

E-mail
dt@datatilsynet.dk
www.datatilsynet.dk

J.nr. 2014-122-0597
Sagsbehandler
Trine Cseh-Lessel
Direkte 3319 3219

Vedrørende høring om næste generation af den nationale identidikations- og digital signaturinfrastruktur (NemID)

Ved e-mail af 28. maj 2014 har Digitaliseringsstyrelsen anmodet om Datatilsynets eventuelle kommentarer til høring om næste generation af den nationale identifikations- og digital signaturinfrastruktur (NemID).

Høringen indeholder ingen nærmere beskrivelse af en kommende løsning. Digitaliseringsstyrelsen har imidlertid i overskriftsform angivet en række temaer, indenfor hvilke styrelsen ønsker bemærkninger.

I den anledning skal Datatilsynet fremkomme med følgende overordnede bemærkninger:

1. Datatilsynet skal generelt understrege, at den til enhver tid gældende persondatalovgivning skal iagttages i forbindelse med udstedelsen af signaturen. Efter Datatilsynets opfattelse ligger ansvaret for, at sikkerheden i den nye løsning er tilstrækkelig høj, hos såvel Digitaliseringsstyrelsen som en evt. kommende leverandør.

2. Herudover skal persondatalovgivningen iagttages, når signaturen bruges hos myndigheder og virksomheder – f.eks. i selvbetjeningsløsninger for borgerne eller ved medarbejderes log-in til myndigheders eller virksomheders systemer.

3. Datatilsynet kan generelt pege på følgende regler i persondataloven:

- Grundbetingelserne i persondatalovens § 5 om god databehandlingsskik, saglighed, proportionalitet, datakvalitet og sletning.
- Behandlingsbetingelserne i persondatalovens § 6 om almindelige personoplysninger, §§ 7 og 8 om følsomme personoplysninger samt § 11 om personnumre.
- Reglerne om de registreredes personers rettigheder i kapitel 8-10, herunder.
    - Den dataansvarliges oplysningspligt ved modtagelse/indsamling af oplysninger, jf. persondatalovens §§ 28 og 29.
    - Den registreredes ret til indsigt og øvrige rettigheder.

- Reglerne om datasikkerhed i §§ 41 og 42 – kravet om fornødne sikkerhedsforanstaltninger, skriftlig databehandleraftale og kontrol med databehandleren.
- De nærmere krav i sikkerhedsbekendtgørelsen, hvis den dataansvarlige er en offentlige myndighed, samt eventuelle sikkerhedskrav i vilkår fra Datatilsynet, hvis den dataansvarlige er en privat virksomhed.
- Reglerne om anmeldelse til og tilladelse/udtalelse fra Datatilsynet i kapitel 12 og 13 samt reglerne om tilladelse fra Datatilsynet i bl.a. § 27, stk. 4.

4. Beskyttelsen af personoplysninger og privatliv bør efter Datatilsynets opfattelse indgå som en integreret del af systemudviklingen. Databeskyttelsen skal indbygges i løsningen fra en start. Der bør i den forbindelse tages hensyn til, at forskellige brugere kan have forskellige ønsker og behov i forhold til brug af tjenesten, og der bør etableres valgfrihed for brugerne, hvor dette er relevant.

Datatilsynet skal i den forbindelse anbefale, at der foretages en analyse af konsekvenserne for privatlivet (PIA) i forhold til den påtænkte nationale identifikations- og digital signaturinfrastruktur.

5. Datatilsynet skal endvidere pege på de elementer, der indgår i Kommissionens forslag til databeskyttelsesforordning[1].

Datatilsynet kan umiddelbart fremhæve følgende elementer fra forslaget:

- Retten til dataportabilitet (artikel 18).
- Princippet om ansvarlighed (artikel 22).
- Indbygget databeskyttelse og databeskyttelse gennem indstillinger (artikel 23).
- Kravet om dokumentation (artikel 28).
- Konsekvensanalyse vedrørende databeskyttelse (artikel 33).
- Forudgående godkendelse og forudgående høring (artikel 34).

Det er uvist, hvordan reglerne bliver i deres endelige udformning. Datatilsynet skal derfor foreslå, at Digitaliseringsstyrelsen følger udviklingen og tager skridt til at sikre, at næste generation af den nationale identifikations- og digital signaturinfrastruktur (NemID) kan leve op til de kommende regler, når de engang træder i kraft.

Med venlig hilsen

Lena Andersen
Kontorchef

[1] Com(2012) 11 final. Forslag til EUROPA-PARLAMENTETS OG RÅDETS FORORDNING om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger (generel forordning om databeskyttelse).

Høringssvar

Vedr. Offentlig høring om næste generation af den nationale identifikations- og digital signaturinfrastruktur (NemID)

Afsender	Den Uafhængige Politiklagemyndighed
Dato	27. juni 2014

Kære Morten

Vedhæftet finder du kopi af høringssvar fra Rigspolitiet, Domstolsstyrelsen, Kriminalforsorgen, Udlændingestyrelsen og Datatilsynet.

Det bemærkes, at hverken Den Uafhængige Politiklagemyndighed eller Civilstyrelsen har haft bemærkninger.

Med venlig hilsen

Morten Chjeffer Rasmussen
Fuldmægtig

JUSTITSMINISTERIET
Budget- og Planlægningskontoret
Slotsholmsgade 10
1216 København K
Tlf. direkte: 7226 8437
Tlf.: 7226 8400
www.justitsministeriet.dk
jm@jm.dk

Digitaliseringsstyrelsen
Att.: Morten Jørsum
Landgreven 4
Postboks 2193
1017 København K

Danish ICT and Electronics Federation

Høring vedr. næste generation digital signatur

DI og DI ITEK takker for henvendelsen af 28. maj 2014 vedrørende høring af "næste generation af den nationale identifikations- og digital signaturinfrastruktur (NemID)". Vi har i den anledning følgende bemærkninger til forslaget.

Overordnet er det vigtigt, at den fremtidige løsning er baseret på størst mulig konkurrence på markedet, fungerer på tværs af platforme og hardware, kan anvendes internationalt, er let at administrere, er fleksibel for brugerne og kan justeres til den internationale udvikling.

Det er vigtigt, at løsningen er anvendelig til en lang række forskellige formål fra digitale selvbetjeningsløsninger i det offentlige til autentifikationstjenester på private internettjenester, og for både borgere og medarbejdere i virksomheder og offentlige myndigheder.

Endelig er det vigtigt, at Digitaliseringsstyrelsen i det fremtidige arbejde med næste generation digital signatur sikrer sig en bred opbakning fra de danske aktører, og dermed får lavet et solidt grundlag for det kommende udbud.

De mere detaljerede bemærkninger følger den struktur, som Digitaliseringsstyrelsen har foreslået i høringsbrevet.

Fremtidige forretningsmæssige behov

1. Pseudonymer og afledte identiteter
Den fremtidige løsning bør åbne op for en fleksibel anvendelse af attributter, så den muliggør forskellige typer af anvendelse i både offentlige og private tjenester. Løsningen bør således tillade, at enkeltstående attributter kan anvendes til at sikre brugeren anonymitet - f.eks. ved alene at autentificere at brugeren er over 18 år. Løsningen bør ligeledes kunne anvendes således, at brugeren fleksibelt kan anvende attributter i en konkret situation og dermed kan oprette afledte identiteter eller pseudonymer.

2. Videregivelse af identiteter

Det er vigtigt, at der fastholdes en sikker initial identifikationsproces guidet af sikre processer og kontroller. På baggrund af den sikre initiale identitet bør brugeren let kunne videregive eventuelle afledte identiteter til andre identity management services.

Anvendelsen af afledte identiteter bør ikke kunne registreres af den oprindelige udbyder, ligesom denne ikke bør kunne tage betaling for anvendelsen af afledte identiteter.

3. Kompatibilitet med eksisterende identity management systemer
Der er på den globale markedsplads en massiv konkurrence om at tilbyde identity management for brugerne. Der er tilsvarende blandt brugerne vidt forskellige årsager til at have tillid til de forskellige serviceudbydere. Den fremtidige løsning bør tage højde for denne situation og sikre en høj grad af kompatibilitet med eksisterende identity management-systemer.

4. Kompatibilitet med eksisterende standarder
Danmark bør ikke låse sig fast på en national løsning, der ikke kan finde global anvendelse. Løsningen bør derfor være baseret på og være kompatibel med internationale åbne standarder på området. Dette er væsentligt for såvel brugernes anvendelse af og tillid til løsningen som udbydernes muligheder for at agere på et globalt marked.

Funktionalitet og anvendelse

1. Fleksibel løsning
Det er centralt, at den fremtidige løsning fungerer på tværs af platforme - f.eks. java, .net og linux - og på tværs af hardware enheder - f.eks. PC, tablet og Smartphones.

2. Flere sikkerhedsniveauer
Der er behov for, at den fremtidige løsning kan anvende flere sikkerhedsniveauer afhængigt af den service, som løsningen skal bruges i. Der er f.eks. ikke samme behov for sikkerhed, når der logges på skat.dk, som når der logges på dba.dk. Sikkerhedsniveauerne bør bl.a. afhænge af risikoprofilen for services og dataklassifikationen. Serviceudbyderen kan f.eks. anvende password, to-faktor autentifikation eller biometri afhængig af det behov for sikkerhed, som det vurderes, at den pågældende tjeneste bør udbyde.

3. Én medarbejdersignatur
Den fremtidige løsning bør sikre, at medarbejdersignaturers rettigheder kan justeres således, at der kun skal oprettes én signatur pr. medarbejder, og at denne kan bruges på tværs af CVR-numre - f.eks. indenfor samme koncern.

4. Administration af medarbejdersignatur
Administrationen af medarbejdersignaturerne opleves som ganske besværlig. Når der skal tildeles rettigheder til den enkelte bruger, skal der logges ind mange forskellige steder. Det vil være nyttigt, hvis administrator alene skulle logge ind ét sted, og herfra kunne fordele alle rettigheder til medarbejderen. Tilsvarende ville det være nyttigt, hvis administrator kunne kopiere en rolle med et givent sæt rettigheder fra én bruger til en anden bruger, så man ikke skal starte forfra for hver bruger.

Behov for brugervenlighed

1. Sprog
Mange danske virksomheder agerer i en global kontekst og har derfor behov for support på flere sprog - især engelsk.

2. Fleksible signaturer
For nogle virksomheder er det nyttigt at have en medarbejdersignatur, som er forskellig fra brugerens private signatur. For andre virksomheder - typisk enkeltmandsvirksomheder - er det besværligt at have forskellige signaturer. Der bør gives højere grad af fleksibilitet på dette område, således at det er op til brugerne, om den ene eller den anden model skal anvendes.

3. Sikker e-mail
Det er fra flere sider blevet påpeget, at mange virksomheder har vanskeligt ved at integrere den nuværende løsning i deres e-mail. Der bør arbejdes på at lave en enkel og brugervenlig løsning til at modtage et certifikat til sin egen mailklient (og i tilknytning hertil også til de gængse webmailklienter).

4. Delegering af signaturer
Det bør være muligt at delegere anvendelsen af signaturer til andre. Særligt it-svage familiemedlemmer kan have en fordel af at delegere signaturen til et nært familiemedlem, som kan foretage transaktioner på vedkommendes vegne.

Teknik og infrastruktur

1. Opbevaring af nøgler
Det er vigtigt at sikre høj grad af fleksibilitet i forhold til den fremtidige opbevaring af nøgler, således at brugerne kan vælge den model, som passer til deres behov. Desuden anbefales det, at undersøge mulighederne for at kunne tilvejebringe en signaturløsning for virksomheder, som baseres på en hardware-model, hvor udstyret ikke skal tilsluttes terminalen.

2. Mulig adskillelse af signatur og single sign-on
Det bør overvejes at adskille den digitale signatur fra single sign-on. Det må antages, at der i praksis meget sjældent er brug for en egentlig dokumentsignering, ligesom brugen af signaturen kan give udfordringer efter udløb af signaturen.

Samspil med interessenter

1. Samarbejde med identity management leverandører
Der bør sikres et samarbejde mellem andre leverandører af identity management systemer. Dels nationale leverandører, f.eks. jvf. eID-direktivet, og dels private leverandører på det globale marked. Det kan ikke understreges nok, hvor vigtigt det er, at den fremtidige løsning kan bruges i en global kontekst.

2. Samspil med danske interessenter

Det er vigtigt, at Digitaliseringsstyrelsen i forlængelsen af denne høring fastholder en åben proces og inddrager de danske aktører, som har en interesse i dette område, således at det kommende udbud i stort muligt omfang afspejler de ønsker, de forskellige aktører har.

Fremtidig forretningsmodel

1. Flere udbydere
Der bør fra Digitaliseringsstyrelsen lægges op til en struktur, hvor det kan sikres, at flere leverandører kan løse opgaverne. Dette skal have til formål at skabe konkurrence på området, at sikre etablering af flere markedsdrevne forretningsmodeller samt at sikre, at de forskellige krav til attributhåndtering, som den offentlige og private sektor har, imødekommes. For at nå dette må er det vigtigt, at Digitaliseringsstyrelsen, som anbefalet ovenfor, baserer sig på åbne internationale standarder.

2. Attribut ontologier
Det private marked har ofte brug for andre attributter end den offentlige sektor. Samtidig anvender den konkrete løsning, NemID, kun PID, RID og CPR som attributter. Den fremtidige løsning bør indrettes således, at den kan indkooperere de attribut ontologier, som standardiseres af markedsaktørerne. På den måde sikrer man, at f.eks. reputation kan tilknyttes en brugers signatur og understøtter dermed udviklingen af nye markedsbaserede forretningsmodeller.

DI ITEK står naturligvis til rådighed for en uddybelse af ovenstående kommentarer.

Med venlig hilsen

Henning Mortensen
Chefkonsulent, DI ITEK

Naalakkersuisut
Government of Greenland

Digitaliseringsstyrelsen

DIGITALIMIK
SULLISSINERMUT
AQUTSISOQARFIK

27-06-2014

Uunga
Til

Digitaliseringsstyrelsen i Danmark

Assinga uunga
Kopi til

Charlotte Dacoby

Postboks 1078
3900 Nuuk
Tel. (+299) 34 50 00

E-mail: digitalisering@nanoq.gl
www.nanoq.gl

Offentlig høring om næste generation af den nationale identifikations- og digital signaturinfrastruktur (NemID)

Vi takker for høringsbrevet og muligheden for at kommentere på fremtidens NemID løsning.

Digitaliseringsstyrelsen henstiller til:

- at der også i den nye NemID løsning tages hensyn til de grønlandske forhold
- at den grønlandske applet, som er udviklet og finansieret frem til 2017 understøttes af den nye NemID løsning
- at den nuværende kommunikationsproces fortsættes således at Grønland orienteres og dermed kan varetage oversættelse til grønlandsk

Lige som der arbejdes på at gøre NemID tilgængelig for virksomheder i Grønland.

Med venlig hilsen

Dorte Bøge Sørensen
Styrelseschef for Digitaliseringsstyrelsen

Tlf.: +299 587531
Mail: dobs@nanoq.gl

Domstolsstyrelsen

Justitsministeriet
Slotsholmsgade 10
1216 København K

Sendes alene pr. e-mail til jm@jm.dk med kopi til mcr@jm.dk

Store Kongensgade 1-3
1264 København K
Tlf. +45 70 10 33 22
post@domstolsstyrelsen.dk
CVR-nr. 21659509
EAN-nr. 5798000161184

J.nr. 2014-4101-0033-9
Sagsbeh. Jacob Søndergaard
+45 99 68 43 07
jas@domstolsstyrelsen.dk
23. juni 2014

Høring om næste generation af den nationale identifikations- og digital signaturinfrastruktur (NemID)

Justitsministeriet har ved e-mail af 11. juni 2014 anmodet om eventuelle bemærkninger i forbindelse med Digitaliseringsstyrelsens høring om næste generation af den nationale identifikations- og digital signaturinfrastruktur (NemID), jf. Digitaliseringsstyrelsens brev af 28. maj 2014.

Domstolsstyrelsen kan i den anledning oplyse følgende:

Ad 2 Funktionalitet og anvendelse
Med øgede krav om digital selvbetjening er der et stigende behov for velfungerende og nemt tilgængelig fuldmagtsgivning. Både i form af en generel fuldmagt, for eksempel ved værgemål, men også i form af en specifik fuldmagt, for eksempel hvis en borger i en specifik sag er repræsenteret af en advokat og derfor har behov for at give den pågældende repræsentant fuldmagt til at få adgang til visse digitale tjenester eller dokumenter i forbindelse med den specifikke sag. Brug af fuldmagter skal i dag håndteres i den enkelte myndigheds systemer, hvorved mange bruger ressourcer på at udvikle samme funktionalitet. Det vil være hensigtsmæssigt, at det undersøges, om fuldmagtsgivning kan løses med en fællesoffentlig digital løsning tilknyttet NemID.

Ad 3 Behov for brugervenlighed
Der bør være mulighed for fuld anvendelse af NemID fra mobile platforme, og det vil tillige øge brugervenligheden, hvis engangspassword kan tilgå brugeren digitalt.

Ad 5 Samspil med interessenter
I sikkerhedsspørgsmål og ved mistanke om sikkerhedshændelser virker det nuværende setup ikke tilstrækkeligt. Der mangler en synlig adgang for myndigheder og borgere til at indrapportere mistanke om sikkerhedshændelser, og der bør i organiseringen omkring NemID være et proaktivt beredskab til håndtering af sikkerhed, herunder til at sikre den nødvendige kommunikation til offentligheden, således at der ikke opstår tvivl om sikkerhedsniveauet i en så vital fællesoffentlig infrastruktur.

Med venlig hilsen

Niels Juhl

Ballerup d. 25/6 2014

Digitaliseringsstyrelsen
Att. Morten Jørsum
Landgreven 4
Postboks 2193
DK-1017 København K

Pr. e-mail: kis@digst.dk

Høringssvar vedrørende næste generation af den nationale identifikations- og digital signaturinfrastruktur (NemID)

e-Boks A/S skal hermed afgive sine kommentarer til offentlig høring vedrørende næste generation af den nationale identifikations- og digital signaturinfrastruktur (NemID).

e-Boks A/S støtter en fælles infrastruktur for identifikation og digital signatur, som tilgodeser krav til sikkerhed og behov for brugervenlighed på tværs af platforme. En fælles infrastruktur på dette område, som kan anvendes på tværs af offentlige myndigheder og private virksomheder, er et vigtigt fundament for at opnå potentielt store samfundsmæssige gevinster ved digitalisering.

Det er vigtigt at sikre, at alle tjenesteudbydere får samme muligheder for anvendelse af den fælles infrastruktur, så løsningen opleves sammenhængende og ensartet af brugerne på tværs af de forskellige tjenesteudbyderes løsninger. Det er en forudsætning for at udnytte muligheden for private aktører for at udvikle værdiskabende løsninger for myndigheder, virksomheder og borgere i Danmark.

Specifikt har e-Boks A/S følgende kommentarer til tema 2: Funktionalitet og anvendelse:

1) Der bør skabes mulighed for at etablere single sign-on-føderationer mellem tjenesteudbydere, uafhængigt af sektor og på tværs af den offentlige og den private sektor. I en række brugssituationer er der en naturlig sammenhæng mellem forskellige tjenesteudbyderes ydelser, fx ifm. forsikringsydelser, e-Boks, sagsbehandling og lign. En løsning, der understøtter single-sign-on-føderationer ud over den offentlige sektor, vil derfor give mulighed for yderligere digitalisering og automatisering i samspillet mellem sådanne aktørers ydelser, uden at der opstilles barrierer for brugervenligheden ved at kræve fornyet log-on ved skift mellem de involverede tjenesteudbyderes services.

2) En ny løsning bør understøtte differentierede sikkerhedsniveauer for alle tjenesteudbydere uafhængigt af sektor. Der er stor forskel på, hvilket sikkerhedsniveau der kræves for forskellige typer af transaktioner. Dette kendes allerede fra en række bankers såkaldte kiggeadgang, hvor mindre følsomme oplysninger kan tilgås med et lavere sikkerhedsniveau, mens gennemførsel af transaktioner, aftaleindgåelse m.v. kræver autentifikation på et højere sikkerhedsniveau. Et tilsvarende behov findes hos tjenesteudbydere uden for den finansielle sektor, hvor en mulighed for at tilpasse kravene til sikkerhedsniveau til karateren af den enkelte transaktion og følsomheden af de tilgængelige informationer vil bidrage til større brugervenlighed i løsninger, der anvender NemID. Understøttelse af differentierede sikkerhedsniveauer vil dermed kunne bidrage til en øget udbredelse blandt tjenesteudbydere og til at nedbryde brugervenlighedsmæssige barrierer.

3) Mobile tjenester bliver stadig mere udbredt og i fremtiden vil det for nogle services i fremtiden være eneste adgangsvej, så den er afgørende at næste generation NemId kan anvendes på mobile devices med samme hensyn som angivet ovenfor, herunder muligheder for differentierede sikkerhedsniveauer.

Med venlig hilsen

e-Boks A/S

ERHVERVS- OG VÆKSTMINISTERIET

Digitaliseringsstyrelsen
Landgreven4
Postboks 2193
1017 København K

26. juni 2014
14/04919-7
sos-dep

ERHVERVS- OG VÆKSTMINISTERIET

Slotsholmsgade 10-12
1216 København K

Tlf. 33 92 33 50
Fax. 33 12 37 78
CVR-nr. 10092485
EAN nr. 5798000026001
evm@evm.dk
www.evm.dk

Offentlig høring om næste generation af den nationale identifikations- og digital signaturinfrastruktur (NemID)

Erhvervs- og Vækstministeriet har modtaget ovenstående høring fra Digitaliseringsstyrelsen. Erhvervs- og Vækstministeriet har sendt materialet i høring hos Erhvervsstyrelsen, Finanstilsynet, Patent- og Varemærkestyrelsen, Sikkerhedsstyrelsen og Søfartsstyrelsen og har på den baggrund følgende bemærkninger.

I nedenstående dækker betegnelsen "virksomheder" alle virksomhedsformer medmindre andet nævnes. NemID refererer i høringssvaret til NemID til erhverv, herunder NemID medarbejdersignaturer.

I forbindelse med udbuddet af NemID skal Erhvervs- og Vækstministeriet pege på følgende overordnede betragtninger.

- At NemID til erhverv skal designes på en måde, så virksomhedernes forretningsmæssige behov og vækstmuligheder gennem offentlig digitalisering, får bevågenhed da det er forventningen, at der ligger et uudnyttet effektiviserings- og vækstpotentiale for et samlet erhvervsliv ved en nytænkning af fokus for, hvordan offentlig digitalisering gennemføres fremadrettet.
- At anvendelsen af NemID i dag reelt er obligatorisk, da den er tæt knyttet til obligatorisk anvendelse af andre fælles offentlige digitale services som f.eks. Digital Post. Dette bør afspejles i forretningsmodellen for NemID, designet af den og sammenhængen til de øvrige fællesoffentlige digitale services.
- Opfølgningen på de forslag som regeringens Virksomhedsforum for enklere regler har stillet vedr. NemID bør ligeledes indgå i forberedelsen af næste generation af NemID.

Disse tre forhold bør give anledning til, at en nærmere og selvstændig analyse afdækker ikke blot de forretningsmæssige behov i forhold til Ne-

mID, men også samspillet og indbyrdes afhængigheder mellem de forskellige fællesoffentlige services og komponenter.

Høringssvaret indeholder derudover dels nogle overordnede kommentarer om udviklingen af NemID og dels nogle helt konkrete input, som er registreret på baggrund af Erhvervs- og Vækstministeriets opgave med brugersupport for Virk.dk. De konkrete input er listet i punkform under de relevante overskrifter

1. Fremtidige forretningsmæssige behov

Behov for analyse også fra et helikopterperspektiv
I takt med at det på flere og flere områder bliver obligatorisk for virksomheder at kommunikere digitalt med det offentlige, får NemID en mere central betydning for virksomhedernes forretning. Uhensigtsmæssigheder ved NemID er ikke acceptable, når det offentlige reelt gør anvendelsen af NemID obligatorisk for alle, der ønsker at drive virksomhed i Danmark.

At anvendelsen reelt er blevet obligatorisk bør derfor give anledning til, at området analyseres nærmere også fra et helikopterperspektiv. Det er således ikke tilstrækkeligt kun at analysere NemID løsningen. Det er nødvendigt at anskue NemID i den bredere sammenhæng, som den indgår i, da NemID er en løsning der aldrig benyttes alene, men indgår i digitale processer. Der bør fortages analyser af, om virksomhedernes behov kan imødekommes mere hensigtsmæssigt gennem et ændret koncept for NemID, samt om snitfladen mellem NemID og de øvrige fællesoffentlige digitale services kan optimeres til gavn for både virksomheder og den offentlige sektor.

Erhvervs- og Vækstministeriet forventer, at se dette brede analysebehov på virksomhedsområdet afspejlet i projektplanen for udbuddet af NemID.

Brugssituationer og målgrupper der bør indgå i analysen
NemID til virksomheder er væsentligt mere kompliceret end NemID til borgere alene af den grund, at flere brugere skal agere inden for samme enhed (CVR-nummer). NemID findes også på virksomhedsområdet både som nøglefil og nøglekort. NemID til virksomheder skal således understøtte flere brugssituationer og forretningsmæssige behov end på borgerområdet, f.eks.:

- anvendelse i større organisationer hvor forskellige brugere skal have forskellige adgang, uden at det pålægge virksomheden unødige administrative opgaver og tidskrævende log-in procedurer
- små virksomheder og foreninger der i praksis overlader deres forpligtigelser til en tredje part (advokat, administrator eller lign.)
- anvendelse i koncerner med mange CVR-numre og behov for at agere på tværs af disse
- anvendelse af professionelle brugere, der agere på vegne af mange virksomheder og derfor har behov for at tværgående overblik
- anvendelse af foreninger der har et CVR-nummer, men ikke anser sig selv som virksomheder og som typisk kan have jævnlig udskiftning af den tegningsberettigede

Det er væsentligt, at alle disse forskellige anvendelsesmønstre og målgrupper indgår i de forretningsmæssige analyser omkring en ny NemID til erhvervsområdet.

Forretningsmæssige analysepunkter
Som afspejlet i brugssituationerne har mange virksomhedsbrugere behov for at agere på tværs af flere eller mange CVR-numre. Der bør foretages en nærmere analyse af, hvorvidt dette behov kan imødekommes ved at skabe en over-administrator rolle der, med de enkelte CVR-numres tilladelse, kan sammenkoble flere CVR-numres signaturer.

Endvidere foregår i dag brugerrettighedstildeling både i NemID og i NemLogin Brugeradministration foruden i myndighedernes egne systemer. Dette skaber forvirring hos virksomhedsbrugerne, der derved bliver pålagt bebyrdende arbejdsgange og som konsekvens heraf belaster de offentlige supportfunktioner. Der bør fortages en analyse af området og rettighedsstyring bør i fællesoffentligt regi fremadrettet kun ske via ét af de fælles offentlige systemer, dvs. i enten NemID eller NemLogin Brugeradministration.

I praksis drager flere fællesoffentlige systemer og selvbetjeningsløsninger – f.eks. Digital Post og NemLogin - fordel af NemID administratorrollen, idet de på forskellig vis overfører denne til en administratorrolle til det specifikke system. Denne praksis bør konsolideres og strømlines, så det gøres ensartet og således, at den tegningsberettigede ved tildeling af NemID administrator rollen bliver oplyst om, og accepterer de vidtgående

beføjelser, som denne rolle indebærer. En tværgående administrator rolle vil i praksis lette administrationen for mange virksomheder.

For ikke at pålægge virksomheder unødige administrative byrder skal virksomhederne opleve, at de forskellige obligatoriske digitale services supplerer hinanden og at de understøtter hvert deres formål i kommunikationen med det offentlige. Udstedelse af NemID bør fremover ske i en forretningsgang samtidigt med udstedelse af CVR-numre, da alle med et CVR-nummer reelt er forpligtet til at blive NemID bruger blandt andet i forhold til den lovpligtige digitale postkasse. Området bør analyseres nærmere.

NemID på borgerområdet er en succes bl.a. fordi borgerne kan anvende samme signatur ikke blot over for offentlige myndigheder, men også i deres interaktion med banker, forsikringsselskaber mm. Det bør undersøges, om et tilsvarende samarbejde mellem den finansielle og den offentlige sektor kan udvikles på erhvervsområdet.

En stor del af danske virksomheder er enkeltmandsvirksomheder, som er personligt ejede. Juridisk set er det altså en konkret borger, der står til ansvar for virksomheden. Det er uforståeligt for disse virksomheder, at de skal operere med to forskellige signaturer, som begge identificerer den samme person. Det foreslås at disse virksomheder lettes ved, at de kan få knyttet deres private NemID til virksomhedens CVR nummer. Alternativt bør det være meget let rent digitalt med udgangspunkt i den personlige NemID at erhverve en NemID medarbejdersignatur, der kommer med en grundpakke af rettighedstildeling til sig selv, så de kan benytte de fællesoffentlige digital services uden at forholde sig yderlig til brugerrettighedsstyring.

2. Funktionalitet og anvendelse

Bestilling og aktivering af NemID medarbejdersignatur forårsagede mange supportkald under udrulning af Digital Post til virksomheder i efteråret 2013. Dette vidner om, at bestilling, aktivering og anvendelse af signaturen er kompliceret at forstå, samt at brugervenligheden i den nuværende løsning ikke er høj nok.

En on-line brugerundersøgelse om Digital Post udført af Erhvervs- og Vækstministeriet i samarbejde med Megafon i maj 2014 viste, at blot 39

% af virksomhedsbrugerne af NemID medarbejdersignatur var tilfredse med løsningen.

Idet der er tale om en løsning, der reelt er obligatorisk for virksomheder bør løsningen fremadrettet i langt højere grad understøtte virksomhedernes behov. Det bør være enklere at anskaffe og aktivere signaturen, at administrere brugere og arbejde på tværs af CVR-numre.

Herunder listes helt konkrete områder, hvor det er nødvendigt i højere grad at udvikle brugervenlig funktionalitet:

- Det skal være enkelt for virksomhedsbrugere at finde oplysninger om, hvem der er deres NemID administrator. Disse oplysninger bør kunne findes on-line såvel som ved telefonisk kontakt til brugersupporten.
- NemID og NemLogin Brugeradministration bør samtænkes, så det for virksomhederne fremgår klart, hvilke funktionaliteter hvert system understøtter, således at virksomhederne får effektive arbejdsgange på tværs af de to systemer.
- NemID administratoren bør som udgangspunkt kunne blive administrator for alle fællesoffentlige systemer i én arbejdsgang, hvis det ønskes og på sigt også for alle myndigheders erhvervsrettede systemer. Der skal oplyses aktivt herom så den tegningsberettigede kan accepterer dette vilkår, når de opretter deres NemID. Hermed kan virksomheder med 0 ansatte, - op til ca. 400.000 af Danmarks virksomheder, slippe for at foretage yderlig opsætning af brugerrettigheder i fællesoffentlige systemer og hen ad vejen også i myndighedsspecifikke systemer og dermed opnå en væsentlig administrativ lettelse.
- Hvis man bestiller signatur til en anden bruger, skal man også have mulighed for at tildele rettigheder til denne i samme arbejdsgang.
- Ved bestilling af nyt certifikat ved en allerede eksisterende aftale skal der foretages et tjek af, om det er den samme person for at undgå dobbelte brugerprofiler. I en længere periode vedrørte 24 % af henvendelserne til Erhvervsstyrelsens kundesupport sig om NemID dobbelte brugerprofiler. Er der i forvejen tilknyttet en signatur til CVR-numre, bør disse vises, så brugeren kan genudstede det samme certifikat med samme id. nr.
- Udstedelse og administration skal være brugervenligt. Det skal være muligt for virksomhederne hele vejen i forløbet at se, hvor man er og gå tilbage og ændre.

- Der er behov for en rent digital proces som understøtter indgåelse af aftale om NemID, i stedet for eller som supplement for den nuværende med at udskrive, printe og indsende en fuldmagt fra den tegningsberettigede via scannet dokument eller via fysisk post.
- Det bør være muligt at fortage bestilling og administration på engelsk.
- Certifikatpolitikken bag NemID virker hæmmende for udviklingen og brugen af signaturer i fællesoffentligt regi. F.eks. er Digital Post hæftet op på NemID, der er hæftet op på CVR. Det giver utilsigtede situationer f.eks. ved ophør af et CVR-nummer, hvor man f.eks. ikke kan komme ind i den digitale postkasse efter historiske dokumenter. Det betyder at store økonomiske gevinster ikke høstes i det offentlige, fordi der må sendes fysiske breve til virksomheder under ophør. I takt med udbredelse af obligatorisk digitalisering må en fællesoffentlig komponent og tilhørende politikker kunne tilpasses så funktionaliteten følger med.

3. Behov for brugervenlighed

For at udvikle en NemID til erhvervsområdet, der understøtter såvel det offentlige som virksomhedernes behov er det afgørende, at der sker en reel og professionel brugerinddragelse gennem hele processen lige fra de forretningsmæssige analyser, over konceptudvikling til brugertest af det endelige produkt. Erhvervs- og Vækstministeriet forventer, at de forskellige brugerinddragelsesinitiativer, metoder og deres formål vil fremgå af projektplanen for udbuddet.

Konkrete brugervenlighedstiltag:

- Brugerne skal kunne finde relevant og kontekstnær hjælp. Det nuværende hjælpeunivers er vanskeligt at orientere sig i, og tager ikke afsæt i brugernes behov.
- Det kan ikke på forhånd forudses, hvor brugerne vil møde udfordringer i en digital løsning. Det er derfor væsentligt, at det som et minimum vil blive muligt løbende og fleksibelt at kunne tilrette tekster, vejledninger m.m. i den nye NemID løsning.
- Betegnelsen ”NemID medarbejdersignatur” skaber meget forvirring blandt virksomhedsbrugerne: Foreninger ser ikke sig selv som virksomheder eller medarbejdere, mange enkeltmandsvirksomheder ser sig selv som selvstændige, og altså lige netop ikke som medarbejdere. Mange NemID administratorer er selskabsejere, hvorfor de heller ser sig selv som medarbejdere.

Der bør arbejdes på at finde en mere intuitiv og hensigtsmæssig terminologi for NemID til virksomheder, foreninger m.v. med et CVR-nummer.

- Nøglekortet som pragmatisk løsning skal fastholdes, men nøglekort til borgere og virksomheder bør adskille sig mere visuelt fra hinanden, så brugere der besidder begge ikke tager fejl af, hvilket kort der skal anvendes i den givne situation.
- Konsekvent og konsistent anvendelse af terminologi både i NemID regi, men også på tværs af de fælles offentlige digitale services.

4. Teknik og infrastruktur

- NemID bør til en hver tid understøtte mindst 95 % af de af brugerne anvendte browsere, styresystemer og mobile devices.
- NemID mobil skal understøtte virksomhedernes behov, herunder mobil adgang for virksomhedsbrugere der anvender NemID nøglefil.
- Migration af brugere til det nye NemID bør i videst muligt omfang ske uden brugernes aktive involvering og gøres let tilgængelig på de punkter, hvor brugerne skal involveres. Ved migrering fra Digital Signatur til NemID i 2013 var der 80.000 brugere, der ikke migreredes over. Disse 80.000 ender let med at få dobbelte brugerprofiler, hvilket generede mange kald hos Erhvervsstyrelsen og mange utilfredse og frustrerede kunder. En gnidningsløs migration er vigtig både i forbindelse med fuldmagter, rettigheder og Digital Post.

5. Samspil med interessenter

NemID på borger området er en succes bl.a. fordi borgerne kan anvende samme signatur ikke blot over for offentlige myndigheder, men også i deres interaktion med banker, forsikringsselskaber m.v. Det bør undersøges om et tilsvarende samarbejde mellem den finansielle og den offentlige sektor kan udvikles på erhvervsområdet.

6. Fremtidig forretningsmodel

Betalings- og incitamentsstruktur

Betalings- og incitamentsstrukturen for NemID skal i langt højere grad end tilfældet er i dag, understøtte en fortsat udvikling af NemID samt gode brugeroplevelser.

Ingen betaling af support for virksomheder
Virksomheder skal i dag betale for basal support samt elementære ydelser, som f.eks. flere end 3 NemID medarbejdersignaturer. Dette er ikke rimeligt når det reelt er obligatorisk for virksomheder at anvende NemID. Basale ydelser og support der understøtter de gængse behov på virksomhedsområdet bør være gratis for virksomheder. Det kan overvejes, at specialydelser samt support heraf kan være forbundet med betaling, da de erfaringsmæssigt anvendes af store virksomheder.
Support af NemID bør således frikøbes.

Sammenhængende support
Virksomhederne differentierer ikke mellem snitflader for de forskellige digitale services, myndigheder eller leverandører. Virksomhedsbrugerne ønsker at kunne henvende sig ét sted for at få hjælp til deres digitale kommunikation med det offentlige. Og denne hjælp bør være tilgængelig i de sammenhænge, hvor virksomhederne møder de offentlige digitale services.

Herudover er det vigtigt i forhold til udenlandske virksomheders brug, at der er en begrænset registreringsbarriere, så det er nemt for virksomhederne at anvende, samt en fornuftig vetting procedure, så myndighederne i rimelig grad kan have tillid til, at brugerne er dem, som de udgiver sig for at være.

Erhvervs- og Vækstministeriet finder generelt, at man bør bestræbe sig på at lave en løsning, der så vidt muligt er "platform as a service", således at forskellige myndigheder og det private erhverv nemt og billigt kan integrere til løsningen samt være med til at fremme og udvikle den. Samtidigt skal løsningen i så høj grad som muligt være platformsuafhængig, hvilket også er den vej, som NemID er rettet imod med javascript løsningen.

Erhvervs- og Vækstministeriet har ikke yderligere bemærkninger til høringen.

Med venlig hilsen

Sanne Olsen
Sekretær
sos@evm.dk

Høringssvar

Vedr. Offentlig høring om næste generation af den nationale identifikations- og digital signaturinfrastruktur (NemID)

Afsender	Finans og Leasing
Dato	1. juli 2014

Til Digitaliseringsstyrelsen, Morten Jørsum

Høringsvar vedr. næste generation af den nationale identifikations- og digital signaturinfrastruktur (NemID) J.nr. 2014- 5155-013

Finans og Leasing er en brancheorganisation med 42 medlemmer, der til samme omsætter for ca. 100 mia. kr. om året. Alle vores medlemmer har berøring med NemID i deres forretningsgang. Vi ønsker at komme med på høringslisten næste gang og deltage i den videre høringsproces.

Vi forventer, at brug af NemID, såvel som andre eID´s kun vil stige i de kommende år, hvorfor det er yderst vigtigt for os, at der sigtes mod en "blivende" løsning, uden for mange platforms & funktionalitets skift over tid. Ud fra udviklingen som den tegner sig i dag, regner vi med, at NemID i 2017 vil være den altoverskyggende form for identifikation der benyttes.

1.Fremtidige forretningsmæssige behov, for henholdsvis virksomheder, offentlige sektor og borgere i Danmark og udlandet samt eventuelle juridiske

Generelt forventer vi udviklingen går i retning af:

- Generel dokumentunderskrift via NemID – også af kunder bosiddende i udlandet – evt. begrænset til EU.
- Mulighed for sikker e-kommunikation med alle
- Online chat
- NemID er fuldt dækkende for Kend-din-kunde-forpligtelserne (og i øvrigt complient) iflg. Hvidvaskloven. NemID skal anerkendes fuldt på linie med pas/kørekort.
- Brugervenligt system, som er simpelt for kunden at benytte og administrere
- Platformsuafhængighed
- Samme sikkerhedsmodel på tværs af platforme, leverandør, eID mv.

Vi ønsker endvidere, at man i næste generation af NemID kan trække offentlig data (fra offentlig registre) om personen, herunder roller/beføjelser i selskaber (daglig leder, bestyrelsesmedlem mv.), rettigheder for selskabet (prokura, sigantur) og oplysninger til brug for hvidvaskcompliance (reelle ejere):

CVR opslag

For overholdelse af tegningsregler og tegningsberettigede (kræver en modellering af CVR registeret,

hvor en virksomhedsejer kan administrere disse ud fra helt specifikke retningslinjer – se

tinglysning.dk som inspiration).

Fuldmagter/ Autorisation

Det ville være ønskeligt om næste generation NemID havde mulighed for (potentielt), at kunne trække data fra et fuldmagtsregister – for at sikre at den ansattes MOCES certifikat kan signere på særlige forudsætninger. Dette vil kræve et register hvor en virksomhedsejer kan administrere fuldmagter – evt.

udbygge CVR registeret med denne funktionalitet. Fuldmagtsregistre findes i andre lande f.eks. i Norge.

Ift. hvidvask (fsva. tjek af reele ejere mv.) kunne ønskes mulighed for opkobling til det (forhåbentligt snart) kommende ejer-register hos Erhvervsstyrelsen samt mulighed for opkobling til kørekortregisteret hos SKAT/Politi, hvor der automatisk hentes billede ID for den part som signerer et dokument.

Først efter fejlfri endt kontrol i disse registre vil signeringen blive gennemført. Den nye model af signering skal være entydig.

Endelig skal den nye model kunne skaleres til at omfatte yderligere kontrolopslag, såfremt behovene eller lovgivningen kræver det – fx aktiebog/ejerbog af en virksomhed.

2. Funktionalitet og anvendelse, herunder eksempelvis niveaudelt sikkerhed, lokal administration af autorisation, single sign-on mv.

Vi ønsker bl.a. single sign-on (og dermed brug af NemID over en eller flere sessioner. Formålet med dette er, at minimere det antal gange kunden skal præsenteres for NemID login), niveaudelt/gradueret sikkerhed (f.eks. mulighed for NemID light sign on, uden brug af 2 faktor sikkerhed), tidsstyring/varighed på adgang, signering af dokumenter.

For virksomheder, offentlige myndigheder og foreninger skal det være muligt at opbygge et elektronisk hierarki, så de interne beføjelser kan håndteres, herunder krav om underskrift af flere personer i fællesskab. Administrationen skal som udgangspunkt ske lokalt. Ved benyttelse af signaturerne skal der ske automatisk kontrol af, at underskriftsreglerne er fulgt.

Der skal være mulighed for system-til-system-integration og indlejring i vore forretningsprocesser.

3. Behov for brugervenlighed, herunder forskellige brugeres aktiviteter fra bestilling til anvendelse og eventuel spærring mv.

Vi ønsker identificering og signering i et step (signering afvises hvis identificering ikke godkendes), samt platforms/deviceuafhængighed. Der skal kun være en type signering, og den skal understøtte alle devices – fra PC til mobile enheder.

Løsningen skal have mulighed for personlig styring på tværs af platforme og skal endvidere benytte den samme sikkerhedsmodel, på tværs af platforme, leverandører, eID mv

Endvidere ønskes central og simpel distribution af NemID til kunder. Altså fremadrettet ingen udlevering af NemID via banken.

Stærkt forbedret support på såvel NemID som eID relaterede ydelser. Der skal være en langt mere kundevendt support, for såvel kunder som tjenesteudbydere. For tjenesteudbydere skal der være mulighed for support/driftovervågning 24/7

4. Teknik og infrastruktur, herunder eksempelvis adskillelse af eID og eSignering, single sign-on, sammenhængende IT-arkitektur, sikkerhed mv.

Sikkerheden skal forbedres fra 3 faktor sikkerhed, evt. suppleret med biometrisk login og biometrisk

signeringsproces (da løsningen skal være langtidsholdbar og biometriske muligheder kan blive almindelige indenfor få år).

Der skal være en uafhængighed af andre IT-systemer/platformes funktionsdygtighed – fx Java – så vedvarende drift sikres, og således at systemets oppetid er i top.

Sikkerheden skal være i højsædet i forbindelse med udstedelsen af signaturen – evt. krav om personligt fremmøde og legitimering ved privatpersoners bestilling af NemID.

Via single sign-on skal password automatisk dannes og ajourføres – eventuelt suppleret med nøglekort i udvalgte situationer. Generel bekræftelse via SMS o.l., at signaturen er benyttet. Automatisk spærring ved forkert angivne nøgler. Manuel spærringsmulighed – online, via SMS eller telefon.

5. Samspil med interessenter, herunder tjenesteudbydere, administrative procedurer, sikkerhedsprocedurer mv.

Som ovenfor nævnt ønskes mulighed for samspil med offentlige registre CVR, SKAT etc., så man på en enkel måde kan få indblik i selskabers reelle ejere, så hvidvasklovens regler om legitimering og identifikation af disse er opfyldt uden yderligere tiltag, men også mulighed for samspil med private registre såsom Bisnode mv.

Det skal sikres, at NemID kan benyttes som eID i samspil med, som minimum, eID fra skandinavien i øvrigt. Altså muligheden for at bygge løsninger med brug af flere forskellige typer af eID.

Simpel og ”kundevendt” implementering af NemID løsninger som tjenesteudbyder. I forhold til den nuværende procedure for etablering af NemID løsninger er der behov for et massivt løft i form af bedre arkitektur, support samt dokumentation. Der skal tænkes kundevendt fremfor det modsatte.

6. Fremtidig forretningsmodel, herunder leverandørstyring, support, betalingsstruktur, en model med flere leverandører mv.

Det kan overvejes, at udarbejde centrale aftaler f.eks. med alle mobiloperatører ifb. med NemID på mobil (simkort), således at man ikke skal lave mange aftaler for at komme ind på markedet, men kan nøjes med en central/fælles aftale gennem NemID**.**

NemID ønskes som isoleret ydelse (eID), uafhængig af løsningsvalg. Dvs. NemID skal isoleres til at være "ID" ydelsen, og alt andet er tillægsprodukter. Vi vil således gerne have muligheden for at integrere flere forskellige eID's ind i løsninger der ikke nødvendigvis leveres af NemID leverandøren.

Der ønskes endvidere en bred produkt-palette hos leverandøren af NemID. Uagtet at vi gerne ser NemID adskilt fra løsninger for at sikre det frie leverandørvalg, vil vi foretrække at den valgte leverandør har en bred palette af ydelser til f.eks. E-signering, E-arkiv, E-identifikation og lignende eID relaterede ydelser. Alt andet lige, vil det være at foretrække med en sammenhængende IT arkitektur, med løsninger fra samme leverandør indenfor dette område

Det må sikres at brugerne ikke påvirkes ved ændringer i leverandør, supportør og betalingsstruktur. Det er vigtigt, at brugervenligheden og stabiliteten er i top. Eventuelt må lovreguleret, central enhed være det nødvendige filter, så vedvarende drift sikres – uanset leverandører eller udskiftninger i disse – og således at brugerne får kvalificeret hjælp.

7. Andre bemærkninger

Vitterlighedsvidner

Bør fortsat være løst som i den nuværende model, at certifikatets ægthed indestås af certifikatudsteder (pt. Nets/DanID).

Generelle bemærkninger i øvrigt

Fejlfri funktionsdygtighed og brugertillid må være i højsædet. Brugerne (alle typer) må holdes skadesløse for fejl, opstået som følge af svigt i det tekniske setup f.eks. via klageadgang til et offentligt nævn, som tager stilling til evt. efterforskning og regres mod skadevolderne – samt sikrer at der sker tiltag til tekniske udbedringer.

Endeligt er det vigtigt, at Digitaliseringsstyrelsen fokuserer på nogle særlige områder for at sikre NemID's fremtidige succes:

- Arbejde for at gøre NemID endnu mere udbredt og accepteret som standarden indenfor online legitimation og signering. Et eksempel kan være i forhold til Hvidvaskningslovgivningen, hvor NemID i dag ikke accepteres på linje med fysisk legitimation som f.eks. kørekort. NemID fungerer således kun som legitimation ved mindre forbrugerkreditter og andre lavrisikoprodukter så som billån og leasing. NemID bør anerkendes fuldt ud på lige fod med pas/kørekort.

- Arbejde for at gøre NemID mere brugervenligt end tilfældet er i dag. Det burde være muligt at lave en løsning, der er nemmere for brugeren end den nuværende som baseres på et stykke lamineret pap med 100 koder, der fremsendes med posten, og som brugeren efterfølgende skal have med sig overalt. Der skal tænkes i nye teknologier og laves løsninger, der baseres på fremtidens teknologiske muligheder (mobile enheder, tablets osv.), uden at der gives køb på sikkerheden.

Finans og Leasing står naturligvis til rådighed for yderligere oplysninger og deltager meget gerne i den videre proces/høring. Vi vil foreslå oprettelse af en følgegruppe og vi deltager gerne heri.

Med venlig hilsen

Thomas Benjamin Johansen
Chefkonsulent, Finans og Leasing
Torveporten 2, 4. sal
2500 Valby
Tlf 27369019
tbj@finansogleasing.dk
www.finansogleasing.dk

Til Digitaliseringsstyrelsen, kis@digst.dk

27. juni 2014

Høringssvar vedrørende næste generation af den nationale identifikations- og digital signeringsinfrastruktur (NemID)

Finanssektorens Hus
Amaliegade 7
DK-1256 Copenhagen K

Telefon 3370 1000
Fax 3393 0260

mail@finansraadet.dk
www.finansraadet.dk

Kontakt Henriette Rolskov
Direkte +45 3370 1102
her@finansraadet.dk

Journalnr. 466/01
Dok. nr. 523629-v1

Ved brev af 28. maj 2014 har Digitaliseringsstyrelsen anmodet Finansrådet om bemærkninger forud for genudbuddet af næste generation af den nationale identifikations- og digitale signeringsinfrastruktur (NemID).

Bankerne bakker op om det digitale Danmark og er positive i forhold til at fortsætte et samarbejde om en fælles kerne for næste generations NemID på tværs af den offentlige og finansielle sektor. Dette både for at bidrage til at understøtte løsningen af samfundsmæssige udfordringer, for at høste synergi på tværs af sektorerne og for, at borgerne/kunderne får en god brugeroplevelse.

Det bemærkes, at situationen i 2017 vil være ændret i forhold til samarbejdet om det eksisterende NemID, der er blevet implementeret fra 2010 og frem. Eksempelvis er langt flere borgere og virksomheder i dag digitale i forhold til offentlige myndigheder, bl.a. på grund af regeringens ambitiøse borger- og virksomhedsrettede digitalisering. Samtidig har den offentlige sektor i dag større erfaring med at forvalte sikkerhedsløsninger. Dermed er der både en høj digitaliseringsparathed i Danmark at bygge på og mange indhøstede erfaringer at bringe videre i forhold til at skabe fremtidens løsning.

I det følgende er Finansrådets bemærkninger indsat i den struktur, som Digitaliseringsstyrelsen har udbedt bemærkningerne i:

1. Fremtidige forretningsmæssige behov

Bankerne ser den digitale bank som omdrejningspunktet for den fortsatte forretningsmæssige udvikling af de danske banker og er dermed meget positive i forhold til at fortsætte et samarbejde om en fælles kerne for den nationale identifikations- og digitale signeringsinfrastruktur på tværs af den offentlige og finansielle sektor. Det er vigtigt for bankerne, at den næste generations NemID bliver en omkostningseffektiv løsning.

2. Funktionalitet og anvendelse

Kernen i det fælles samarbejde bør tage udgangspunkt i en sikker autentifikationsservice, hvilket vil sige en løsning, som borgeren/kunden kan anvende til ensartet at logge ind i offentlige løsninger og i banksektorløsninger.

Derudover er bankerne interesserede i en løsning, der er mindre kompleks og modulært opbygget i services med veldefinerede grænseflader.

3. Behov for brugervenlighed

En af de væsentligste forudsætninger for samarbejdet er at give kunderne en brugervenlig og sikker digital identifikationsløsning, som kan bruges på tværs af den offentlige forvaltning og bankerne. Dette giver genkendelighed og en god brugeroplevelse.

4. Teknik og infrastruktur

I forhold til den tekniske infrastruktur ser bankerne behov for en løsning, der er opbygget i servicemoduler med klare grænseflader og en agil tilgang, med en hovedvægt på at kunne reagere hurtigere på kundernes behov og løbende levere nye services.

Løsningen skal imødekomme behovet for:

- forretningsmæssigt løbende, at kunne videreudvikles så det til stadighed sikres, at både den offentlige sektor og finanssektoren er der, hvor borgerne/kunderne er.
- Sikkerhedsmæssigt at kunne ændres hurtigt, så både aktuelle og potentielle trusler løbende og professionelt imødegås.

5. Samspil med interessenter

I forhold til samarbejdskonstruktion under projektets gennemførelse er det vigtigt for bankerne at finde en løsning, hvor governance er enkel med fleksibilitet for begge parter.

6. Fremtidig forretningsmodel

Det er væsentligt for bankerne, at der gennemtænkes en fair økonomisk fordelingsnøgle, og at den kommende generations NemID er omkostningseffektiv i såvel anskaffelse som drift.

7. Andre bemærkninger

Ingen.

Finansrådet uddyber gerne ovenstående ved et møde med Digitaliseringsstyrelsen.

Med venlig hilsen

Henriette Rolskov

Direkte +45 3370 1102
her@finansraadet.dk

Høringssvar

Vedr. Offentlig høring om næste generation af den nationale identifikations- og digital signaturinfrastruktur (NemID)

Afsender	Finanstilsynet
Dato	24. juni 2014

Her er Finanstilsynets bemærkninger inden for følgende temaer:

Funktionalitet og anvendelse

Det bør sikres, at løsningen kan anvendes uanset brugerens valg af teknisk platform. Derfor er det vigtigt, at it-sikkerheden i høj grad er indkapslet i NemId-løsningens it-arkitektur.

Teknik og infrastruktur

Der har været flere uhensigtsmæssigheder omkring den nuværende java-platform, herunder flere it-hændelser, hvorfor det bør overvejes, om den nye NemId-løsning kan skabes på en platform med et højere sikkerhedsniveau generelt.

Vi skal gøre opmærksom på, at PSD2 og SecurePay har flere anbefalinger bl.a. omkring anvendelse af stærk autentifikation. Det er hensigtsmæssigt, at medtænke disse anbefalinger, så en kravspecifikation i forbindelse med et NemId-udbud bliver fyldestgørende og fremtidssikret.

Fremtidig forretningsmodel

Vi mener, at det er hensigtsmæssigt, at undersøge om en flere-udbyder-løsning vil passe til danske forhold.

Med venlig hilsen

Alexander Trolle
IT inspektør
Kontor for realkredit

FINANSTILSYNET

Århusgade 110, 2100 København Ø
Tlf.: +45 33 55 82 82 / Fax: +45 33 55 82 00
Direkte tlf.: +45 33 55 82 78
mailto:atr@ftnet.dk
www.finanstilsynet.dk

Fiolstræde 17 B, Postboks 2188, 1017 København K
T: +45 7741 7741, F: +45 7741 7742, fbr@fbr.dk, taenk.dk

Digitaliseringsstyrelsen
Sendt pr. e-mail

27-06-2014
Dok. 142538/ah

Vedrørende offentlig høring om næste generation af den nationale identifikations- og digital signaturinfrastruktur (NemID).

I det vi henviser til Digitaliseringsstyrelsens høringsbrev af 28. maj 2014, skal Forbrugerrådet Tænk hermed fremkomme med nogle generelle bemærkninger til næste generation NemID.

En sikkerhedsnøgle som NemID er et vigtigt værktøj til sikker kommunikation med det offentlige. Når forbrugeren skal se eller oplyse fortrolige og følsomme oplysninger på internettet er høj sikkerhed helt fundamentalt. Tilstrækkelig sikkerhed øger forbrugerens tillid til at anvende digitale tjenester, hvilket sammen med brugervenlighed er en forudsætning for en succesfuld overgang til en fuld digital offentlig forvaltning i Danmark.

NemID har i dag en stor udbredelse, hvilket naturligvis har været vigtigt for hurtigt at få øget det generelle sikkerhedsniveau. Her har brugervenlighed også været et afgørende kriterium for den hurtige udrulning. Forbrugerrådet Tænk mener at tiden derfor er inde til at sætte særlig fokus på beskyttelse af den enkelte forbrugers privatliv i det fremtidige system.

Her bør privatlivsfremmende teknologier som brug af pseudonymer eller andre krypteringsteknologier, som kan "skjule brugernes identitet" være centralt, således at en ny NemID-løsning på én gang skaber sikkerhed og privatlivsbeskyttelse for den enkelte.

Ved at lade én leverandør stå for ét centraliseret system, som sammen med staten håndterer samtlige data i den offentlige og i et vist omfang data i den private sektor, som er tilknyttet NemID, gøres forbrugerne mere sårbare overfor databrud. Både i forhold til den potentielle risiko for hacking, som Rigsrevisionen advarer i mod i deres rapport fra 2013, misbrug som set i Nets-skandalen og ved servernedbrud, som hindrer brugen af NemID.

Vi foreslår derfor, at Digitaliseringsstyrelsen overvejer at åbne op for flere udbydere af digitale signaturer, så der dels kan skabes konkurrence på markedet, dels gives adgang til brug af flere digitale identiteter.

Når man som kan forbruger kan anvende flere digitale identiteter online, fordi man decentraliserer dataopbevaringen og samtidig anvender pseudonymisering, må det antages, at den potentielle risiko for datamisbrug, opbygning af én følsom, digital profil eller sammenkøring på tværs af sektorer minimeres.

I den forbindelse skal vi opfordre Digitaliseringsstyrelsen til at lade sig inspirere af det engelske system, som efter vores oplysninger, netop har flere "NemID"-leverandører, som er underlagt statens sikkerhedskrav, men samtidig sikrer mere databeskyttelse i kraft af decentraliseringen af data og den enkeltes mulighed for at bruge flere identiteter.

Forbrugerrådet
Tænk

Afslutningsvis skal vi anbefale, at den kommende analyse bør indeholde en vurdering af samspillet mellem fremtidens NemID-løsning og de foreslåede regler om tredjepartsadgang til forbrugernes betalingskonto i forslag til revideret direktiv om betalingstjenester.

Med venlig hilsen

Vagn Jelsøe
Vicedirektør

Anette Høyrup
Seniorjurist

28. juli 2014

Digitaliseringsstyrelsen
Landgreven 4
1017 København K

Sendt pr. email til kis@digst.dk og mjrsm@digst.dk

Høring om næste generation af den nationale identifikations- og digitale infrastruktur (NemID)

Jeg skal først på FDIHs vegne beklage, at vi kommer for sent med vores kommentarer til ovenstående høring. En ærgerlig og ganske analog/menneskelig fejl med forkert registrering af høringsdato er grunden, men ikke desto mindre håber vi på jeres forståelse, så vores bemærkninger indgår i arbejdet, ligesom vi meget gerne uddyber dem.

FDIH er Danmarks førende interesseorganisation for virksomheder, der driver handel på eller på anden måde bruger internettet kommercielt. Vores primære virke er inden for e-handel, herunder rammevilkår, lovgivning, betalinger og statistik med hovedvægten på B2C området. Ligeledes deltager vi i tilsvarende arbejde i europæisk regi via Ecommerce Europe.

Vores fokus er primært på det forretningsmæssige, hvor vi arbejder mod en så ukompliceret brug af nettet for såvel virksomheder som borgere. Dette afspejler sig også i vores svar i forhold til de af styrelsens angivne interesseområder.

1. Fremtidige forretningsmæssige behov
Der er grundlæggende et stigende behov for, at deltagerne i kommunikationen på nettet, ikke mindst i e-handel, er sikre på hinandens identitet. Det skyldes primært to forhold; svindel og aftaleindgåelse.

Vi oplever desværre en stigende grad af svindel og misbrug, ofte som en grad af identitetstyveri, fx afluring af betalingskortnumre. Mange betalinger tilbagekaldes efter handlen er indgået, og varen er afsendt. Det er en belastning for såvel borgere, der føler sig udnyttet, som netbutikker, der taber betragtelige summer.

Mulighederne for at tjekke den præcise identitet og placering af kunden er desværre meget vanskelig og ressourcekrævende, hvilket står i skarp kontrast til kundens forventninger om hurtig og gnidningsfri handel på nettet.

En lang række aftaler, herunder telefonabonnementer, kræver allerede i dag et ekstra tjek af kundens identitet, typisk via cpr-kontoret. Her vil et fælles identifikationssystem være en stor hjælp, hvis det i løbet af aftaleindgåelse kan indgå i det løbende flow mellem virksomhed og kunde.

Den stigende grænsehandel via nettet, som EU promoverer kraftigt som det digitale indre marked, vil ligeledes stille stadig større krav til sikker ID. En dansk udvikling af NemID bør derfor tage højde herfor.

Ligeledes er det værd at bemærke, at der arbejdes i EU-systemet for at etablere et fælles europæisk ID-system. Det er et arbejde, hvor vi fra dansk side med den høje grad af national digitalisering bør tage en proaktiv og gerne ledende rolle, ligesom vi bør tage højde for den europæiske udvikling i den kommende udgave af NemID.

FDIH ønsker et identifikationssystem, der i forskellige niveauer kan fastslå identitet af alle parter på nettet. Forretningen kan tjekke en række basisoplysninger, typisk navn og adresse, på kunden, og kunden kan være sikker på, at der faktisk findes et reelt firma bag hjemmesiden. En kobling mellem kundens valgte betalingsmiddel, der i stigende grad er mobiltelefonen, og fremtidens NemID ligger ligeledes lige for. Identifikation og betaling kobles i én arbejdsgang til glæde for både kunde og virksomhed.

Forretningernes behov for at fastslå identitet og bopæl hos deres kunder er i sin natur knapt så omfattende eller følsomme, som de identifikationskrav der forventeligt stilles af offentlige myndigheder til borgeren, når der ønskes adgang til alt fra straffeattester over adgang til egne patientjournal eller skatteoplysninger.

En enkel udgave af NemID med de relevante basisoplysninger bør derfor prioriteres højt. NemID skal fungere på mobile platforme.

2. Funktionalitet og anvendelse

E-handel er i sin natur ”NemShopping”, og derfor er vores ønske til et identifikationssystem, at det er - **nemt!**

Begrebet ”Nem” indebærer for os, at for såvel kunden som netbutikken er der alene behov for en grundlæggende sign-on til systemet. Herefter er det muligt at bruge systemet uden at skulle ”fægte” med flere redskaber fx papkort end det instrument, man selv bruger til at gå på nettet.

Som eksempler vil vi fremhæve nogle af de nyere betalingsløsninger som fx Mobile Pay fra Danske Bank. Efter at man er tilsluttet systemet med behørig identifikation er det meget enkelt at bruge systemet – man skal alene huske sit kodeord.
Den samme funktionalitet kan genfindes i bankers app til netbank, fx Nordea. Den enkle login – uden brug af papkort – giver også mindre begrænsninger i forhold til den fulde netbankløsning, men til daglig brug fungerer det og dækker behovet.

Ligeledes er det væsentligt, at en kommende ID løsning fungerer neutralt i forhold teknologi fx den valgte terminaltype (pc, tablet, mobil etc). ID-løsningen skal altså fungere på alle platforme.

3. Behov for brugervenlighed,
Dette er **helt afgørende**, for alle parter, både virksomheder og borgere. Som ovenfor beskrevet er det lykkedes at etablere løsninger, der nok hviler på den nuværende NemID platform, men som fungerer nemt og gnidningsfrit i hverdagen.
De samme krav om enkelhed og simpel betjening bør være ledetråden i det fremtidige arbejde.

4. Teknik og infrastruktur,
5. Samspil med interessenter,
6. Fremtidig forretningsmodel,

På baggrund af de erfaringer vi har med NemID og til én udbyder af løsningen, Nets, må vi konstatere, at der skal sikres en fremtidig incitamentsstruktur, som sikrer, at kundeorientering og funktionalitet set fra **brugernes** synspunkt prioriteres højt.

Alene forløbet omkring at etablere en NemID løsning på virksomhedsniveau illustrerer med al ønskelig tydelighed, at udgangspunktet må være NemIDs egne behov, og ikke den virkelighed, som virksomhederne færdes i.

7. Andre bemærkninger

Ingen

Vi står meget gerne til rådighed med uddybende kommentarer, ligesom vi også er parate til at deltage i eventuelle arbejdsgrupper inden for vores virkefelt.

De bedste hilsner

Henrik Theil
Public Affairs & Kommunikationschef

Tlf: +45 7225 5667
Mobil +45 2096 5667
E-mail: het@fdih.dk

Digitaliseringsstyrelsen
kis@digst.dk

NemID - svar fra Forsikring & Pension på offentlig høring om næste generation

27.06.2014

Forsikring & Pension
Philip Heymans Allé 1
2900 Hellerup
Tlf. 41 91 91 91
Fax 41 91 91 92
fp@forsikringogpension.dk
www.forsikringogpension.dk

Peder Herbo
IT-chef
Dir. 41 91 91 70
phm@forsikringogpension.dk

Vores ref. PHM
Sagsnr. GES-2014-00202
DokID 340326

Forsikring & Pension er glade for, at beslutningsgrundlaget for næste generation af den nationale identifikations- og digitale signaturinfrastruktur er sendt i offentlig høring.

Forsikring & Pension var ikke med på den officielle høringsliste, hvilket overrasker os, da vores medlemmer (de danske forsikring- og pensionsselskaber) er blandt de private virksomheder, der anvender NemID mest. Vi blev først opmærksomme på denne høring den 11. juni 2014. Vi har derfor ikke haft mulighed for en tilbundsgående drøftelse af høringens indhold med de danske forsikrings- og pensionsselskaber.

NemID omtales som den nationale digitale signatur, men det har alene været ønsker og behov fra de offentlige interessenter og pengeinstitutterne, der er tilgodeset i forbindelse med den hidtidige udvikling af NemID. Private virksomheder er ikke blevet involveret. Forsikring & Pension ser derfor meget gerne, at vi inddrages i den videre udvikling af NemID, eksempelvis ved, at der i Digitaliseringsstyrelsen nedsættes en interessentgrupper/følgegruppe for private virksomheder, der anvender NemID i stort omfang. Der vil vi løbende kunne komme med input og sparring, der vil kunne optimere NemID løsningen til gavn for borgerne og til gavn for produktivitet og effektivitet i virksomhederne og i samfundsøkonomien som helhed.

I forsikring- og pensionsbranchen er vi meget flittige brugere af NemID. Forsikrings- og pensionsselskaberne har etableret mange netservices for deres kunder, der er baseret på NemID. Disse netservices gør det nemmere for forbrugerne at komme i kontakt med deres selskab, at holde sig orienterede og foretage transaktioner. Desuden har branchen i samarbejde med pengeinstitutter, ATP og offentlige myndigheder etableret en fælles portal pensionsinfo.dk, hvor borgerne kan få et samlet overblik over alle deres pensionsrettigheder. I 2012 havde denne portal mere end 3,3 mio. logons fordelt på mere end 1,1 mio. brugere. Portalen er helt unik i verden og påkalder sig stor international opmærksomhed.

På baggrund af dette erfaringsgrundlag har vi følgende ønsker til den fremtidige udvikling af NemID:

1. Fremtidige forretningsmæssige behov

Forsikrings- og pensionsselskaberne har dels udenlandske kunder, dels kunder der er bosiddende i udlandet. Den første gruppe kan ikke få NemID og den anden gruppe har svært ved at få NemID. Det lægger begrænsninger på fuldstændig digitalisering af processer i forsikrings- og pensionsselskaberne, med de urealiserede effektivitetsgevinster det afføder. Vi ønsker derfor, at disse grupper også får mulighed for at få og anvende NemID.

2. Funktionaliteter og anvendelse

Det er altafgørende, at NemID også i fremtiden overholder alle juridiske krav til en gyldig og entydig digital signatur. Hvis de økonomiske gevinster ved én digital signatur skal realiseres, må der ikke kunne rejses tvivl om NemID's gyldighed og ægthed.

Andre private virksomheder end pengeinstitutter bør kunne anvende NemID uden nøglekortskode. Pengeinstitutterne anvender eksempelvis denne en-faktor-løsning, når kunderne blot skal ind at kigge i netbank. Nøglekortskoden skal først anvendes, hvis der også skal udføres transaktioner. Vi har tidligere rettet henvendelse til Digitaliseringsstyrelsen med henblik på at opnå denne mulighed, men blev afvist med henvisning til, at en sådan løsning ikke er tilstrækkelig sikker. Forsikring & Pension føler sig betrygget om, at det sikkerhedsniveau, der generelt anvendes i netbanker, også er tilstrækkeligt for tilsvarende funktionaliteter i forsikrings- og pensionsselskaber.

3. Behov for brugervenlighed.

Forsikring & Pension mener, at det skal være muligt for forsikrings- og pensionsselskaber og andre private virksomheder at viderestille til andre hjemmesider, uden at brugeren igen skal indtaste brugernavn, adgangskode og nøglekortskode. Det er en mulighed pengeinstitutterne har, men som andre private virksomheder ikke har. At vi ikke har denne mulighed forringer brugeroplevelsen og er formentlig med til at fordyre anvendelse af NemID. En ekstraomkostning som i sidste ende bæres af vores kunder.

4. Teknik og infrastruktur

Det er vigtigt, at ændringer i NemID, der afføder behov for ændringer i de private virksomheders set-up for anvendelse af NemID i den daglige forretning, varsles i god tid. Forsikrings- og pensionsselskaberne har omfattende og komplekse it-systemer, hvor udefrakommende ændringsbehov kan have vidtforgrenede konsekvenser. Det kræver tid at tilpasse sig disse ændringer, uden det skal gå ud over kundernes oplevelse og uden det giver behov for, at selskaberne sætter midlertidige nødløsninger op.
Den nuværende standardvarsling som beskrevet i tjenesteudbyderaftalen er ikke tilstrækkelig.

Vi foreslår desuden, at der opsættes et testmiljø for NemID.

5. Samspil med interessenter

Som nævnt indledningsvis foreslår vi en løbende og helst formaliseret dialog mellem Digitaliseringsstyrelsen og de private virksomheder, der anvender NemID. Det mener vi begge parter vil have stor gavn af.

De tjenesteudbyderaftaler, som private virksomheder skal underskrive, når de anvender NemID er hverken juridisk eller teknisk tilstrækkeligt dækkende for de behov forsikrings- og pensionsselskaberne har. Det havde vi et længere forhandlingsforløb med Nets om i 2010 til 2012, der desværre endte resultatløst. Igen kan vi konstatere, at pengeinstitutterne har en særstilling, hvor de har opnået betydeligt bedre vilkår end andre private virksomheder. På visse forretningsområder ligger pensionsselskaber og pengeinstitutter i konkurrence. Konkurrencevilkårene i markedet påvirkes af den ulige behandling.

6. Fremtidig forretningsmodel

Det er Forsikring & Pensions opfattelse, at prisstrukturen for anvendelse af NemId bør gentænkes. Givet NemID's store succes bør stk. prisen kunne sættes ned. Særligt i lyset af NemID's monopolstilling, bør der arbejdes intenst for sikre rimelige priser til gavn for forbrugere og virksomheder.

***

Som sagt har vi haft ganske kort tid til at forhold os til denne høring og vi vil derfor muligvis på et senere tidspunkt spille ind med mere input, som vi mener bør indgå i overvejelserne om den næste generation af NemID. Hvis de synspunkter, vi her er kommet med, giver anledning til spørgsmål, stiller vi naturligvis gerne op til en videre drøftelse.

Med venlig hilsen

Peder Herbo

FORSVARSKOMMANDOEN

Til:
Digitaliseringsstyrelsen

Eft.:
Forsvarsministeriet
Beredskabsstyrelsen
Forsvarets Efterretningstjeneste
Forsvarets Materieltjeneste
Forsvarets Koncernfælles Informatiktjeneste

Emne:
Svar på høring om næste generation af den nationale identifikations- og digital signaturinfrastruktur (NemID)

Dato: 27. juni 2014
Sagsnr.: 2014/005443
Dok.nr.: 1038023
Tillæg: Ingen
Bilag: Ingen
Sagsbeh.: PLI102

Forsvarskommandoen
Danneskiold-Samsøes Allé 1
1434 København K

Tlf.: 4567 4567
Fax: 4589 0748
E-mail: fko@mil.dk
www.forsvaret.dk

EAN: 5798000201507
CVR: 16 28 71 80

Sagsbehandleren direkte:
Tlf.: 4567 3912
E-mail: fko-pli102@mil.dk

Digitaliseringsstyrelsen har ved skrivelse af 28. maj 2014 anmodet om at modtage bemærkninger og bidrag til næste generation af den nationale identifikations- og digital signaturinfrastruktur (NemID).

Forsvarskommandoen (FKO) har på Forsvarsministeriets vegne følgende bemærkninger til høringen.

Fremtidige forretningsmæssige behov.
FKO har behov for, at flere medarbejdere har mulighed for logon med NemID således den enkelte medarbejder enkelt og fleksibelt kan logge på sikre systemer. Logon bør kunne foretages fra såvel intranet som internet og systemet skal kunne registrere hvilke brugere der logger på.
Funktionalitet og anvendelse.
Afhængig af den tekniske løsning, finder FKO det relevant at kunne administrere adgang via NemID lokalt ved de enkelte myndigheder. Dette vil understøtte enkelthed og fleksibilitet. Dermed vil anvendelsen af NemID formentlig ikke blive oplevet som besværlig men som et "værktøj" i hverdagen.
Behov for brugervenlighed.
Det bør være enkelt og fleksibelt at oprette og nedlægge brugere af NemID. Dette bør ikke overstige 2-5 hverdage. Det er væsentligt, at brugervenligheden er høj således medarbejdere og brugere reelt oplever, at "produktet" har en lav kompleksitet. Hvis kompleksiteten opleves som høj, øges risikoen for, at brugerne ikke anvender systemet. Hertil kommer betydningen af kompabiliet. Hvis brugerne oplever stort sammenfald mellem det system der bruges privat og det system

FRIGIVET TIL INTERNETTET

der bruges på arbejdspladsen, så opleves systemet mindre kompleks og bruger-venligt.

Med venlig hilsen

JESPER HAMMER
major
Sagsbehandler

FRIGIVET TIL INTERNETTET

Høringssvar

Vedr. Offentlig høring om næste generation af den nationale identifikations- og digital signaturinfrastruktur (NemID)

Afsender	Henrik Schack
Dato	2. juni 2014

Hej Digitaliseringsstyrelse

Jeg faldt lige over http://hoeringsportalen.dk/Hearing/Details/33814 via et link fra version2.dk

Jeg er overhovedet ikke klar over hvordan man overholder formalia i forbindelse med denne her slags aktiviteter, så i får bare min ide på godt gammeldags dansk.

Vedrørende "4. Teknik og infrastruktur"

Det ville være godt for næste version af NemID hvis der blev gjort lidt ved de mange problemer der idag eksisterer med Phishing.

Den for tiden bedste tekniske løsning hedder DMARC (http://www.dmarc.org) DMARC løser ikke alle problemer, men implementeres DMARC kan man ihvertfald sige man har gjort alt der pt er teknisk muligt at gøre ved phishing, modsat idag hvor Nemid.nu domænenavnet ligger fuldkommen ubeskyttet og kan misbruges frit af enhver kriminel.

--

Mvh/Best regards
Henrik Schack
Blog: http://henrik.schack.dk/

HÅNDVÆRKSRÅDET
for små og mellemstore virksomheder

Digitaliseringsstyrelsen
kis@digst.dk
Att: mjrsm@digst.dk

Islands Brygge 26
Postbox 1990
2300 København S

tlf. 33 93 20 00
fax 33 32 01 74

hvr@hvr.dk
hvr.dk

4. juli 2014

Høringssvar til udbud af næste generation af den nationale identifikations- og digital signaturinfrastruktur (NemID)

Håndværksrådet tanker for det fremsendte høringsmateriale beklager det sene svar fra vores side. Nedenfor afgives kommentar til de enkelte temaer:

Generelt bør man overveje tilgangen og brugervenligheden i et system, som nu er obligatorisk for alle virksomheder. Prioriteres ressourcerne korrekt, så vil de digitalløsninger kunne give gevinst for alle parter.

Ad 1 – fremtidige forretningsmæssige behov
Gevinsten ved brug af NemID skal gøres synlig for virksomheden, så det ikke bliver opfattet som en ny administrativ byrde. NemID giver mulighed for 24-7 opkobling og kontakt med myndighederne, og derfor er oppetid en væsentlig parameter. Samtidig må og skal en tilgængelig tværgående support være tilstede, så brugeren upfront hjælpes med evt. problemer.

Ad 2 – funktionalitet og anvendelse
Der er behov for en eller flere administrator(er) på den enkelte virksomheds NemID, og det skal sikres, at man kan parre flere CVR-numres NemID. Således en administrator relativ let kan have overblik, og styre autorisation for det enkelte medarbejder NemID. Muligheden for at kopiere autorisationen mellem forskellige CVR-numre skal overvejes. Eksempelvis hvis der er tale om et selskab, der kontrollerer flere CVR-numre og der i selskabet er et antal medarbejde, som på den ene eller anden måde har behov for adgang, så skal opsætningen for det ene CVR-nummer kunne spejles til de øvrige CVR-numre og så fremdeles.

Det bør overvejes hvor vidt adgang kun skal sikres med nøglekort, eller om der tilbydes alternative adgangsmuligheder. Eksempelvis SMS-kode eller andet, som kan gøre adgangen mere fleksibel og håndholdt.

Ad 3 – behov for brugervenlighed
Der skal allokeres flere ressourcer ift. bestilling og opsætning af NemID, samtidig med at supporten skal sikres. Nye brugere bliver ofte hægtet af allerede i opstarten, hvor

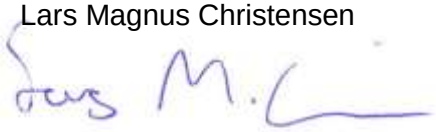
der sendes forskellige mail-adviseringer, som ikke kan være svære at tolke. Derfor er bestilling til anvendelse en af de vigtigste faser ift. anvendelse af NemID.

Ingen kommentarer til pkt. 4-7

Håndværksrådet stiller sig naturligvis til rådighed i forbindelse med uddybende spørgsmål eller kommentar.

Med venlig hilsen

Lars Magnus Christensen



INSTITUT FOR
MENNESKE
RETTIGHEDER

WILDERS PLADS 8K
1403 KØBENHAVN K
TELEFON 3269 8888
DIREKTE 32698979
MOBIL 32698979
EMKI@HUMANRIGHTS.DK
MENNESKERET.DK

J. NR.
540.10/30790/MPED/RFJ/EMKI

25. JUNI 2014

Digitaliseringsstyrelsen
kis@digst.dk

OFFENTLIG HØRING OM NÆSTE GENERATION AF DEN NATIONALE IDENTIFIKATIONS- OG DIGITAL SIGNATURINFRASTRUKTUR

Digitaliseringsstyrelsen har ved e-mail af 2. juni 2014 anmodet om Institut for Menneskerettigheders eventuelle bemærkninger til den fremtidige identifikations- og digital infrastruktur.

Instituttet har følgende bemærkninger:

RETTEN TIL PRIVATLIV

Instituttet gør indledningsvis opmærksom på, at it-løsninger der behandler personoplysninger ofte vil have konsekvenser for beskyttelsen af borgeres ret til privatliv.

Instituttet vil derfor foreslå, at der i forbindelse med valg af den fremtidige identifikationsløsning udarbejdes en analyse af påvirkningen af retten til privatliv, jf. den "Guide til konsekvensvurdering af privatlivsbeskyttelse" og tilhørende Vejledning som Digitaliseringsstyrelsen har udarbejdet.

Institut for Menneskerettigheder anbefaler – med henblik på at fremme den enkeltes menneskerettigheder – at

- der, i det samlede beslutningsgrundlag for fremtidens identifikations- og digital signaturinfrastruktur, indgår en analyse af de privatlivsmæssige implikationer ved valget af mulige løsninger.

HØRINGSBREVETS PKT. 3: BEHOV FOR BRUGERVENLIGHED

PERSONER MED HANDICAP

Danmark bliver mere og mere digitalt. I den forbindelse er det vigtigt at sikre, at den nye digitale verden bliver tilgængelig for alle. Desværre

viser Digitaliseringsstyrelsens kortlægning af offentlige hjemmesiders tilgængelighed fra december 2012, at 34 % af offentlige hjemmesider har en mangelfuld tilgængelighed. Det vil sige, at hjemmesiderne har adskillige formelle tilgængelighedsfejl og flere væsentlige funktioner og/eller væsentligt indhold, som ikke kan anvendes af alle brugere. Samtidig anvendes digitale løsninger – herunder identifikations- og digital signaturinfrastruktur – i stigende grad, også som obligatoriske løsninger for borgerne.

Digitalisering kan på mange måder være positivt for bl.a. personer med handicap, fordi mange gennem it kan opleve større mulighed for selv at tilegne sig viden og kommunikere på lige fod med andre. Det forudsætter imidlertid, at de digitale løsninger ikke blot er brugervenlige men også tilgængelige for personer med forskellige handicaps.

Brugervenlighed er ikke det samme som tilgængelighed. Manglende brugervenlighed rammer således både personer med handicap og personer uden handicap. Men manglende brugervenlighed vil ramme personer med handicap særligt hårdt, hvis de i forvejen har problemer med at navigere digitalt på grund af manglende tilgængelighed.

MENNESKERETTIGHEDERNE

FN's handicapkonvention artikel 9 indeholder en ret til tilgængelighed, der betyder, at Danmark skal arbejde for, at samfundet – herunder samfundets digitale løsninger - er tilgængelige for alle.

Tilgængelighed er en af de grundlæggende rettigheder i FN's handicapkonvention. Tilgængelige omgivelser er således også en forudsætning for, at mange af konventionens øvrige rettigheder kan opfyldes. Artikel 9 fastslår, at Danmark har pligt til at fremme adgangen for personer med handicap til fysiske omgivelser, transportmuligheder, information, kommunikation og øvrige faciliteter, som er tilgængelige for offentligheden. Tilgængelighed angår således meget mere end blot tilgængelighed til fysiske strukturer. Artikel 9 indeholder således også en ret til tilgængelighed til blandt andet hjemmesider og andre digitale faciliteter.

Retten til tilgængelighed gælder også, selvom borgerne kan undtages for de digitale løsninger ved fx fortsat at anvende almindelig post. Muligheden for at blive undtaget for de obligatoriske digitale løsninger må således aldrig fungere som alternativ til at gøre de digitale løsninger tilgængelige, da dette ville ekskludere personer med handicap for at deltage i samfundet på lige fod med andre.

EU Kommissionen har i december 2012 fremlagt et forslag til direktiv om tilgængeligheden af offentlige organers websteder, der har som målsætning at sikre personer med handicap adgang til offentlige hjemmesider (COM (2012) 721). Direktivet er endnu ikke endeligt vedtaget, men det bør allerede nu sikres, at de nye digitale løsninger, der vælges i dag, lever op til de standarder om tilgængelighed, som direktivet henviser til.

Regeringen har i sin Handicappolitiske Handlingsplan fra 2013 fastsat et mål om, at alle obligatoriske digitale offentlige selvbetjeningsløsninger skal være fuldt tilgængelige for personer med handicap.

ANBEFALINGER

Institut for Menneskerettigheder anbefaler – med henblik på at styrke vidensgrundlaget – at

- tilgængelighedsproblemer med den nuværende identifikations- og digitale signaturinfrastruktur identificeres.

- personer med handicap inddrages i processen med at etablere et beslutningsgrundlag for anskaffelse af den næste generation af den nationale identifikations- og digital signaturinfrastruktur.

Institut for Menneskerettigheder anbefaler – med henblik på at sikre at krænkelse af menneskeretten undgås – at

- tilgængelighed indgår som en betingelse for valget af den næste generation af den nationale identifikations- og digital signaturinfrastruktur.

Der henvises til j.nr.: 2014-5155-013.

Med venlig hilsen

Emil Kiørboe

FULDMÆGTIG

IT-Branchen

27.06.2014

IT-Branchens høringssvar vedrørende næste generation af den nationale identifikations og digital signaturinfrastruktur Nemid

IT-Branchen takker for muligheden for at bidrage til høringen. At skabe en tidssvarende, sammenhængende, velfungerende, brugervenlig og økonomisk forsvarlig digital identitet for borgerne i Danmark er et stærkt ønske blandt IT-Branchens medlemmer.

En åben proces om komplekse valg
Danmark er kommet langt med nuværende Nemid der er udviklet og udbredt i et effektfuldt samarbejde mellem offentlige aktører og private aktører, herunder den finansielle sektor.

Nu skal vi fremtidssikre os som samfund til i en ny årrække at give danskerne muligheder for trygt at kunne agere digitalt – identificerende, autentificerende og signerende. Både som privatpersoner og som medarbejdere i myndigheder eller virksomheder.

Det handler ikke kun om tekniske udfordringer, som eksperter kan give faglige svar på. Der skal også træffes valg om udbudsmodeller og organisering, som medfører fordele og ulemper, der sætter rammer for hvilke løsninger og aktører, der skal samarbejde om danskernes e-id fremover. Det er svære valg, som skal træffes på et oplyst og åbent gennemdebatteret grundlag.

De trufne valg skal understøtte en morgendag, hvor e-id ikke kun primært bruges i dialogen med det offentlige og med banken. Men også i langt højere grad af og imellem virksomheder, og af og mellem medarbejdere og privatpersoner.

Konkurrence og forretning
IT-branchen ser det som en central udfordring hvordan det offentlige skal understøtte muligheden for flere aktøerer på levering af fremtidens e-ID.

Hvis der satses på et udbud med én vindende leverandør til eks. den offentlige og finansielle sektor giver det fordele mht. at tilpasse systemer dertil. Det skaber genkendelighed for brugerne at der er en og samme løsning at forholde sig til, og det gør opfølgning lettere på, om de opstillede krav om eks. stabilitet og funktionalitet overholdes. Én vindende leverandør vil have bedre økonomi til at videreudvikle på løsningen til samfundets løbende ændrede behov og til at imødegå trusler mod eks. sikkerhed og driftsstabilitet.

Omvendt vil det gøre det svært for et bredere felt af leverandører at overleve på markedet med alternative eid-løsninger, der kan være gode svar på specifikke behov i dele af markedet. Der vil i så fald skulle tænkes i, hvordan det undgås, at en leverandør til offentlig sektor/bankerne får en udkonkurrerende markedsfordel mod aktører med løsninger, der er målrettet den private sektor.

Satses der på en markedsdreven tilgang med flere sideløbende løsninger kommer der valgfrihed og løbende konkurrence der styrker innovation og giver nye forretningsmodeller mulighed for at vise deres værd.

Muligheden for i samfundet at kunne identificere og signere digitalt kan måske lettere opretholdes, med flere sideløbende løsninger, der kan bruges til samme formål. Der er ingen tvivl om, at det i et digitalt samfund er frustrerende for både leverandør, forbrugere og virksomheder, hvis den ene løsning man plejer at bruge, er utilgængelig grundet nedbrud eller ondsindet cyberangreb. Derfor kan en mulighed også være at stille krav om en fall-back-løsning.

IT-Branchen opfordrer til, at det analyseres i hvilket omfang der i udlandet (eks. England) med succes er fundet implementeringsparadigmer for hvordan et multi-leverandør system kan fungere, og hvilke læringspunkter det kan bidrage med til en dansk model.

Er der herfra viden om det er realistisk at myndigheder/virksomheder vil bære medomkostningerne ved at tilpasse systemer til i udbredt grad at kunne anvende flere sideløbende e-id løsninger? Er valgmulighed omkring e-id en styrke eller barriere for udbredt digitalisering?

Med en markedsdreven tilgang vil flere leverandører byde sig til med løsninger på bl.a. de lavere sikkerhedsniveauer. Spørgsmålet er om og hvordan det samtidig kan gøres kommercielt rentabelt at levere løsninger på et lille dansk marked, der modsvarer kravene til de meget høje sikkerhedsniveauer, der er brug for at have udbredt og anvendt bredt. Brug af standardiserede og internationale krav er da vigtigt, så en løsnings rentabilitet kan styrkes på tværs af flere markeder.

IT-Branchen er fortaler for markedskonkurrence. Vi mener det er sundere med flere leverandører på et marked. Men vi anerkender at dette er et område, hvor principper skal opvejes mod andre komplekse hensyn. Vi anbefaler ikke på forhånd én udbudsmodel, men opfordrer i stedet til, at Digitaliseringsstyrelsen går i tæt dialog med branchens store og små leverandører, om at finde det bedst mulige match af balancerede hensyn. Og derfra om at forklare nuancerne og konsekvenser af valget for beslutningstagerne.

Den brede dialog herom er godt påbegyndt med denne høring, men den skal opretholdes i den videre proces. Også her ser IT-Branchen frem til at bidrage.

Nedenfor gives yderligere konkrete input, opdelt efter høringens 7 tematikker.

- **Tema 1 - Fremtidige forretningsmæssige behov, for henholdsvis virksomheder, offentlige sektor og borgere i Danmark og udlandet samt eventuelle juridiske forhold**

  Privat sektor: Intensiveret opmærksomhed på behov og digitale potentialer for at identificere og signere i det private erhvervsliv. Eks. til brug for webbutikker, intranet, aftaler B2B samt B2C, sikker mail og kommunikation.
  Det offentlige: Fortsat fokus på udbredt standardiseret brug af e-id i det offentlige.
  Børn og Unge: E-id løsninger til børn og unge, samt til brug for tjenester der benyttes af privatpersoner, og hvor sikkerhed i dag ikke er højt prioriteret. Eks. pga. frygt for at sætte adgangsbaren for højt, for nye kunder/brugere.
  Datakilder: Fokus på også at højne kvalitet i og adgang til tilknyttede registre, eks. Pas, Kørekortregistre, CVR mm, for at kunne øge funktionaliteten i tjenester der baserer sig på e-id. Herunder eks. adgang til Skats e-indkomst-register der kan bruges til at angive rolle-baseret tilhørsforhold i virksomheder.
  Lovgivning: Mere fokus og opfølgning på lovmæssige udfordringer, fx Retsplejeloven

- **Tema 2 - Funktionalitet og anvendelse, herunder eksempelvis niveaudelt sikkerhed, lokal administration af autorisation, single sign-on mv.**

  Niveaudelt sikkerhed: E-id med niveaudelt sikkerhed, baseret på ensartede, internationalt

anerkendte standarder. Der er både brug for 1 faktor og for 2 faktor sikkerhed – sidstnævnte ikke kun med nøglekort, men også elektronisk authentificerings-mekanismer. Mulighed for at styrke sikkerheden yderligere med kombinationer af eks. biometriske data eller yderligere digitale beviser fra de devices og netværk brugeren anvender. Evt. mulighed for pseudonymificering.
Ens og testbare krav: Der er brug for testbare krav til sikkerhed og tilgængelighed, som i en model med flere leverandører skal være ens for alle leverandører til hvert sikkerhedsniveau.
Nøgler: Der skal være åbenhed for, at løsninger både skal kunne operere med en central og en decentral opbevaring af nøgler. IT-Branchen vurderer, at det for mange privatpersoner uden dybere teknisk forståelse også i en årrække frem vil være at foretrække både af hensyn til sikkerhed og brugervenlighed med en central placering af nøgle. Afgørende er dog at brugerne har tillid til den løsning de anvender. Hvis nogle – borgere eller virksomheder – er mere tryg ved at deres nøgler er decentralt placeret, så skal de kunne anmode om det.
Fuldmagt- og rollestyring: Så eks. en person, med samme e-id kan udstyres med rettigheder/attributter, der gør at vedkommende kan identificere/signere på vegne af andre personer eller for flere virksomheder. Uden at skulle anvende forskellige e-ids for hver virksomhed.
Let integration: Mulighed for på enkel måde at blive en del af en "E-id" føderation med veldefinerede politikker og overkommelig tekniske integration

Tema 3 - Behov for brugervenlighed, herunder forskellige brugeres aktiviteter fra bestilling til anvendelse og eventuel spærring mv.

Brugeroplevelse: En ensartet brugeroplevelse ved brug af E-id på både PC- og mobile platforme er ønskelig. Ved en evt. multi-leverandør strategi kan det eks. sikres ved at der i fællesskab etableres en ensartet brugergrænseflade for bestilling, anvendelse, spærring m.v hvori den enkelte signatur-leverandør integrerer sin signaturløsning

Tema 4 -Teknik og infrastruktur, herunder eksempelvis adskillelse af eID og eSignering, single sign-on, sammenhængende IT-arkitektur, sikkerhed mv.

Platform: Skal fungere på tværs af teknologiske platforme (java, .net, linux etc.)
Hardware: Skal fungere på tværs af hardware enheder (som PC, Slates, Tablets, SmartPhones etc.)
Internationalisering: Skal virke sammen med internationale, herunder nordiske og europæiske e-id-løsninger.
Interoperabilitet med andre identityprovidere som fx sociale medier og det bør sikres, at borgerne kan forbinde loyalitetskort m.v. til ens digitale identitet, således at danskerne – der måtte ønske det – kan anvende sin digitale identitet til al elektronisk identitetskrævende interaktion.

Tema 5 - Samspil med interessenter, herunder tjenesteudbydere, administrative procedurer, sikkerhedsprocedurer mv.

Brug af flere **åbne standarder**

Tema 6 - Fremtidig forretningsmodel, herunder leverandørstyring, support, betalingsstruktur, en model med flere leverandører mv.

Central certificeringsinstans – som beskrevet ovenfor er der ikke en entydig anbefaling med hensyn til én / flere leverandører. Det er IT-Branchens vurdering, at en fuldstændig

udrulning på tværs af brancher og services, kræver at der skabes en attraktiv økonomisk model for såvel brugere som service-leverandør. En central og uvildig certificeringsinstans er dog afgørende for at flere leverandører kan få verificeret at deres løsning lever op til fælles standardiserede krav.

Betalinger: IT-Branchen anbefaler frihed til at udvikle og anvende forskellige forretningsmodeller. Bærende for en forsat masseanvendelse blandt borgerne bør dog fortsat være, at borgernes brug af den digitale identitet er gratis. Evt. med mulighed for at sælges mere avancerede "nøgle-visere", kortlæsere mv.

Tema 7 – Andre bemærkninger

Kryptering: Anvendelse af nyere krypteringsstandarder, eks. XADES, som tillader lang gyldighed i signaturer.

For yderligere kontakt venligst: Bjørn Borre, Chefkonsulent, bjb@itb.dk Tlf. 72255502

IT-Politisk Forenings høringssvar om næste generation af den nationale identifikations- og digital signaturinfrastruktur (NemID)

Vi er glade for, at der denne gang kommer en høring inden de overordnede principper i den nye løsning fastlægges – i modsætning til den første version af NemID, som i 2008 blev forhandlet på plads før høringen. Vi finder det afgørende at analysearbejdet til brug for den næste version af NemID sker i åbenhed, så borgere, virksomheder og politikere har mulighed for at følge processes. For IT-Politisk Forening er det ikke kun et spørgsmål om pris, teknik og udbredelse. Det handler også om respekt for borgernes privatliv og frie valg af applikationer.

Overordnede principper

- Borgerne skal så vidt muligt kunne bruge NemID på den måde som de selv finder hensigsmæssigt.
- NemID skal være fleksibelt, så det kan bruges til mere end hvad man kan forestille sig i dag.
- NemID skal så vidt muligt kunne fungere decentralt, så man ikke er afhængige af centrale servere.
- NemID skal i størst muligt omfang baseres på internationale standarder.

Fremtidige forretningsmæssige behov

I dag bruges NemID hovedsageligt til single sign-on til banker og offentlige systemer. Der er meget få applikationer, der kræver rigtige digitale signaturer. Det er meget få emails, der bliver signeret eller krypteret med OCES NemID. Kommunikation mellem borgere og virksomheder og myndigheder kommer til at foregå gennem dokumentbox, hvor NemID kun bruges til sign-on. Selv den digitale tinglysning foregår ved, at man logger ind på en hjemmeside. I sådanne tilfælde bør der ikke signeres med den enkelte borgers signatur, men med f.x. Domstolsstyrelsens signatur, idet der reelt skrives under på, at man har kontrolleret, at det var den pågældende borger, der var logget ind. Derfor mener IT-Politisk Forening, at det vil give bedst mening at lave en offentlig single sign-on løsning, der ikke baserer sig på digitale signaturer. Det vil gøre implementationen langt simplere og dermed give mulighed for at flere leverandører kan implementere løsningen. I de tilfælde, hvor der reelt er brug for en ægte, digital signatur, er der typisk tale om avanceret brug i form af f.x. automatisering eller anvendelse i et klientprogram. Det vil være omsonst at gætte på, hvad fremtidens behov vil være i detaljer - derfor er det vigtigt, at digitale signaturer kan anvendes fleksibelt uden at være bundet op på en central server eller en speciel teknologi. De avancerede brugere, der har behov for at kunne anvende en ægte digital signatur, bør derfor have fri adgang til deres nøgle og certifikat.

Teknik og infrastruktur

Primært single sign-on

IT-Politisk Forening foreslår, at det nye NemID primært fungerer som single sign-on, og at NemLogin i OIO arkitekturrammen bliver hjørnestenen i det nye NemID. Fra brugernes side skal løsningen kunne anvendes med ren HTML, dvs. uden brug af Java, JavaScript, Flash, Active-X, Silverlight og lignende. Det vil gøre det muligt at bruge løsningen på stort set alle gængse platforme. Borgerene og virksomheder har krav på, at login til offentlige services - og andre services, som de er lovmæssigt forpligtet til at anvende - virker med ren HTML.

Certifikater

Det vil kun være avancerede brugere, der har brug for en digital signatur. Til dette formål kan single sign-on løsningen anvendes til en tjeneste, hvor borgere og virksomheder kan få udstedt digitale signaturer.

Det er helt afgørende, at brugerne selv kan generere og opbevare de certifikater, som de får signeret af NemID. Det er afgørende for at borgerne kan have tillid til NemID og for at kunne bruge certifikaterne decentralt.

NemID skal kunne signere nøgler fra gængse certifikatformer, herunder X.509 og OpenPGP, som begge er internationalt udbredte og understøttet i mange eksisterende applikationer. Det skal være muligt at få udstedt så mange certifikater, man ønsker, og det skal være muligt for brugerne at vælge, hvilke verificerbare attributter, der skal være med i de enkelte certifikater, f.x. navn, adresse, CPR-nummer.

Certifikatudstedelsestjenesten skal også indeholde mulighed for at spærre certifikater ved at tilføje dem til en central revokeringsliste.

Grænseflader

Der skal udvikles et API til udstedelse af certifikater, og et API til single sign-on. Udover at borgere og virksomheder kan bruge en web-baseret single sign-on løsning til at tilgå tjenester på nettet og til at få signeret deres certikater, skal de også kunne bruge de underlæggende OIO grænseflader. Veldokumenterede API'er gør det muligt at lave forskellige konkurrende klienter eller indbygge klienterne i forskellige programmer, så det bliver nemmere at benytte. For eksempel vil det være muligt for økonomiprogrammer, at koble op mod banken; eller ens kalenderprogram kunne koble op til lægens kalender og foreslå en tid, hvor begge kan. Dette vil muliggøre automatisering og understøtte udbredelsen af digitalisering.

Forretningsmodel

Servicen skal udbydes af staten. Staten skal tilbyde, at single sign-on-delen kan anvendes af andre tjenester mod at ejerne af de disse betaler nogle få ører per login. Ved at løsrive den digitale signatur fra single sign-on-delen, bliver single sign-on-delen væsentlig billigere at implementere og drive. Eventuelt kan staten lade flere leverandører tilbyde parallelle single sign-on løsninger, som brugerne frit kan vælge imellem. Sådanne løsninger skal certificeres af staten, og en certifikation skal i så fald medføre, at løsningen kan anvendes på alle de sider, som tilbyder login med NemID. De enkelte leverandører vil ligeledes modtage betaling pr. login fra de hjemmesider, som anvender NemID. Hvis der vælges en løsning med flere leverandører, bør alle leverandører have lige adgang til indrullering via Borgerservice, og det skal være muligt at indrullere via en anden leverandør. På den måde vil borgere og virksomheder kunne vælge den leverandør (eller flere leverandører), som udbyder den bedste service. Certifikatsigneringstjenesten vil betyde, at certifikater bliver opbevaret decentralt og at der dermed ikke kan forventes en indtjening ved hver brug af en ægte digital signatur. Til gengæld vil der ikke være behov for en central tjeneste til hver brug af signaturen, bortset fra drift af en revokeringsliste. Samlet vil det betyde, at der bliver færre barrierer for at anvende den ægte digitale signatur. Support kan opdeles følgende scenarier:

- **Indrullering.** Til dette er der brug for en troværdig, bred lokal repræsentation. Den nuværende løsning med Borgerservice fungerer udmærket. Ikke mindst i betragtning af, at de fleste borgere allerede er indrulleret i den eksisterende NemID og derfor ikke skal indrulleres igen. Udover dette vil der være brug for en driftsorganisation til indrullering af virksomheder. Dette kunne integreres i Virk.dk
- **Drift**. Herunder f.x. udsendelse af nye nøglekort. I en model med flere leverandører kunne dette foretages af de enkelte leverandører.
- **Vejledning**. Det må forventes, at der er brug for væsentligt mindre vejledning, hvis løsningen bliver simplere og ikke kræver brug af særlig software. I en løsning med flere leverandører vil det påhvile den enkelte leverandør at vejlede om sin egen løsning.

DIREKTORATET FOR KRIMINALFORSORGEN
KONCERN-IT

HØRINGSSVAR

Dato	25.06.2014	Sagsnr.	14-049-0014
Emne	Høringssvar vedr. næste generation af den nationale identifikations- og digital signaturinfrastruktur (NemID)		
Til	Departementet		
Kopi til	Kristina Skovdal og Ole Makne Jørgensen		
Sagsbehandler	Charlotte Bjerrum-Niese		

Hermed svar fra Justitsministeriets Koncern-IT på høring af 28. maj 2014 om næste generation af den nationale identifikations- og digital signaturinfrastruktur. (NemID).

Justitsministeriets Koncern-IT fungerer som rådgivende på digitaliseringsområdet for en række institutioner og myndigheder under Justitsministeriets ressort og repræsenterer derved flere myndigheders interesser i relation til høringen.

1. **Fremtidige forretningsbehov**
    a. Der er behov for at kunne anvende internationalt ID i sammenhæng med den danske identifikationsløsning, en form for udveksling af persondata med betroede internationale parter.

2. **Funktionalitet og anvendelse**
    a. Sikkerhedsniveauet skal være højt
    b. NemID kunne indarbejdes i et nationalt identifikationskort.
    c. Der bør etableres ekstra sikkerhed ved at brugeren skal svares på personlige spørgsmål som f.eks.: hvor er du født, hvilken skole gik du på osv.
    d. Der bør ikke indgå CPR nr. i NemID
    e. Der bør være teknologiuafhængighed
    f. Der bør være platformuafhængighed
    g. Det foreslås, at man lægger sig op af en ISO standard f.eks.17839 eller tilføjer biometri omsat til matematisk algoritme.

3. **Behov for brugervenlighed**
   Ingen bemærkninger.

4. **Teknik og infrastruktur**
    a. <u>"Single sign-on" på tværs af services.</u>
    Det bør være muligt at anvende samme login på tværs af services f.eks. på Borger.dk, således at services indeholder information om hvilket niveau af autentifikation, der er nødvendig for at tilgå en service.

b. SAML-protokollen bør genovervejes.
Der skal udvikles bedre modeller for understøttelse af REST f.eks. mhp. cloud. SAML-protokollen skal genovervejes i forhold til andre muligheder. der er typisk stadig problemer med at udveksle SAML 2.0 internt, hvorfor mange services modtager SAML 2.0 tokens, men veksler dem til SAML 1.1 og ikke veksler dem tilbage. Det er således ikke muligt at bevare sin session på tværs af myndighedsservices uden at skulle logge ind igen. Der er behov for en mere smidig udveksling mellem applikationer og serviceudbydere, samt bedre cloud-parathed.

c. eID bør forberedes til højere autentifikationsniveau.
Et fremtidigt eID bør forberedes til et højere autentifikationsniveau f.eks. ved at udvide persondatamodellen med biometriske data. Dette kan bruges til udveksling af af data imellem betroede parter, og åbner også for en fleksibel anvendelse til f.eks. døre, rejsekort, etc.
Der bør ikke opbevares biometriske data, men udelukkende matematiske værdier, således at en persons biometri altid veksles ved hjælp af en algoritme og at det er sammenligning af de matematiske værdier som bruges til autentificering. Mønsteret bør være i overensstemmelse med EU-kommissionens regler for personhøringer mellem lande.

5. Fremtidig forretningsmodel
Ingen bemærkninger.

6. Andre bemærkninger
Ingen bemærkninger.

Til Digitaliseringsstyrelsen

Vedrørende Offentlig høring om næste generation af den nationale identifikations- og digital signaturinfrastruktur (NemID)

IT-brancheforeningen Professionelle Linux-interessenter I Danmark (KLID) påskønner at kunne komme med vores kommentarer til denne høring.

Funktionalitet

Løsningen skal alle steder kunne håndtere analog autorisation, i form af håndskreven underskift på papir, som dernæst kan indskannes og behandles digitalt. Der er undtagelsesbestemmelser for Digital Post i dansk dansk lovgivning både for borgere og virksomheder. og myndighederne regner med at omkring 20 % af borgerne får undtagelsesgodkendelse, eller omkring 1 million borgere i Danmark. Det kan også forventes at andre EU-medlemstater ikke vil kunne have digitale løsninger, eller have digitale løsninger med bedre kvalitet end de danske løsninger, og den nye arkitektur må nødvendigvis også kunne håndtere dette.

Teknisk infrastruktur

Vi mener at der skal etableres en arkitektur der kan håndtere den eksisterende mængde af løsninger, inklusive papkortløsningen og X.500 løsningen, men at arkitekturen også skal kunne behandle kommende udenlandske eID løsninger og en ny NemID-løsning.

Løsningen skal være bygget på åbne standarder, herunder X.500, offentliggjorte procedurer og gensidig trust-netværk (a.l.a. pgp) med deklarede sikkerhedsniveauer, så flere udbydere kan løse opgaven og interagere med hinanden.

Support for OCES-certifikater (a.k.a. NemID på hardware) i den nuværende løsning skal fortsat understøttes som Open Source og godkendelse af Hardware skal være en offentlig opgave - ikke som nu hvor én ~~virk~~somhed - Nets/DanID, kun tillader én, noget obskur leverandør - for at undgå konkurrence til deres øvrige NemID-løsninger.

Løsningen skal bygge på open source, for at der kan ske peer review, og løsningen er alligevel betalt af offentlige midler.

Løsningen bør ikke bruge Java af sikkerhedsmæssige og distributionsmæssige årsager.

Fremtidige forretningsmæssige forhold

Det skal understreges, at der gælder samme regler for identitetstyveri og dokumentfalsk - at det er "modtagere" der bærer ansvaret - ikke dem, hvis identitet stjæles/forfalskes.

Andet

Iøvrigt henvises til britiske og svenske løsninger.

Med venlig hilsen

Keld Simonsen
Formand for KLID
bestyrelse@klid.dk

NOTAT

Erfaringsopsamling vedr. NemID fra kommunerne

Den 27. maj 2014

Sags ID: SAG-2014-01164
Dok.ID: 1864361

PFL@kl.dk
Direkte 3370 3736
Mobil 2913 1728

Weidekampsgade 10
Postboks 3370
2300 København S

www.kl.dk
Side 1/4

Generel kvalitativ vurdering af den eksisterende NemID-løsning

Kommunerne oplever overvejende tilfredshed med den eksisterende NemID-løsning. Dette gælder såvel for brugere og administratorer. Dog melder kommunerne tilbage at:

- Der har været udfordringer med at få leverandørerne til at tage NemID Erhverv i anvendelse – da det ikke er en komponent de ellers anvender med andre "kunder". Den administrative del af medarbejdercertifikater har været "tung", herunder etableringsprocessen.

- NemID på mobile platforme har længe været et udækket forretningsmæssigt behov.

- Der er et forretningsmæssigt behov for at anvende en mere differentieret tilgang til sikkerhedsniveauet som det bl.a. kendes fra bankernes løsninger. For medarbejderen i kommunen kan det eks. være i relation til at tilgå den enkelte kommunes intranet.

- Legitimationskravene nævnes også som begrænsende faktor i relation til at hjælpe bestemte grupper af borgere. Eksempelvis i de tilfælde, hvor borgeren kun har tilknyttet NemID til banken, men ønsker at anvende det til de offentlige sider også. Der kræves det fra NemID's side, at borgen har gyldig billede legitimation, hvis ikke der skal oprettes et NemID på ny. Borgeren har da to NemID og er nødsaget til at logge på med to forskellige NemID numre samt nøgle-kort i stedet for blot at bruge cpr nr. Ved adressebeskyt-

telse er det ikke muligt at fremsende NemID-materiale til borgere som kun har fremvist legitimation uden billede.

- I forhold til selvbetjeningsløsningerne – hvor borgerne både bruger NemID til at logge ind og signere, fx en ansøgning – har det været uklart, hvilken juridisk status NemID´en har. NemID´en har primært været opfattet som et identifikationsværktøj. Hvorvidt man kan signere med NemID (give udtryk for en viljestilkendegivelse) og hvordan har været uklart. Herunder har der ikke været information/viden om, hvordan man i givet fald gemmer en NemID-signering, så den har juridisk gyldighed. Det ville have været godt, hvis man havde haft et lovgrundlag (ligesom for Digital Post) hvoraf det fremgik, hvilke retsvirkninger brugen af NemID har.

- Borgerne kan gratis erhverve en NemID, hvorimod virksomheder (herunder kommuner) skal betale for at have medarbejdersignaturer til deres medarbejdere. Derfor har flere kommuner af økonomiske grunde bedt de kommunale medarbejdere om at anvende deres private NemID til login i kommunens systemer. Datatilsynet har efterfølgende påpeget, at denne fremgangsmåde ikke er lovlig. En erfaring er derfor, at incitamentstrukturen/det økonomiske setup ikke har understøttet en lovlig anvendelse af NemID´en.

- Udstedelse af NemID kræver af sikkerhedsmæssige årsager personligt fremmøde. De borgere, som af den ene eller anden grund har problemer med fysisk fremmøde – fx ældre og fysisk svækkede – har derfor ikke kunnet erhverve NemID. På trods af, at NemID ellers netop ville kunne hjælpe dem med at klare kontakten til det offentlige digitalt i stedet for fx at skulle møde op i borgerservice.

- Borgere som har brug for hjælp til den digitale kontakt med det offentlige – fx handicappede på institutioner – er udfordret af, at NemID´en er personlig. Man kan derfor ikke få andre – fx en ansat på en institution – til at logge ind for sig. Dette har forhindret disse borgere i at anvende NemID, eller i værste fald betydet, at de pågældende borgere har været nødsaget til at kompromittere sikkerheden omkring deres NemID ved at oplyse personlig kode til en kommunal medarbejder. Vi må derfor konstatere, at det ikke har været hensigtsmæssigt, at man ikke kunne give andre fuldmagt til at anvende NemID´en – fx som en indbygget del af løsningen.

- Der efterlyses en løsning vedr. aldersgrænsen på de 15 år., herunder kobling med UNI-logon mv.

Teknisk løsning og kvalitet

- Det opleves som en ulempe at der har været to tekniske adskilte løsninger på tværs af privat- og offentlig sektor. Det har været svært at forklare borgerne og andre interessenter, hvorfor kommunerne ikke har kunnet anvende de samme løsninger som bankerne. I den sammenhæng at der kan være forskellige krav til anvendelsen.
Næste generation af NemID bør adressere behov på tværs af sektorer og finde en model der understøtter sammenhæng set ud fra brugerne af NemID.

- NemIDs afhængighed af Java har været et stort minus ved løsningen. At tvinge borgerne til at installere et tredjepartsprogram, som er en af de platforme der bliver ramt af flest sårbarheder og er en af de største mål for hackere, er ikke optimalt. Desuden har bøvl med Java opdateringer skabt frustrationer hos borgerne.

- Der efterlyses en højere driftseffektivitet på løsningen.

- Brug af en central server til lagring af de private nøgler vækker også bekymring, idet en kompromittering af serveren vil give adgang til alle borgeres private nøgler. Endvidere er der bekymring vedr. at løsningen benytter det såkaldte "security by obscurity" som en sikkerhedsforanstaltning.

- Løsning for opbevaring af medarbejdercertifikater er ikke skaleret til centralt brug. 3. parts software har været en løsning på denne udfordring.

- Ang. NemID selvbetjening til erhverv:
    - Dårlig håndtering af fejl, kompliceret at aflevere opgaver og få svar på supportopgaver.
    - Dyr prispolitik ift. LRA, betyder at man bibeholder en central administration.
    - Når man søger en specifik bruger frem vises resultatet ikke hvis man har over 500 certifikater. Hvilket betyder at man kan misforstå fremsøgningen som om at brugeren ikke findes.
    - Der sendes mails til LRA om fornyelse af alle V-cert / M-cert. Det er ikke muligt at fra/tilmelde sig disse automatiske mails.
    - Det er ikke muligt at omdøbe en brugergruppe til et andet navn eller flytte alle medlemmer af en gruppe til en ny gruppe samtidigt.

- Der er positive erfaringer med papkort og nøgleviser i et teknisk perspektiv. Der efterlyses dog alternativer, eksempelvis SMS.

Brugerdesign, brugervenlighed og support

- Anvendelsen af NemID Privat har vist sig stærk ved sin store udbredelse og homogenitet og dermed sikres det at løsningen bliver lettere at huske og genkende. Løsningen virker samlet set brugervenlig, herunder også grundet at der eksisterer en engelsksproget version. Dog virker designet utidssvarende og ufleksibelt på forskellige platforme.
- Ved fornyelse af udløbet certifikat, kan beskeden godt gives mere end én gang, da borgeren sommetider glemmer at forny og derfor er nød til at møde op i Borgerservice for at få hjælp til at åbne deres NemID op igen.

- I forbindelse med opgaven som udsteder, er det et ønske at RA-modulet der anvendes til formålet bliver opdateret hyppigere. Det er angående noteringsfelter o.lign. når der sker ændringer i det dokumentation som borgerne skal fremvise for, at få udstedet et NemID.
- I starten var der lagt op til, at man udelukkende måtte udstede på baggrund af de oplysninger man kunne se i RA-portalen og så den dokumentation som borgeren medbringer. På det seneste er der åbnet op for flere dokumentationsmuligheder, dog uden at det er muligt i RA-portalen at anføre hvad man her set af dokumentation.
- Brugervenligheden på RA-portal kunne med fordel optimeres.

Governance og organisering

- Kommuner, KL og SKAT har løbende deltaget i RA-formum i regi af Digitaliseringsstyrelsen.
Her er der løbende kommet en del ændringsønsker, men ofte så kan disse ikke lade sig gøre, da DanID ikke har fået økonomi til dette. Så ved fremtidigt udbud, bør der også sættes økonomi af til, at de praktiske værktøjer løbende kan forbedres og justeres, og i hyppigere takt.

KONKURRENCE- OG FORBRUGERSTYRELSEN

N O T A T

Dato: 25. juni 2014

Sag: TIFS-14/06365-2

Sagsbehandler: /MTP

KONKURRENCE- OG FORBRUGERSTYRELSEN

ERHVERVS- OG VÆKSTMINISTERIET

Svar på offentlig høring om næste generation af den nationale identifikations- og digital signaturinfrastruktur (NemID)

Konkurrence- og Forbrugerstyrelsen har modtaget høringsbrevet vedrørende næste generation af den nationale identifikations- og digital signaturinfrastruktur (NemID). Konkurrence- og Forbrugerstyrelsen er sekretariat for Konkurrencerådet. I den egenskab er styrelsen en uafhængig konkurrencemyndighed. De følgende høringsbemærkninger afgives udelukkende som konkurrencemyndighed. Styrelsen har bemærkninger til høringsbrevets punkt 2 vedrørende funktionalitet og anvendelse.

Bemærkninger til punkt 2. Funktionalitet og anvendelse

EU-Kommissionen fremsatte i juli 2013 udkast til et nyt betalingstjenestedirektiv. Det fremgår af direktivforslaget, at såkaldte tredjeparter (TPP) i fremtiden skal have adgang til forbrugernes betalingskonti for at kunne tilbyde en betalingstjeneste, hvor TPP foretager en kontooverførsel på vegne af forbrugeren.

De seneste års udvikling i betalingsløsninger er i overvejende grad baseret på betalingskort-infrastruktur, og derved på eksisterende gebyrer, der er fastlagt mellem bankerne for transaktioner med betalingskort. En reel konkurrent til betalingskortene er tredjepartsbetalinger, der er billige og effektive, idet produktet er baseret på en simpel kontooverførsel.

Der er fra flere sider ytret bekymring sikkerheden i denne forbindelse, fordi visse TPP-løsninger baserer sig på brugen af forbrugerens egne NemID-oplysninger. For at imødekomme sådanne bekymringer, kan der udvikles et såkaldt fuldmagtsmodul.

Digitaliseringsstyrelsen har allerede fået udviklet en løsning, hvorved brugen af offentlige selvbetjeningsløsninger kan give fuldmagt via sit NemID til en privat eller juridisk person. Ordningen fungerer således, at fuldmagtstageren logger ind via sin egen NemID og herefter har adgang til de sider og tjenester fuldmagten angår.

En lignende effektiv digital fuldmagtsordning i banksektoren vil netop indebære, at kunden via fuldmagtløsningen kan legitimere en TPP til at få adgang til hele eller dele af kundens konto og tilknyttede tjenester. Her-

ved vil TPP'en i kraft af fuldmagten kunne logge ind med TPP'ens egen NemID – altså uden at benytte kundens NemID-oplysninger – hvormed der skabes grundlag for en billig, effektiv og sikker betalingsløsning.

På baggrund heraf anbefaler Konkurrence- og Forbrugerstyrelsen, at den næste generation af NemID udvikles med et selvbetjeningsmodul, hvor både offentlige og private selvbetjeningsløsninger kan give fuldmagt via NemID til en privat eller juridisk person.

SLOTTE & KULTUR- EJENDOMME

Styrelsen for Slotte og Kulturejendomme
H.C. Andersens Boulevard 2 | slke@slke.dk
1553 København V | www.slke.dk
T 3395 4200 | CVR-nr. 34072191

Digitaliseringsstyrelsen
digst@digst.dk

26. juni 2014
J.nr. 14/00253-28

Att.: Morten Jørsum

Offentlig høring om næste generation af NemID

Kulturministeriet har den 28. maj 2014 modtaget den offentlige høring om næste generation af den nationale identifikations- og digital signaturinfrastruktur (NemID). Styrelsen for Slotte og Kulturejendomme (Koncern It) har på vegne af ministerområdets institutioner følgende bemærkninger.

Statens Arkiver

Der forventes en stigende brug af NemID under sagsbehandling og arbejdsgange, som fordrer at borgere eller myndigheder identificerer sig på en sikker måde. Det forventes imidlertid ikke, at behovene vil adskille sig væsentligt fra behovene hos andres myndigheder eller organisationer, men det er vigtigt, at der findes en velfungerende håndtering af medarbejdercertifikater, hvor offentligt ansatte kan agerer på vegne af en myndighed f.eks. ved anmeldelse, aflevering eller ansøgning om adgang til arkivalier.

Digitale arkivalier, som skal bevares, skal afleveres til Statens Arkiver i en særlig arkivversion jf. gældende regler (p.t. bekendtgørelsen om arkivversioner af 20. august 2010). Den fremtidige løsning skal understøtte, at al information i arkivversionen afleveres dekrypteret og kan tilgås uden nøgle. Videre skal den information, som myndigheden har brugt til f.eks. identifikation af afsender o.l., findes som klar tekst i et eller flere felter i ESDH-systemet - også selv om informationen måtte kunne uddrages af mailsignatur eller andet.

Statens Arkiver finder endvidere, at det vil være relevant med en nærmere vurdering af, hvilke juridiske og samfundsmæssige behov der måtte være for at bevare signaturoplysninger på lang sigt. Arkivet forventer, at de digitalt signerede dokumenter i myndighedernes ESDH-systemer er kontrolleret i forbindelse med registrering i systemet, og at arkiveringsversionen er en autentisk repræsentation af de data og dokumenter, som fandtes i systemet på afleveringstidspunktet.

Set i et bredere samfundsmæssigt perspektiv ville det være nyttigt, hvis der i forbindelse med den fremtidige løsning blev udarbejdet en udredning om behovet for langsigtet bevaring af digitale signaturer eller som minimum dokumentationen for, at et givet dokument var forsynet med en gyldig digital signatur på modtagelsestidspunktet. Statens Arkiver deltager gerne i en evt. arbejdsgruppe om emnet.

Spørgsmål kan rettes til Jan Dalsten Sørensen, jds@sa.dk eller 41 71 72 46.

Nota - Nationalbiblioteket for mennesker med læsevanskeligheder

Den fremtidige løsning skal kunne bruges af personer med handicap - herunder blinde, svagtseende, ord- og talblinde personer samt øvrige personer, som pga. handicap er ude af stand til at læse trykt tekst.

Løsningen bør samtidig erstatte alle tidligere offentlige identifikations- og signaturløsninger - herunder UniLogin, virksomheds- og medarbejdersignaturer. Videre er det vigtigt, at løsningen fungerer på alle gængse platforme, både hvad angår klienter og servere - og gerne baseret på JavaScript.

Spørgsmål kan rettes Ole Holst Andersen, oha@nota.nu eller 39 13 46 28.

Statsbiblioteket

Biblioteket har i forbindelse med materialebestillinger behov for at kunne tilgå brugernes oplysninger efter, at de har forladt bibliotekets web-tjenester. Det ville derfor være ønskeligt med en national login-tjeneste, som kunne udlevere unikke bruger-id med tidsbegrænset gyldighed på tværs af tjenester.

Videre ville det være ønskeligt med en infrastruktur baseret på kendte teknologier med international udbredelse, og at Danmark dermed afholder sig fra at definerer nationale varianter af internationale standarder.

Spørgsmål kan rettes til Svend Larsen, sl@statsbiblioteket.dk eller 89 46 22 21.

Med venlig hilsen

Jørgen C. Andersen

Digitaliseringsstyrelsen
Sent pr. e-mail til: kis@digst.dk

Landbrug & Fødevarer

Axelborg, Axeltorv 3
DK 1609 København V

T +45 3339 4000
F +45 3339 4141
E info@lf.dk
W www.lf.dk

CVR DK 25 52 95 29

Offentlig høring om næste generation af den nationale identifikations- og digital signaturinfrastruktur (NemID)

Landbrug & Fødevarer og Videncentret for Landbrug takker for muligheden for at komme med vores bemærkninger til ovennævnte høring. Videncentret for Landbrug står i høringslisten anført som "Landbrugets Rådgivningscenter". Vi skal anmode om, at dette fremover rettes til Videncentret for Landbrug. Samtidig bemærkes, at dette høringssvar et et fællessvar fra Landbrug & Fødevarer og Videncentret for Landbrug.

Konkrete bemærkninger til de af Styrelsen opstillede temaer:

1. Fremtidige forretningsmæssige behov, for henholdsvis virksomheder, offentlige sektor og borgere i Danmark og udlandet samt eventuelle juridiske forhold.

I Landbrugets organisationer, det vil sige både i Landbrug & Fødevarer, i Videncentret for Landbrug og i Dansk Landbrugsrådgivning & Fødevarer har vi et klart forretningsmæssigt behov for en sikker, effektiv og nem digital signaturinfrastruktur. Dette gælder især følgende:

- som udvikler og leverandør af løsninger, der potentielt kan anvende en fremtidig NemID fremfor egenudviklede identifikationsløsninger i vore systemer
- via vore foreninger som repræsentant for landmænd og landbrugets anvendelse af it-systemer
- som serviceleverandør direkte til landbruget i form af virksomhederne i Dansk Landbrugsrådgivning

2. Funktionalitet og anvendelse, herunder eksempelvis niveaudelt sikkerhed, lokal administration af autorisation, single sign-on mv.

Næste version af NemId bør tag højde for væksten i anvendelse på mobildevices, som også har stor betydning for landbruget både generelt ved mobile online løsninger og fagspecifikt ved landbrugsfaglige registrerings-, informations- og beslutningsstøttesystemer, som bl.a. Videncentret for Landbrug og Dansk Landbrugsrådgivning aktivt bidrager til udviklingen af.

Ved mobile løsninger er traditionel en- eller tofaktorautentificering med komplekse passwords besværligt på grund af ringe inputmuligheder. Dette kunne forbedres, såfremt en ny NemID løsning tilbyder niveaudelt sikkerhed, hvor man kan anvende svagere men lettere autentifikations-mekanismer (fx PIN), mod at tjenesteudbyderen informeres om det sænkede sikkerhedsniveau i autentificeringen.

Ligeledes er det vigtigt, at næste version af NemId arbejder effektivt sammen med de gængse standarder for autorisation i såvel rige klienter som mobilapplikationer som f.eks. OAuth.

3. Behov for brugervenlighed, herunder forskellige brugeres aktiviteter fra bestilling til anvendelse og eventuel spærring mv.

Selvom det umiddelbart vil være i konflikt med en god autentificering, vil det ikke desto mindre være interessant/relevant, såfremt der vælges en løsning, der kan understøtte en eventuel serviceudbyderes adgang til indberetninger på vegne af en landmand. Dette kunne f.eks. være tilfældet i situationer, hvor en landmand har outsourcet føringen af sit regnskab til et rådgivningscenter.

4. Teknik og infrastruktur, herunder eksempelvis adskillelse af eID og eSignering, single sign-on, sammenhængende IT-arkitektur, sikkerhed mv.

Bedre beskyttelse mod phishing
Det vil være hensigtsmæssigt, hvis autentificeringsdialogen i en ny løsning er centraliseret hos leverandøren(e), i stedet for som i dag at være indlejret hos tjenesteudbyderne. Dette vil i modsætning til i dag give brugerne reel mulighed for at beskytte dem selv mod phishing i kraft at de ved, at deres akkreditiver kun anvendes på eet specifikt domæne, som browseren kan hjælpe dem med at validere (antal tidligere besøg, check af at SSL certifikatet er det rigtige mv).

Sikkerhed gennem transparens
Der er i den nuværende version af NemId blevet brugt energi på "security through obscurity", f.eks. JAR-filer kamufleret som billeder i den oprindelige NemId, og senest prototypen på Javascript-udgaven af NemId, der inkluderer 1 MB kode. Øget transparens omkring, hvorledes sikkerheden er implementeret, er ønskeligt, da det resulterer i en simplere løsning, som lettere kan peer-reviewes af det danske såvel som af det internationale sikkerhedscommunity.

5. Samspil med interessenter, herunder tjenesteudbydere, administrative procedurer, sikkerhedsprocedurer mv.

Ingen kommentarer til dette punkt.

6. Fremtidig forretningsmodel, herunder leverandørstyring, support, betalingsstruktur, en model med flere leverandører mv.

Sagerne omkring læk af transaktionsdata fra Nets, Java-sikkerhedshuller med mere har skabt et stort behov for at sikre tillid til sikkerheden i næste version af løsningen, både set fra bruger- og tjenesteudbyderside. Det ville i den forbindelse være et væsentligt skridt fremad for næste version af NemId, hvis der kan etableres en teknisk såvel som en økonomisk model, der kan understøtte, at borgeren kan vælge mellem flere leverandører som Identity Provider. Arbejdet kan med fordel inspireres af det britiske IDAP http://oixuk.org/?page_id=305, hvor en række organisationer har meldt sig på banen som identity providers, og hvor de modtager betaling alt efter, hvor mange borgere der vælger at anvende den pågældende organisation til at validere deres identity og foretage autentificering af dem. En model med flere leverandører vil også potentielt kunne skabe en konkurrence på området omkring understøttelse af nye behov, der ikke er kendt ved kontraktindgåelse, men som vil opstå i det hastigt voksende internetmarked.

7. Andre bemærkninger

Ingen kommentarer til dette punkt.

Såfremt ovenstående giver anledning til spørgsmål eller i øvrigt ønskes uddybet, er I meget velkomne til at kontakte os.

Med venlig hilsen

Annika Lund
Erhvervsjuridisk Konsulent

Generel Erhvervspolitik

D 33394210
M 51671545
E anl@lf.dk

Indledning

Vi ønsker at afgive høringssvar til den offentlige høring om næste generation af den nationale identifikations- og digital signatur infrastruktur (NemID).

Som privatpersoner i forhold til høringen og med den givne tidsfrist kan vi ikke give et fuldstændigt og fuldt gennemarbejdet hørringssvar – selvom vi har en del kendskab til emnet, og bl.a. har deltaget i det fællesoffentlige arbejde der førte frem til den nuværende infrastruktur.

Svaret er derfor både en liste af konkret del-svar og tænkt som en retningsangivelse for de øvrige områder i den næste version af NemID.

Vi stiller os gerne til rådighed for en uddybning og også til sparring eller deltagelse i eventuelle referencegrupper.

I vores diskussion der fører frem til dette høringssvar har vi brugt følgende begreber, hvilket kan være betydende for forståelse af svaret

- *NemID* anvendes om autentificering af en (anonym) ID
- *ID* er en autentificeret ID
- *Bekræftet person*: når en ID kan bekræftes tilhører en person
- *Bekræftede persondata:* oplysninger fra autoritativ kilde (typisk CPR) vedrørende en bekræftet person
- *Bekræftet virksomhed og virksomhedsdata*: ækvivalent til ovenstående
- *ID oplysninger*: oplysninger der relateres til konkret ID ('er)
- *ID-holder*: en person/virksomhed der potentielt skal autentificeres med NemID, uanset om personen kan bekræftes[1]
- *Autentificering*: Processen at sikre at den der "er for enden af en (computer) dialog" er en konkret ID
- *Rolle*: en ID kan optræde i væsentlig forskellige situationer eller kontext, der gør at samme ID skal have forskellige adgange og/eller respons alt efter rollen.[2]
- *Anvender*: alle personer der anvender infrastrukturen, uanset rolle
- *Interessenter*: Udbydere, anvendere, myndigheder, virksomheder, organisationer
- *Udbyder*: den der stiller en tjeneste til rådighed, som kræver ID (samt eventuelt bekræftelse) for at anvendes
- *Autentificeringsniveau*: Grader af sikkerfor for at anvenderen retteligt benytter ID.

Behov

Der er behov for større valgfrihed, bedre funktionsadskillelse, at understøtte deltagernes behov og ønsker om (fleksibilitet) i sikkerhedsniveau'er og sikkerhedsmetoder, samt at understøtte en form for roller.

Der er et behov for øget transparens, i løsningerne, så store dele som muligt skal kunne gennemskues af interessenterne, og løsningerne (arkitektur og kildekode) bør anvende anerkendte

1 Dette vil også kunne være ikke danske statsborgere, og borgere der ikke optages i CPR

2 Typiske roller: privat-person ifht. person som representerer (eksempelvis som ansat) en organisation, eller "almindelig bruger" ifht. "administrator"

standarder. Udviklet kode bør udstilles til offentlig verifikation – og til offentlig anvendelse.

Der er behov for at NemID også bliver operationel for mindre spillere (end Banker), til virksomheder indbyrdes, virksomheder ifht. personer og mellem personer.

Eksempler:

- Der skal tilbydes flere autentificering niveauer og -kanaler end i den nuværende løsning. Og løsningen må ikke stå så stille over flere år, funktionelt på dette område, som den nuværende har gjort
- Lovgiver og Udbyder skal kunne vælge forskellige autentificeringsniveauer til forskellige tjenester.
  Eksempelvis kan en virksomhed vælge at sende en vare til en ikke bekræftet person, biblioteket kan vælge at udlåne alene på bruger/password, adgang til personlige helbredsoplysninger kræver et højere niveau.
- Anvenderen skal have ret til at vælge et højere niveau en krævet af lovgiver og udbyder
  Eksempelvis skal en borger kunne vælge, at alle handlinger ifht. enten bank eller det offentlige kræver et højere certificeringsniveau end det nuværende.[3]
- Alle personer skal kunne bruge tjenesterne med flere ID'er.[4]
- Autentificering og signering kunne være nyttig ifht. privat email
- Autentificering og evt. udveksling af bekræftede persondata og/eller ID oplysninger mellem personer og virksomheder kan øge sikkerheden for begge parter f.eks. ved nethandel.
- Bekræftede persondata må ikke duplikeres mellem parter, bare fordi det er bekvemt for udbyderne – arkitekturen skal indrettes så dette undgås. Herved mindskes risikoen for – og ved konkrete angreb, ligesom løsningens troværdighed øges.

Hvordan?

I stedet for at beskrive funtionaliteten direkte og for sig selv, tager vi udgangspunkt i en ændret infrastruktur og beskriver hvordan den kan virke

Infrastrukturen har 5 typer af aktører / elementer:

1) ID-udsteder og provider af autentificeringsniveauer; “autID”
2) ID-ekstra-verifikation, “verifyAut”
3) ID-bekræfter, “attribID”
4) ID-holderen, “ID”
5) Service provider, den som man identificerer sig over for, for at indgå i eller anvende en given service[5]

3 Hvis en person føler sig utryk ved den nuværende NemID – måske fordi password og challenge afleveres over samme kanal (samme browser vindue) – skal borgeren kunne kræve at “bekræftet person” for denne borger kræver to kanaler (eksempel browser og mobiltelefon).

4 En person kan således vælge at benytte en ID ifht det offentlige og en anden ID ifht. f.eks. sin Bank – eksempelvis for at mindske det samlede trusselsbillede personen oplever. Flere NemID kan også vælges som en måde at håndtere roller på – idet der dog også skal være mulighed for nogle roller til samme ID, for dem der foretrækker denne “ease of use”.

5 Service provideren skal naturligvis også være ID-holder selv, men beskrives her i rollen som den der udbeder sig ID på den ID-holder der forbinder sig til Service provideren

1) ID-udsteder og provider af autentificeringsniveauer; "autID"

Denne service svarer til en delmængde af den nuværende NemID.
Der skæres ind til en delmængde for at opnå en modularitet der

- Øger fleksibilitet
- Adskiller autentificering fra "persondata" og mindsker både adgangen til personrelaterede data og mindsker risici hvis uvedkommende får/anvender adgang til autID's data.

Denne serviceprovider "sponsoreres" af staten, til at drive en helt åben service. I princippet vil alle (på kloden) kunne anvende servicen[6], omend i praksis kun med kobling til 2) og 3) for målgrupperne (danske borgere, virksomheder/organisationer og myndigheder).

ID-udsteder skal stille følgende service til rådighed:
1a) Oprettelse og administration af ID
1b) Oprettelse og udveksling af challenge-response ark
1c) Interface til ID ekstra verifikation
1d) Autentifcerings provider
1e) Modul for ID rolle signering

1a) Enhver skal gennem et webinterface kunne oprette en ID[7].

Brugeren angiver selv et unikt brugernavn og et tilhørende password, som systemet husker.
(dette er autentificering niveau 0[8])

Systemet laver en signatur til brug for denne ID.

Brugeren kan tilknytte/aktivere et challenge-response ark til sin ID, uanset om brugeren har genereret det online, eller har fået det af en anden kanal. Aktivering sker ved hjælp af kortets unikke nummer.

Brugeren kan vælge hvilken challenge kanal brugeren ønsker at anvendes til challenge
#0: challenge ikke valgt
#1: ID-udsteders challenge-response, 1b)
>1: ID ekstra verifikation

Når en organisation (virksomhed, forening, …) skal oprettes, vil dette altid ske ud fra en anden ID, som fra start bliver organisationens administrator.

Der skal være mulighed for at tilføje (og fjerne) administratorer til en organisations ID, tilføjelsen krævet accept af såvel en administrator, som af den ID der tilføjes.

1b) ID-udsteder opretter og udveksler challenge – respons ark
Algoritmen – måske koden - til at generere indholdet af et challenge – respons ark bør gøres offentlig tilgængelig, således at alle kan se at det er tilfældige tal.

6 En konsekvens af at det rene snit mellem aktører
7 En borger kan således selv oprette flere – eller ny - ID
8 Niveau betegnelsen i denne tekst er illustrativ, og følger ikke eksempelvis de niveauer der normalt diskuteres i en SAML 2.0 implementering

Systemet kan generere et elektronisk (signeret af ID-udsteder) challenge – respons ark med samme indhold, som vi kender fra NemID's "papkort". Hvert kort identificeres med en unik ID (et nummer).

En bruger, der er logget på ID-udsteder, kan få elektronisk udleveret et challenge – respons ark, valgfrit[9]

- leveret på skærm (brugeren kan så printe)
- leveret som download fil
- leveret som fysisk brev, gennem "folkeregistret"[10] (hvis ID er bekræftet person)

1c) Interface til ID ekstra verifikation

Når brugeren har valgt at ville have ID ekstra verifikation – eller hvis service provideren angiver at ID ekstra verifikation skal anvendes, skal ID-udsteder (efter brugernavn & password identifikation) sende ID til pågældende "verifyAut" aktør, og afvente respons.

1d) Autentificerings provider

Der skal laves et modul til fri afbenyttelse af alle ID-holdere, som ønsker at være en service provider.[11]

Når en service provider anvender dette modul (med sin ID), kan service provideren angive hvilke kanal niveau der kræves for at anvende service providerens service (0, 1 >1, samt i tilfældet >1 angive hvis en bestemt kanal kræves)[12]

Ligeledes kan en service provider angive om der ønskes en bekræftet person og eventuelt angive hvilke bekræftede persondata der ønskes. I dette tilfælde skal ID-holderen præsenteres for disse krav/ønsker som indledning til autentificering og skal kunne afvise de enkelte elementer.

Efter (succesfuld) autentificering sender ID-udsteder ID-holderen og Service Providerens ID til ID-bekræfteren, "attribID", – se nærmere i afsnit 3) – med oplysning om hvilke bekræftede attributter der ønskes og er accepteret af ID-holder. Svaret på dette modtages fra "attribID", krypteret mod service providerens ID, således at alene service provideren ser de aktuelle data.

1e) Modul for ID rolle signering

En person kan selv vælge at lave flere ID'er ved ID-udstederen[13] og således ved egen administration indføre roller for personen, uden yderligere infrastruktur, og uvedkommende for de enkelte service providere.

9 Vi lægger ikke op til at de forskellige forsendelsesmetoder skal opfattes som sikkerhedsniveauer. Det fremsendte kort bruges i alle tilfælde på samme kanal som brugerID/password (samme browser session), og vi opfatter "brev er sikker levering som ikke kan opsnappes" som misbrug af en juridisk overlevering og ikke mere reelt end "browseren/pc'en er ikke overtaget"

10 Bemærk at servicen med print og forsendelse af nøglekort sker i regi af myndigheden (staten). ID-udstederen sender krypteret challenge respons ark med angivelse af ID til myndigheden til print og forsendelse – uden at ID-udsteder kender personadata herunder navn og addresse.

11 Denne brede formulering er for at flest mulige parter kan få glæde af infrastrukturen, eksempelvis også mindre virksomheder i kommunikation med forbrugere, eller mellem borgere, i foreninger osv.

12 Se 1a)

13 Bemærk at ID-bekræfteren ("CPR" myndigheden) skal kunne bekræfte den samme person på flere ID

Men der er behov for at kunne se når en virksomhed agerer, henholdsvis en virksomheds ansat agerer.

Det første understøttes ved at virksomheden også kan være ID-holder (myndighedsbekræftelse er her ifht. CVR). Virksomheden som entitet tegnes så ved signering med ID'ens signatur – f.eks. gennem automatiske/server baserede transaktioner.

For at man kan se at en konkret ansat i virksomheden handler på virksomhedens vegne, skal en (personID) kunne tilknyttes en eller flere virksomhedsID'er. En organisationsID skal således kunne tilføjes et vilkårligt antal person ID'er (og de skal kunne fjernes igen) af organisationens administratorer[14] – hver ID skal dog også godkendes af ID-holderen før den er tilføjet.

Under autentificering af en person ID vil systemet bede ID-holderen[15] vælge en organisation (eller vælge "som person").

… de nærmere mekanismer omkring håndtering af signatur og af signeringsopgaven er ikke endnu gennemarbejdet, men skal understøtte den retning dette afsnit angiver.

2) ID-ekstra-verifikation, "verifyAut"[16]

I stedet for at fortsætte ud af den hidtidige strategi "one size fits all", mener vi det er vigtigt at give valgfrihed på kanaler, metoder og sikkerhedsniveauer for autentificering.

I "ID-udstederen" ligger niveau 1 og 0, svarende til de sikkerhedsniveauer der findes i den nuværende NemID løsning med og uden "papkort" i autentificeringen.

Det er klart at det er nødvendigt, at der skal være styr på aktører til eID ekstra verifikation, og at der samtidig gives bedst mulighed for konkurrerende alternativer.

Der skal derfor laves en sæt regler og en beskrivelse for hvorledes en virksomhed kan blive "verifyAut", hvordan løsningens sikkerhedsniveau klassificeres - og hvordan løsningens sikkerhedsniveau kan klassificeres og indgå i ID infrastrukturen .

Eksempler på alternative eller ekstra verifikationer:

a) "SMS challenge respons verifyAut" - challenge respons med mobil som kanal
Ækvivalent med ID-udstederens "challenge-respons ark" genereres et ark, som kan leveres af de samme kanaler og/eller til mobil telefon.

Autentificering sker ved at verifyAut sender SMS med challenge og verifyAut modtager respons modtages pr SMS .

14 Ved tilknytningen kan administrator sætte hvilket challenge/verifikations niveau der kræves for at handle med denne organisation som "rolle"

15 Hvis person ID'en er tilknyttet mindst en organisation

16 Det skal bemærkes at det opfattes som være en styrke for opfattelsen af sikkerheden i den samlede infrastruktur, at ID ekstra verifikation ikke foretages af samme operatør som foretager ID udstedelse. Og at denne adskillelse derfor skal være et krav. Det er kun adskillelsen til ID udstedelse der er afgørende – en operatør kan godt tilbyde flere alternative ID ekstra verifikation .

b) verifyAut dongle
I stedet for challenge-respons ark tilbydes en hardware dongle

VerifyAut kan være med SMS, eller over netværk,...

c) ….
mange andre løsninger findes, og der vil givetvis komme flere med tiden

Løsningerne kan være gratis (sponsorerede af staten) eller finansierede af brugerne.

Vi mener at løsning a) skal etableres (sponsoreres) af staten til fri anvendelse af bekræftede ID'er, således at borgene kan vælge denne løsning gratis (hvis de har mobil, hvilket vi ikke mener at myndighederne bør kunne stille krav om)

Vi mener at staten (fortsat) bør overveje at sponsorere en eller flere løsninger af typen b), hvor ID-holderen skal medfinansiere ID-holderens hardware.

3) ID-bekræfter, "attribID"
AttribID er en service som myndigheden står for.

Grundlæggende skal denne service baseres på at en persons identitet og ejerskab af en ID verificeres af autoritativ kilde , som efterfølgende kan bekræfte sammenhæng og associerede data over for tredjepart

Denne opgave har man også haft ved etableringen af NemID. Det er vores opfattelse af selvom den bekræftede sammenhæng givetvis hovedsaglig er korrekt, er de hidtidig anvendte metode dybest set meget usikre. I princippet usikre, men som det også er beskrevet i pressen i praksis ikke håndteret korrekt, så selv den forestillede sikkerhed har ikke været til stede.

Særligt her skal det overvejes hvordan der sker en nem overgang fra den eksisterende nemID – her må vi erkende behovet for en strømliniet konvertering (uanset ovenstående betragtninger om svagheder i kilden). Vi forestiller os at alle anvendere af den nuværende nemID skal kunne tilgå en særlig konverteringsfunktion hos ID-bekræfteren, hvor den nye ID kobles til en CPR-person gennem anvendelse af den gamle nemID autientificering og CPR opslag.ID-bekræfterID-bekræfterID-bekræfter.

Herefter mener vi at den eneste rigtige måde, at etablere sammenhængen mellem person-identitet og ID, er gennem en myndighedsbehandling. Hvor en myndighedsperson fysisk møder ID-holderen, og checker præsenteret dokumentation, og lader ID-holderen autentificere sig over for myndigheden (gennem ID-udstederen).

I praksis kan dette eksempelvis ske
* gennem eksisterende kommunal borgerservice,
* i særlige servicefunktioner (f.eks. en borgerservice/politifunktion) etableret på trafikknudepunkter
* gennem opsøgende borgerservice (borgerservice med rundt i bogbusser, eller....)

ID-bekræfteren ("CPR myndigheden") skal således etablere procedurer og ID understøttelse af borgerbetjening på dette område – hvilket i et vist omfang også er tilfældet i dag.

ID-bekræfteren skal etablere et aftalegrundlag, som en service provider skal indgå i, for at kunne få et svar[17]. Dette aftale grundlag skal sikre, at service provideren håndterer data på betrykkende vis, lader sig revidere osv. Dette kan virke som overlappende med dataloven/datatilsynets rolle, men det er vores opfattelse at en sådan aftale vil være en styrke ifht. danske virksomheder under dansk lov. Og det er absolut afgørende for at kunne håndtere service providere, hvor der kan være tvivl om hvilke love der gælder, eller hvor vi ved at dataloven ikke gælder.

ID-bekræfteren skal etablere et system der kan modtage en forespørgsel fra ID-udsteder, og besvare disse – krypteret til den konkret modtagende service provider.

Under forudsætning af, at ID-udsteder har indhentet ID-holderens samtykke i den konkrete autentificeringssession, taler vi om følgende oplysninger som ID-bekræfter kan udsende
a) Er ID en bekræftet person
b) Den bekræftede persons person-ID[18]
c) Den bekræftede persons navn[19]
d) adresse
e) alder
f) fødselsdato
g) … ?

Hvor ovenstående forkuserer på bekræftelse af en person, så skal der derudover tilsvarende kunne indhentes bekræftelse på organisationer (virksomheder) gennem autoritativ sammenknytning mellem en organisations ID og en entitet i CVR.

I dette tilfælde vil samtykke / fortrolighed have en mindre rolle, idet eksempelvis navn og adresse her skal være offentligt tilgængeligt.
ID-bekræfterID-holder

17 Alle vil dog kunne få svar af attribID på om "er dette en bekræftet person", hvis ID-holderen har accepteret at svaret gives

18 Her skal det bemærkes at vi absolut mener at denne ID ikke er CPR nummer, men at CPR registret (som minimum til denne service, men klart kan det bruges bredere) skal etablere et selvstændigt unikt ID til alle personer der registreres i CPR. Der er skrevet meget om CPR-nummeret den seneste tid, men vores ærinde her er alene at sikre en korrekt og holdbar datamodellering. CPR nummeret har som minimum den svaghed at man ud fra nummeret kan se to personhenførbare oplysninger; køn og fødselsdato. Og ID infrastrukturen skal kunne arbejde med en entydig identifikation af en person, uden at "vedlægge" personhenførbare oplysninger.

19 For flere af data c), d)... vil et svar kunne være "må ikke oplyses" - ved hemmelig adresse osv.

Den 27. Juni 2014,

Lars Ole Belhage
Bjarne C. Jacobsen
Lars Roark

Høringssvar

Vedr. Offentlig høring om næste generation af den nationale identifikations- og digital signaturinfrastruktur (NemID)

Afsender	Michael Møller
Dato	10. juni 2014

http://www.computerworld.dk/art/231127/opfordring-til-laeserne-vaer-med-til-at-designe-nemid

Udfordring modtaget..

Vedr område;

teknisk infrastruktur

Tag et kik på;

https://www.grc.com/sqrl/sqrl.htm

Det er en løsning der kombinerer web login med brugerens smart phone, måske denne eller noget lign kunne blive en del af det nye NemID V3.

Og ellers som minimum en kode generator til smart phones, når andre som eg. VeriSign kan lave en "sikker" løsning til smartphones burde NemID også kunne sikres tilstrækkeligt.

Best regards / Med venlig hilsen

Michael Møller
IT Operations Specialist
Mobile Phone: +45 27 876 121
I always consider opposing viewpoints – I consider them silly..
SWYgeW91IHJlYWQgdGhpcyB5b3UgZ290IHRvbyBtdWNoIGZyZWUgdGltZQ==

Høringssvar

Vedr. Offentlig høring om næste generation af den nationale identifikations- og digital signaturinfrastruktur (NemID)

Afsender	Miljøministeriet
Dato	27. juni 2014

Til Digitaliseringsstyrelsen

I forbindelse med etablering af beslutningsgrundlaget for den næste generation af identifikations- og digital signaturinfrastruktur i Danmark har Digitaliseringsstyrelsen ønsket at høre relevante interessenter om deres behov og ønsker i denne sammenhæng. Miljømisteriet og Miljøstyrelsen er blevet kontaktet i forbindelse med den offentlige høring.

Miljøministeriet har koordineret høringen internt og kan melde følgende tilbage:

Miljøministeriet har ikke den fornødne indsigt, kompetence og ressource til at gå dybere ind i de udmeldte temaer, men kan dog ud fra vores erfaringer med den hidtidige infrastruktur pege på enkelte ønsker og anbefalinger til den fremtidige infrastruktur.

I forbindelse med temaet **Funktionalitet og anvendelse** er det ønskværdigt, at det bliver muligt for udlændinge og udenlandske virksomheder at benytte danske offentlige selvbetjeningsløsninger (gerne med tilhørende Digital Post) med sikker identifikation. Endvidere finder vi det vigtigt, at den planlagte vej med øget mobilitet (pr. sommer 2014) forfølges yderligere.

I forbindelse med temaet **Behov for brugervenlighed** vil ministeriet tillægge det værdi, hvis den tekniske implementering i selvbetjeningsløsninger og fagsystemer bliver nemmere for de relevante myndigheder, og hvis der bliver sat fokus på brugervenligheden i installationen på brugersiden.

I forbindelse med temaet **Teknik og infrastruktur** finder vi det vigtigt, at løsningen bliver sikkerhedsmæssig fuldt forsvarlig.

I forbindelse med temaet **Fremtidig forretningsmodel** mener vi, at det vil være befordrende for udbredelsen og ressourceformindskende med et fuldt frikøb på statens område.

Med venlig hilsen

Helle Wentzer Licht
Seniorkonsulent
Anvendelse – Land og By
Dir tlf.: (+45) 72 54 56 60
Mobil: (+45) 20 87 00 60
hwl@gst.dk

Miljøministeriet
Geodatastyrelsen

Rentemestevej 8
DK - 2400 København NV
Tlf.: (+45) 72 54 50 00
www.gst.dk

Høringssvar

Vedr. Offentlig høring om næste generation af den nationale identifikations- og digital signaturinfrastruktur (NemID)

Afsender	Ministeriet for Børn, Ligestilling, Integration og Sociale Forhold (MBLIS)
Dato	27. juni 2014

Ministeriet for Børn, Ligestilling, Integration og Sociale Forhold (MBLIS) har følgende bemærkninger til nedenstående høring:

Digitaliseringsstyrelsen har i høring af 28. maj 2014 bedt om ønsker til næste generation af NemID, der nu skal i udbud. Digitaliseringsstyrelsen ønsker bemærkninger inden for følgende temaer:

1. Fremtidige forretningsmæssige behov, for henholdsvis virksomheder, offentlige sektor og borgere i Danmark og udlandet samt eventuelle juridiske forhold.

2. Funktionalitet og anvendelse, herunder eksempelvis niveaudelt sikkerhed, lokal administration af autorisation, single sign-on mv.

3. Behov for brugervenlighed, herunder forskellige brugeres aktiviteter fra bestilling til anvendelse og eventuel spærring mv.

4. Teknik og infrastruktur, herunder eksempelvis adskillelse af eID og eSignering, single sign-on, sammenhængende IT-arkitektur, sikkerhed mv.

5. Samspil med interessenter, herunder tjenesteudbydere, administrative, procedurer, sikkerhedsprocedurer mv.

6. Fremtidig forretningsmodel, herunder leverandørstyring, support, betalingsstruktur, en model med flere leverandører mv.

7. Andre bemærkninger

MBLIS skal **indledningsvist** bemærke, at det er uklart i høringen, om vi som ministerium ud over egne forretningsmæssige behov herudover skal varetage interessen for de borgergrupper, som ministeriet

har ansvaret for at udføre politiske initiativer over for, fx ældre, borgere med handicap, borgere med psykiske lider, hjemløse mv. I høringen har vi også taget hensyn til sidstnævnte aspekter, idet der må tages højde for, at vi ikke på dette punkt har ladet os begrænse af eventuelle tekniske begrænsninger og krav til sikkerhed mv., som vi ikke har fuld indsigt i.

MBLIS skal bemærke, at der i offentligheden har været rejst problemstillinger i forhold til mennesker med handicaps og ældres brug af NemID, herunder både i forhold til kontakten til det offentlige samt vedr. muligheder for administration af den enkeltes egen økonomi. Det vurderes væsentligt, at man i arbejdet med næste generation af NemID er opmærksom på disse problemstiller, der er rejst af bl.a. handicaporganisationer, ældreorganisationer og KL.

Det er vigtigt at den kommende løsning understøtter brugere med særlige behov, uanset om det er en borger eller en offentligt ansat medarbejder. Der skal tages hensyn til handicap. Samtidig skal løsningen også tage hensyn til særligt udsatte og svage grupper, fx svage eller ældre it-brugere, indvandrere med dårlige sprogkundskaber, hjemløse og andre. Der kan også være grupper af unge / halvstore børn, som har brug for identifikation fx ved eksamener, bus- og togkorterhvervelse mv.

I forhold til de problemstillinger, som MBLIS kender til, anbefaler vi, at der i næste generation NemID gives mulighed for, at en øget og fleksibel adgang til at give fuldmagter til anvendelse af NemID (herunder fx også enkeltfuldmagter, hvis der skal flere underskrivere på fx en boligstøtteansøgning). I forhold til svage brugere bør man også overveje fuldmagtsgivning eller delegering af ret til at benytte identitets- eller fuldmagtsgivning eller underskriftsfunktionen til støttepersoner til svage borgere eller borgere med funktionsnedsættelser.

Det anbefales derudover, atNemID skal være så brugervenlig som muligt og kunne anvendes på mobile enheder.

Der er også identificeret et problem i forhold til hjemløse, der mister deres NemID mv. Her er det ønsket, at overveje om det er muligt at kunne anvende NemID, så den er tilgængeligt via nettet uden brug af nøglekort mv. På denne måde undgår man problemet med borgere, der ikke kan få adgang til Digital Post eller digitale selvbetjeningsløsninger mv., fordi de mister deres nøglekort. Herudover vil man løse problemet for borgere, der ikke ønsker at have NemID på sig af og i dag kun har den mulighed at opbevare nøglekortet i sikre bokse. Det gælder fx for hjemløse borgere.

Herudover bør det overvejes at gøre det nemmere for borgere med fast bopæl i udlandet, at få udstedt NemID.

Det er endvidere vigtigt for MBLIS, at løsningen tilgodeser de behov for tilgængelighed, som mennesker med særlige behov måtte have, hvad enten disse skyldes handicap (funktionsnedsættelser), kulturelle, sociale eller sproglige forhold.

I forhold til **tema 3 ”Behov for brugervenlighed”** bemærker MBLIS, at der fortsat skal være fokus på at sikre en NemID løsning, som er handicapvenlig, både for borgere med fysiske og psykiske funktionsnedsættelser".

Det er således vigtigt, at gældende regler og retningslinjer for tilgængelige webløsninger og services overholdes og anvendes i udviklingen af systemet (f.eks. WCAG 2.0 og WAI-ARIA). Ligesom man bør udvikle forskellige løsninger tilpasset brugergrupper med specielle krav til brugergrænsefladen.

Løsningen skal være med til at sikre, at borgere med handicap er i stand til at kommunikere med det offentlige på lige fod med andre borgere, så man også her lever op til kravene i FN's handicapkonvention.

Det er vigtigt, at man foruden tilgængeligheden også sikrer en brugervenlig løsning, så alle borgere uanset evt. handicap vil være i stand til at kommunikere med det offentlige på en nem og betrykkende måde, uden at den enkelte bliver begrænset i sine muligheder i forhold til obligatorisk digitalisering og digital post.

Det er vigtigt, at gældende regler og retningslinjer for tilgængelige webløsninger og services overholdes og anvendes i udviklingen af systemet (f.eks. WCAG 2.0 og WAI-ARIA). Ligesom man bør udvikle forskellige løsninger tilpasset brugergrupper med specielle krav til brugergrænsefladen. Løsningen skal være med til at sikre, at borgere med handicap er i stand til at kommunikere med det offentlige på lige fod med andre borgere, så man også her lever op til kravene i FN's handicapkonvention.

Endvidere gør MBLIS opmærksom på, at der er kønsforskelle i netadfærden hos henholdsvis ældre kvinder og ældre mænd, og at der bør tages højde for disse i forbindelse med overvejelserne om brugervenlighed og tilgængelighed.

I forhold til **tema 1 "Fremtidige forretningsmæssige behov"** bemærker MBLIS, at de mange sager i pressen med sikkerhedsbrister, hvor borgeres cpr-nummer er blevet offentliggjort, misbrugt eller anvendt til kriminalitet peger på, at den nye generation af Nemid skal udvikles til en sikkerhedsmæssig holdbar løsning.

I forhold til **tema 2 "Funktionalitet og anvendelse"** bemærkes, at løsningen evt. kunne anvende differentierede sikkerhedsniveauer, hvorved eksponeringen af cpr-numret kunne styres.

I forhold til **tema 4 "Teknik og infrastruktur"** bemærkes især, at den nye generation af NemID bør være uafhængig af platforme eller kunne understøtte alle platforme. Det er ligeledes vigtigt, at løsningen understøtter mobilitet.

Adskillelse af identifikationsdelen og underskriftsdelen vil være at foretrække. Det bør altså være muligt at skelne mellem den digitale identifikation og de situationer, hvor borgeren eller brugeren skal underskrive digitalt.

En ny generation NemID bør udformes, så ansatte i den offentlige administration kan teste deres 'egne' offentlige systemer uden at skulle gøre brug af deres private og personlige NemID som borgere.

Offentligt ansatte kan ikke benytte NemID erhverv til dette, da NemId erhverv er offentligt ansattes mulighed for at kontakte og verificere sig over for andre offentlige systemer i deres egenskab af at være sagsbehandlere i egen organisation.

Statsrevisorerne Beretning nr. 3 om forebyggelse af hackerangreb 2013-14 opsætter en række anbefalinger (der i praksis fungerer som krav) til de offentlige institutioner, som bl.a. bør sikre, at der er

* teknisk begrænsning af download af programmer fra internettet

* begrænsning af brugen af lokaladministratorer

Disse anbefalinger er i modstrid med den nuværende tekniske løsning i NemID.

Java-appletten skal nemlig installeres og opdateres med jævne mellemrum og derfor må brugere, som er ansat på en offentlig arbejdsplads, stole på, at it-afdelingerne får udsendt opdateringerne til Java uden forsinkelse.
Derfor bør en kommende NemID løsning tage højde for sådanne forhold; eksempelvis ved at kunne fungere uafhængigt af platforme og uafhængigt af installation.

I forhold til **tema 5 "Samspil med interessenter"** bemærker MBLIS, at det bør være et krav, at rigsrevisionen godkender den næste generation af NemID som valideringsmekanisme op imod offentlige systemer.

MBLIS bemærker endeligt, at MBLIS har sendt høring til Udbetaling Danmark, som ikke var på høringslisten. Udbetaling Danmark svarer Digitaliseringsstyrelsen direkte. MBLIS har herudover givet input til høring af en række yderligere organisationer, som Digitaliseringsstyrelsen supplerende har hørt.

Med venlig hilsen
Lisbeth Krogh
Specialkonsulent
SOCIALMINISTERIET
Jura og International
Holmens Kanal 22
1060 København K
Tlf. nr. 33924337
E-mail: lbk@sm.dk

Ministeriet for Fødevarer, Landbrug og Fiskeri
NaturErhvervstyrelsen

Den 25. juni 2014
Ref.: FRJO / Center for It

Svar vedr. høring om ny digital identifikations- og signaturinfrastruktur (NemID)

Den nuværende NemID-løsning har været en central drivkraft for digitaliseringen af offentlige services. NaturErhvervstyrelsen arbejder løbende med at effektivisere sagsbehandling og interne processer gennem digitalisering og automatisering. Centralt i dette arbejde er etableringen af brugervenlige selvbetjeningsløsninger og platforme til kommunikation med styrelsens kunder.

For at kunne gøre det har NaturErhvervstyrelsen brug for en effektiv og sikker digital id- og signaturinfrastruktur, særligt til understøttelse af kommunikation og transaktioner med private virksomheder og borgere. NaturErhvervstyrelsen har følgende bemærkninger inden for de foreslåede temaer:

1) Forretningsmæssige behov
Ejerforhold og relationer mellem virksomheder og mellem virksomheder og borgere har betydning for anvendelse af digitale identifikations-løsninger. Typiske scenarier er fx borgere, der har behov for nem adgang til at administrere en mindre virksomhed (fx en enkeltmandsvirksomhed), virksomheder der administrerer på vegne af en anden virksomhed (fuldmagt) og medarbejdere i virksomheder, der administrerer på vegne af flere virksomheder i samme koncern (kompleks ejer struktur). Der er behov for løsninger, der gør det nemt for virksomheder at få overblik over, hvem der har fået udstedt signaturer i forhold til de organisatoriske strukturer, delegering af rettigheder (fuldmagter) og nem administration af signaturer.

   Der er ligeledes brug for, at medarbejdere i virksomheder kan identificeres i forhold til den specifikke produktionsenhed (p-nummer) de arbejder i. Det skyldes, at indberetning ofte foregår på p-nummer niveau og at denne identitet er central for at kunne tilbyde store virksomheder nem adgang til at administrere deres oplysninger.

   NaturErhvervstyrelsen modtager indberetninger fra virksomheder i andre lande. Indtil EU-Kommissionens forslag til forordning om identifikation og tillidstjenester (eIADS) er implementeret, er der behov for alternativer til at håndtere sikkert login og sikre transaktioner fra virksomheder i andre lande.

2) Funktionalitet og anvendelse
NaturErhvervstyrelsen har behov for et lavere sikkerhedsniveau end det nuværende, fx blot baseret på brugernavn og password. Det skyldes især et ønske om at kunne give nem adgang til egne, ikke følsomme data til virksomheder og dermed udvide funktionaliteten i og brugervenligheden af digitale selvbetjeningsløsninger.

NaturErhvervstyrelsen
Nyropsgade 30
DK-1780 København V
Tel +45 33 95 80 00
Fax +45 33 95 80 80
mail@naturerhverv.dk
www.naturerhverv.dk

3) Brugervenlighed
Kunder på offentlige digitale løsninger skal foreholde sig til en mængde begreber. De offentlige portaler borger.dk/virk.dk, NemLog-in og NemID har hver deres indgange og brugergrænseflader, hvilket gør vejen ind til selvbetjening længere og ofte forvirrende for brugerne.

Der skal sikres en bedre integration af NemId i myndighedernes løsninger for at øge brugervenlighed. Sikkerhedsinfrastrukturen (NemID/ NemLog-in) skal derfor træde mere i baggrunden i forhold til brugeren og de forskellige komponenter skal kunne tilpasses, fx i forhold til lede- og hjælpetekster, for at mindske forvirring og sikre den bedste understøttelse af de centrale forretningsprocesser.

Alle platforme, dvs. de mest anvendte kombinationer af enheder og operativsystemer, skal understøttes og der skal være bedre mulighed for, at brugerne har flere signaturer tilpasset til fx desktopmiljøer og mobile platforme.

4) Teknik og infrastruktur
Konkret er der behov for at kunne signere større dokumenter, end det er muligt i dag. Begrænsninger i signeringskomponenten er en barriere for fuld digitalisering af arbejdsgange i NaturErhvervstyrelsen.

Der er behov for, at egenskaber ift. fx signering og fuldmagtsløsninger integreres i NemLog-in uden tab af funktioner. NaturErhvervstyrelsen oplever udfordringer med at anvende NemLog-in og dermed de centrale fordele ved single sign-on på tværs af offentlige løsninger, fordi Nemlog-in komponenter ikke kan tilpasses tilstrækkeligt til de forretningsmæssige behov eller har begrænsninger, der gør de ikke kan anvendes i konkrete brugerscenarier.

Den offentlige signaturstandard OCES skal være fuldt kompatibel med den private signatur (bankernes). Der er behov for, at de tekniske underliggende forhold omkring sikkerhedsinfrastrukturen træder i baggrunden og gøres transparente for brugeren, så der ikke kan opstå tvivl om, hvad der skal til for, at borgere og virksomheder kan benytte offentlige digitale tjenester.

6) Forretningsmodel
NemID er en af kernekomponenterne i den digitale infrastruktur. Det er derfor centralt at der ydes support til borgere og virksomheder, der har problemer med løsningen. Det skal sikres, at der altid kan findes support til problemer, enten i form af let forståelige vejledninger/guider og selvbetjening eller i form af let tilgængelig og evt. gratis hotline support.

Vi ser frem til at følge arbejdet med en ny NemID-løsning.

Med venlig hilsen

Franci Johansen
IT-Chef, NaturErhvervstyrelsen

Høringssvar

Vedr. Offentlig høring om næste generation af den nationale identifikations- og digital signaturinfrastruktur (NemID)

Afsender	Niels Kleberg
Dato	25. juni 2014

Med udgangspunkt i den offentlige høring har jeg, uden at være høringspart, understående forslag, som jeg som borger og anvender af NemID håber vil blive godt modtaget.

Som led i en generel international tendens mod bedre beskyttelse af privatlivet, mener jeg at NemID's virkemåde og infrastruktur skal udvides til bedre at understøtte dette. Jeg har derfor følgende 3 forslag:

MIN LOG - for at opretholde den høje tillid til den offentlige forvaltning i Danmark, bør offentlige aktører skrive til en personlig log for den enkelte borger, når den anvender borgerens personlige eller følsomme data. Loggen kan placeres under borgerens dokumentboks, således at borgeren har transperant adgang til at se hvilke myndigheder der har anvendt data og i hvilken sammenhæng.

PSEUDONYMISERING - som led i udbredelsen af NemID som autentificeringsmekanisme bør brugeren pseudonymiseres, således at det ikke er muligt at udføre datamining på en bruger som anvender NemID.

CENTRAL SAMTYKKEKOMPONENT - hvor offentlige aktører har behov for en borgers samtykke til at indhente, eller udveksle informationer, bør dette kunne indhentes via en fællesoffentlig komponent under signering med NemID.

Med venlig hilsen
Niels Kleberg

Undskyld kortfattethed. Sendt fra min iPad

Høringssvar

Vedr. Offentlig høring om næste generation af den nationale identifikations- og digital signaturinfrastruktur (NemID)

Afsender	Nimish Gautam
Dato	22. juni 2014

Hej.

Undskyld for engelsk, men jeg kan forklare mine meninger bedre på det.
I've been a software developer here in Denmark for the last 2 years, having worked in the private sector and also for the Undervisningsministerium, and working to set up some secure API protocols at Wikipedia before I moved here.

Most developers who want to use NemID don't really want or need all the verification it provides. You don't necessarily need the user's real name or CPR number... you just want to know 1 thing:
- This user is a unique Danish user on my system that can register exactly once

Based on this, I propose something with the following additional properties:
- I know that a user is only on my system once, and is a user of NemID
- I do not know the user's name, CPR number, or any other information about the user

- Anyone who somehow spoofs my API credentials knows nothing about my application OR anything about the NemID user

This would require an extra interaction by the user...they would have to go some central NemID website and say "send the following confirmation string to this application".

Here's how an example flow would go:
As an app developer, I register an app with app id "1" at nemid.dk.
A user comes to my site, and I say "to complete registration, please log in to nemid.dk and say 'app id 1 should get my confirmation code A123'"
I then go to nemid.dk and make an API call. The API gives me a random ID for this user, with the only guarantee that the identifier will NOT be repeated (which can be accomplished by one-way hashing) and it returns my confirmation code to me. So I get something like:
{ "random-id-here" : "A123" }

Again, even if my API credentials are compromised, it's impossible to construct anything valuable out of this since the random id will be unique for all applications, and the second value is a value that I've asked the user to specify.

Similarly, if the user doesn't want to comply, they retain the right to send whatever arbitrary string or information they want to my system, or nothing at all.

Because there are no security risks in a system like this, it can be open to any developer in Denmark nearly for free (minus storage space and bandwidth costs, which could be throttled).

Of course, if your application wanted more detailed information (CPR number, etc), the more direct login that is available now would still apply, but again, most developers just want user authentication, and bank-grade software isn't required to get it.
(also I'm sure you've gotten plenty of suggestions about not using Java on the client side, but in case you haven't... using Java on the client-side creates a nightmare of usability issues because of the way Java is updated and the way web browsers enforce default security practices, along with the decreasing number of browsers that continue to support Java, notably Chrome and Firefox, not to mention the fact that iOS does not allow for any virtual machines, including the jvm. It's also very slow.)

Thank you for your time.

ODENSE KOMMUNE

Borgmesterforvaltningen

Forretningsudvikling
Arkitektur og Teknologivalg

Rådhuset
Flakhaven 2
Postboks
5000 Odense C

www.odense.dk

Tlf. 65511701
Fax
E-mail it.bmf@odense.dk

DATO
27. juni 2014

REF.
Lanh

Høringssvar for høring ang
"Offentlig høring om næste generation af den nationale identifikations- og digital signaturinfrastruktur (NemID)"

Odense Kommune fremsender hermed høringssvar. Odense Kommunes høringssvar indeholder dels en generel indledning og bemærkninger og dels specifikke bemærkninger og bidrag i forhold de skitserede høringstemaer i Høringsbrevet.

Generel indledning og bemærkninger
Odense Kommune anser denne høring som vigtig og sætter pris på at Digitaliseringsstyrelsen foretager en meget bred og åben høring. Odense Kommune anser denne infrastruktur komponent, som en meget vigtig og central komponent i forhold til en national digitalisering og samspillet imellem offentlige og private virksomheder og borgerne.

Som beskrevet i høringsbrevet udløber kontrakten for den eksisterende først i 2017. Da der på nuværende tidspunkt er over 3 år til udløbet af kontrakten kan det være svært at forudsige hvorledes at IT-landskabet ser ud om 3 år, ligeledes er der heller ingen der ved om virksomheders og borgeres anvendelsesmønster eller it-adfærd har ændret sig i 2017.

På baggrund af ovenstående så er nedenstående bemærkninger og bidrag baseret på erfaringerne med den nuværende løsning. Bemærkningerne og bidragene er angivet i *kursiv* ved hvert høringstema.

Bemærkninger og bidrag i forhold til høringstemaerne:

Høringstema 1: Fremtidige forretningsmæssige behov, for henholdsvis virksomheder, offentlige sektor og borgere i Danmark og udlandet samt eventuelle juridiske forhold.

Bemærkninger / Bidrag:
1.a) Løsningen skal understøtte såvel nationale som internationale standarder som er relevante for en sådan løsning.

2. Funktionalitet og anvendelse, herunder eksempelvis niveaudelt sikkerhed, lokal administration af autorisation, single sign-on mv.

Bemærkninger / Bidrag:
2.a) Behov for mulighed for integration med myndighedens AD, således at det ikke er nødvendigt at tilkøbe et produkt ved 3. parts leverandør for at håndtere dette

2.b) Mulighed for central opbevaring af certifikater således at det ikke skal installeres lokalt på medarbejdernes pc'ere. Med så mange certifikater som

vi har er løsningen ikke skalleret til central brug , vi har tilkøbt 3. parts produkt for at løse dette.

2.c) Behov for" NemID light" løsning: Ligesom de private virksomheder har muliggjort en adgang via mobile devices til fx ens bankoplysninger, så er der også i forhold til offentlige løsninger behov for dette. Der er allerede i dag brug for en såkaldt fælles offentlig NemID light løsning. Et eksempel på behovet for en sådan NemID light løsning i en kommunal kontekst er bl.a. følgende:
- Ligesom på skoleområdet er institutioner også blevet digitale og der informeres derfor fremadrettet via digitale beskeder eller statusopdateringer. I den kontekst så er det overkill at en forældre skal logge ind med 2 faktor for at læse at børnene fx skal huske gummistøvler i morgen, eller andre ikke personfølsomme informationer.
Der er derfor et behov for understøttelse af en ikke to faktor authentifications mekanisme som kan anvendes af fælles offentlige løsninger til ikke personfølsomme kommunikation, men med mulighed for at hvis der skiftes fra ikke personfølsom kontekst til en potentiel personfølsom kontekst(fx at man vil klage over noget eller ansøge om en ydelse) kan lave et såkaldt step-up i sikkerheden(se beskrivelse step-up i sikkerheden i punkt bidrag 2.d)

Ovenstående er blot et af eksemplerne på behovet for en fælles offentlig NemID light funktionalitet i den kommunale.

2.d) I forhold til skift fra en ikke personfølsom kontekst til en personfølsom kontekst skal der være mulighed for at løsningen foretager et såkaldt step-up i sikkerhedsniveau. Med step-up menes at der er behov for en yderligere sikring af at det er den rigtige person som foretager handlingen(fx anmoder om/udfylder et ydelsesskema eller skrive en klage). Løsningen skal så bede om en ekstra faktor som kan være fx som nu indtastning af engangskode fra et papkort eller indtastning af en kode fra en SMS eller anden form for to faktor mekanisme.

3. Behov for brugervenlighed, herunder forskellige brugeres aktiviteter fra bestilling til anvendelse og eventuel spærring mv.

Bemærkninger / Bidrag:
Ang. NemID selvbetjening til erhverv:

3.a) Dårlig håndtering af fejl, svært at aflevere opgaver og få ikke svar på supportopgaver.

3.b) Dyr prispolitik ift. LRA, betyder at man bibeholder en central administration.

3.c) Forbedring af søgefunktion: Når man søger en specifik bruger frem vises resultatet ikke hvis man har over 500 certifikater. Hvilket betyder at man kan forstå det som at brugeren ikke findes.

3.d) Håndtering af mails: Der sendes mails til LRA om fornyelse af alle V-cert / M-cert. Det er ikke muligt at fra/tilmelde sig disse automatiske mails.

3.e) Mulighed for omdøbning/flytning af bruggergrupper: Det er ikke muligt at omdøbe en brugergruppe til et andet navn eller flytte alle medlemmer af en gruppe til en ny gruppe samtidigt.

3.f) I forbindelse med opgaven som udstedere, kan vi godt ønske os at RA-modulet der anvendes til formålet bliver opdateret hyppigere, hvad angår noteringsfelter o.lign. når der sker ændringer i det dokumentation som borgerne skal fremvise for, at få udstedet et NemID.
I starten var der lagt op til, at man udelukkende måtte udstede på baggrund af de oplysninger man kunne se i RA-portalen og så den dokumentation som borgeren medbringer. På det seneste er der åbnet op for flere dokumentationsmuligheder, dog uden at det er muligt i RA-portalen at anføre hvad man her set af dokumentation.

4. Teknik og infrastruktur, herunder eksempelvis adskillelse af eID og eSignering, single sign-on, sammenhængende IT-arkitektur, sikkerhed mv.

Bemærkninger / Bidrag:
4.a) Det skal sikres at man i den fremtidige version ikke binder sig en teknologi der begrænser anvendelsen på bestemte typer devices, som det var tilfældet med JAVA applet versionen. Dette er dog løst med den kommende nye JavaScript version, men det er fortsat vigtigt at sikre at man ikke låser sig fast til en teknologi der fx ikke understøtter mobile devices.

5. Samspil med interessenter, herunder tjenesteudbydere, administrative procedurer, sikkerhedsprocedurer mv.

Bemærkninger / Bidrag:
5.a) Det skal formidles bedre at certifikater kun er til Autentification, men giver ikke nogen Autorisation(rettigheder), hvilket betyder at man fx godt kan lade medarbejdere bruge deres private NemID til Authenfication på fx virksomhedens Intranet, idet at det er systemet bag Intranettet som skal kontrollere hvad medarbejdere har rettigheder til og dermed om medarbejderen må få adgang til fx Intranettet og hvad han/hun må se på fx Intranettet.

6. Fremtidig forretningsmodel, herunder leverandørstyring, support,

betalingsstruktur, en model med flere leverandører mv.

Bemærkninger / Bidrag:
6.a) Der er behov for en kontraktuelt fleksibilitet i forhold til at kunne understøtte og tilpasse løsningen i forhold til brugernes ændrede adfærdsmønster ligesom de private virksomheder i dag er gode til. Med kontraktuel fleksibilitet menes at løsningen ikke skal være "låst" til kun at kunne virke på en bestemt måde eller på bestemte enheder, men det skal være muligt at opdatere og udvide løsningen løbende indenfor kontraktperioden, således at der ikke nødvendigvis skal gå 3 til 4 år før ny understøtter de ændrede adfærdsmønstre.
Ved at kunne agere som beskrevet ovenfor og være mere agil opnås også mulighed for et stærkere image i forhold til disse fælles offentlige løsninger.

Det skal dog understreges at understøttelsen af de fleksible og nye funktionalitet selvfølgelig ikke på nogen måde må kompromittere det høje sikkerhedsniveau som løsningen skal have.

6.b) Selve brugervenligheden af RA-portal og system kan godt optimeres:

Odense Kommune har løbende deltaget i RA-formum i regi af Digitaliseringsstyrelsen, med deltagelse af KL, SKAT og de kommuner der var med til at udarbejde undervisningssetup m.m.
Her er der løbende kommet en del ændringsønsker, men ofte så kan disse ikke lade sig gøre, da DanID ikke har fået økonomi til dette. Så ved fremtidigt udbud, bør der også sættes økonomi af til, at de praktiske værktøjer løbende kan forbedres og justeres, og i hyppigere takt.

7. Andre bemærkninger

Bemærkninger / Bidrag:
Ingen

Venlig hilsen

Lars Nico Høgfeldt
IT-Arkitekt

Direkte tlf. 65511755
E-mail lanh@odense.dk

Peercraft

Lergravsvej 53
DK-2300 København S
Denmark

Phone: +45 46 96 56 31
Email: peercraft@peercraft.com
VAT: DK 33 75 53 41

Til Digitaliseringsstyrelsen

Svar til høring om næste generation af den nationale identifikations- og digital signaturinfrastruktur (NemID)

Peercraft bifalder den åbne høring og håber at også den videre proces kan foregå i åbent samspil med mulige leverandører og markedets øvrige aktører. Nærværende høringssvar fokuserer dels på den generelt hastige teknologiske og markedsmæssige udvikling og dels på nogle af de specifikke teknologier, som netop nu er undervejs og skønnes at have potentiale til at understøtte fremtidens "data driven business".

1. Fremtidige forretningsmæssige behov, for henholdsvis virksomheder, offentlige sektor og borgere i Danmark og udlandet samt eventuelle juridiske forhold.

Den teknologiske og markedmæssige udvikling
Den nuværende NemID løsning har på grund af sin særlige konstruktion vist sig at være ude af stand til løbende at følge med udviklingen i brugernes udstyr og de heraf affødte ændrede krav i udbudsperioden. Den teknologiske og markedmæssige udvikling vil i den næste 5 års periode ske endnu hurtigere. Især må det formodes at udviklingen af IT-baserede ting og tjenester (f.eks. IoT og Big Data) med tilhørende behov for rettighedsbaseret styring vil ske væsentligt hurtigere i den næste udbudsperiode. Der er ingen, der ved præcis hvordan udviklingen vil ske. Det synes derfor mere relevant at arbejde frem mod leverandøraftaler, der sikrer en løbende udvikling og tilpasning til markedet end at satse på specifikation og udvikling af et enkelt specifikt produkt, som ikke eller kun qua store omkostninger og forsinkelser kan tilpasses udviklingen i markedet og brugernes heraf afledte forventninger.

Det private marked
Det private marked har behov for løsninger, der fungerer interoperabelt og brugervenligt på tværs af nationale grænser. Til private anvendelser skal der endvidere kunne håndteres diverse specifikke attributter, herunder såvel oplysninger som det offentlige kan verificere (f.eks. navn, adresse) som handelsrelevante oplysninger, der kan verificeres af eller benyttes overfor private virksomheder.

Ovenstående betragtninger om den markedsmæssige udvikling gælder i lige så høj grad de fleste andre nationale signatur- og loginløsninger i Europa. De fleste øvrige lande i EU har desuden det problem at deres løsninger anvendes af en meget lille procentdel af borgerne. De er derfor særdeles uegnede til brug i kommercielle sammenhænge, hvor der ønskes en bred tilslutning fra befolkningen.

Løbende konkurrence kan fremme både den offentlige og den private sektor
Såfremt man via udbuddet for identitetshåndtering til offentlige formål samtidigt ønsker at fremme – samt drage fordel af – digitaliseringen I den private sektor, bør afløseren for NemID konkurrenceudsættes på en måde, der sikrer løbende konkurrence mellem leverandørerne.

2. Funktionalitet og anvendelse, herunder eksempelvis niveaudelt sikkerhed, lokal administration af autorisation, single sign-on m.v.

Niveaudelt sikkerhed
Niveaudelt sikkerhed er et ubetinget krav for at kunne tilgodese afvejningen mellem krav til sikkerhed og bekvemmelighed (se også punkt 3). Opgaven med at kvalificere sikkerhedsniveauer i relation til forskellige teknologier, applikationer og brugsscenarier er ikke triviel og bør udskilles som en særskilt opgave. Så vidt muligt i et internationalt samarbejde.

Medarbejdersignatur som roller ift. personlig signatur
Der er personer med officielle roller (bestyrelse, direktion) i op til flere hundrede virksomheder. Der er også personer med andre medarbejderroller i adskillige virksomheder. Idag kræver det etablering og brug af et tilsvarende antal separate medarbejdersignaturer. Dette er I modsætning til den traditionelle signatur, hvor der anvendes en personlig underskrift som tilføjes den aktuelle rollebetegnelse. Muligheden for automatisk at tilknytte CVR-registrerede virksomhedsroller som attributter til en personlig identitet vil være en signifikant administrativ lettelse. Samtidigt vil det kunne sikre at der til enhver tid er overensstemmelse mellem oplysningerne i CVR-registret og borgerens virksomhedsrelaterede rettigheder, hvilket ikke sikres med den nuværende lokaladministration.

Fra simpel ID til rettighedsstyring
Mens NemID idag primært giver borgerne mulighed for at identificere sig over for det offentlige for at få adgang til deres egne oplysninger, vil fremtidens scenarie overvejende være at brugeren kan administrere andres adgang til sine data. For at det skal kunne ske på en brugervenlig måde, er det nødvendigt at standardisere denne rettighedsstyring. En mulig kandidat I denne sammenhæng er “UMA” som baserer sig på Oauth2 og OpenID Connect. Den universelt mest udbredte datadelingsprotokol er Oauth2. En primær ulempe ved Oauth2 er at brugeren skal besøge hver enkelt device eller datahost for at administrere tildeling af rettigheder. UMA løser dette problem ved at give enkeltpersoner og medarbejdere en samlet adgang til at administrere rettighedstildeling til deres data og resurser uanset hvordan de faktiske resurser er distribueret. UMA vil derfor være egnet til rettighedsstyring af personlige oplysninger i såvel privat som offentligt regi.

3. Behov for brugervenlighed, herunder forskellige brugeres aktiviteter fra bestilling til anvendelse og eventuel spærring m.v.

Komplexitet af loginproces
En væsentlig årsag til at NemID ikke har fundet bred anvendelse i den private sektor er den omstændelige indlogningsproces (herunder papkort og manglende SSO). Til ikke-kritiske private anvendelser er det et slutbrugerkrav at login til en tjenesteudbyder kan ske med 0 til 1 (eller allerhøjst nogle få) klik.

Håndtering af mange alternative loginmuligheder
Der opstår let et problem med brugervenligheden, når en tjeneste accepterer mange forskellige typer login, herunder flere Identity Providere, som kæmper om plads på loginsiden. Det betegnes Nascar problemet efter de reklametilklistrede racerbiler. Problemet vil blive accentueret af EU krav om support af de øvrige EU-landes nationale løsninger. Account Chooser fra OpenID Foundation er et forsøg på at løse denne problematik. Google og Symantec hoster en (beta)løsning på internationalt plan, men det bør overvejes om der bør etableres en dansk implementation, f.eks. i regi af DK-Hostmaster, med bedre understøttelse for privatlivs-sikrende identitetsudbydere end ovennævnte.

Peercraft

Lergravsvej 53
DK-2300 København S
Denmark

Phone: +45 46 96 56 31
Email: peercraft@peercraft.com
VAT: DK 33 75 53 41

4. Teknik og infrastruktur, herunder eksempelvis adskillelse af eID og eSignering, single sign-on, sammenhængende IT-arkitektur, sikkerhed m.v.

Pseudonymitet
Af hensyn til interoperabilitet på det europæiske og internationale marked bør det være et krav til løsningerne at de ikke er bundet til brugen af CPR-numre, men kan fungere med parvist pseudonyme identifikatorer overfor tjenesteudbydere ("directed identity")

Hold øje med ny internationale standarder
For at kunne tilbyde den størst mulige sikkerhed, privacy, fleksibilitet og interoperabilitet er det afgørende at afløseren for NemID kan rumme eller interagere med de mange ny internationale standarder og teknologier, der er lanceret i år og forventes løbende suppleret i de kommende år. Undladelse af at gøre dette vil føre til dyrere proprietære løsninger, der ydermere isolerer Danmark kommercielt fra de internationale markeder. Særligt relevante standarder i denne henseende er:

Fido Alliance
Fido er afløseren til traditionelt PKI-baseret login. Princippet er at der genereres et unikt nøglepar til hver tjenesteudbyder, så disse ikke umiddelbart vil kunne korrelere og aggregere brugeroplysninger. De første FIDO produkter (U2F) fungerer et som simpelt HW-token, men efterfølgende vil der komme produkter som inkluderer diverse biometriske faktorer (UAF). Samme hardwaretoken kan med fuld privacy benyttes til alle anvendelser uanset om det er købt af borgeren selv, eller udleveret af arbejdsgiver eller af det offentlige.

OpenID Connect
OpenID connect er en SSO protokol med egenskaber lignende SAML2, som pt. anvendes til NemLog-in. SAML2 har imidlertid vist sig for besværlig at implementere til mange private kundevendte anvendelser, herunder e-handels- og medietjenester. OpenID Connect er allerede implementeret af bl.a. Google, Paypal og Deutche Telekom. GSM Association har påbegyndt arbejdet med at definere en fælles profil af OpenID Connect til brug for sine på verdensbasis ca. 800 teleoperatører.

OpenID Connect definerer endvidere en "self-issued" profil, der sammen med avanceret attributhåndtering gør det teknisk muligt for en bruger selv at optræde som SSO identitetsudbyder. Det bør undersøges og gennemtænkes hvordan en sådan løsning kan bringes til at fungere som én blandt flere løsninger såvel funktionelt som udbuds- og certificeringsmæssigt.

Fordele ved kombination af Fido og OpenID Connect
Fido produkter kan også med fordel benyttes ifm SSO løsninger – dels som login til én eller flere Identitets udbydere – og dels som brugerens alternative indgang til vigtige tjenester ved privatlivshensyn eller såfremt en Identitetsudbyder skulle blive utilgængelig p.g.a. tekniske problemer eller DDOS angreb.

Herudover vil brugen af disse teknologier drastisk kunne nedsætte brugen af brugernavn og passwords og dermed risikoen for phishing.

5. Samspil med interessenter, herunder tjenesteudbydere, administrative procedurer, sikkerhedsprocedurer m.v.

International fokus og indflydelse
Med inspiration fra det tilsvarende arbejde I USA (NSTIC / IDESG) foreslås det at Digitaliseringsstyrelsen faciliterer et aktivt og konstruktivt samarbejde mellem danske (og gerne åbent for udenlandske) aktører med henblik på at afdække behov for standardisering samt eventuelle problemer med bestående internationale standarder. Ved at være på forkant med udviklingen vil Danmark have gode muligheder for at påvirke udviklingen af relevante standarder, så danske krav til sikkerhed og privatlivsbeskyttelse kan sikres samtidigt med sikring af international interoperabilitet.

Praktiske forsøg
De indledende faser af processen mod valg af løsningsmodeller og eventuelt leverandører bør involvere praktiske forsøg med eksisterende løsninger eller prototyper på de løsninger, der bringes i forslag. På den måde opdages eventuelle praktiske problemer langt tidligere i processen end når en større udvikling baseres på teorier og tegnebordsarbejde.

6. Fremtidig forretningsmodel, herunder leverandørstyring, support, betalingsstruktur, en model med flere leverandører m.v.

Der ønskes en betalingsstruktur i tråd med modellen i UK, hvor det offentlige primært afregner driftsmæssigt på baggrund af det antal brugere, der benytter den enkelte leverandør. Det er væsentligt at brugerne frit skal kunne skifte udbyder og eventuelt parallelt kan betjene sig af forskellige leverandører til forskellige formål. Det vil føre til mere brugervenlige løsninger og mere effektiv support end med den nuværende NemID løsning, ligesom det offentliges opgave med at føre tilsyn med kvaliteten af supporten herved reelt overflødiggøres.

Leverandørerne bør have vide rammer mht deres forretningsmodel på det private marked, så der kan etableres såvel bruger- som tjenesteudbyder- og trediepartsfinansierede løsninger.

Princippet er grundlæggende at identiteten tilhører brugeren på samme måde som et traditionelt pas. Leverandører skal derfor uanset forretningsmodel acceptere at brugerne kan videregive oplysninger (attributter) tilknyttet en identitet til en anden leverandør (“data portability”) uden at brugeren eller sidstnævnte leverandør kan pålægges betaling udover eventuel normal betaling for simpelt brug af en identitet til den oprindelige leverandør.

En mulig løsning kunne være at det offentlige selv stod for en simpel minimalløsning, som udelukkende tillod leverandører og borgere at generere afledte identiteter med brugervalgte sæt af attributter i form af certifikater eller overdragelse via API til en af brugeren valgt identitetsudbyder.

København, d. 27/6/2014,

Henrik Biering
Peercraft ApS

Høringssvar

Vedr. Offentlig høring om næste generation af den nationale identifikations- og digital signaturinfrastruktur (NemID)

Afsender	PFA Pension
Dato	4. august 2014

Til hvem det måtte vedkomme

Det er netop blevet undertegnede bekendt at der har været denne høring om næste generation af NemID, hvis svarfrist er udløbet, ønsker jeg alligevel at give mit input til da det vil kunne give brugerne af NemID en væsentlig bedre brugeroplevelse.

Mit ønske er tidligere sendt til NemID, der har oplyst at man med den nuværende løsning ikke kan understøtte ønsket og har derfor opfordret mig til at sende ønsket til høringen.

Her i PFA og arbejder vi med at få svartiderne ned så bruger/kundeoplevelsen med NemID bliver bedre. I den forbindelse kan vi ved login lave en løsning som er som følger. Når man skriver sit login, der ligesom ved de flestes brug af NemID er ens CPR nr, og dernæst exit'er ud af login input-boxen og ind i password input-boxen, kan vi sende et Ajax/asynkront HTTPS kald med CPR nummeret fra klienten til serveren (der returnerer HTTPS kode "204 No content" med det samme) om at en bestemt bruger/CPR nr er ved at logge ind. Serveren kan så starte en tråd som kan finde kundes data (policer aftaler m.v.) frem på serveren imens brugeren taster password ind og holde/cache kundens data og så vise det til kunden når der er har indtastet passwordet og logget ind. Ved den løsning sparer vi brugeren/kunden for den tid, der ellers skulle ventes mens serveren finder brugerens data frem. Vi kan implementere denne løsning for vores normale login/password løsning, mens at vi med den nye NemID løsning ønsker at kunne lave (eller få mulighed for at lave) et sådant kald, der vil have stor betydning for brugeroplevelsen; ikke kun for PFA, men for alle de websites som bruger NemID. (Serveren skal ved løsningen sikres mod DoS angreb ved sådant et kald; samt at der ikke bliver forskel på tiden kaldet tager, så der ville kunne skelnes mellem om et CPR nr. er kunde eller ej).

Håber at ønsket vil blive taget i betragtning.

Med venlig hilsen

Kenneth Reinhardt
Java Udvikler - IT Frontend
- E: ker@pfa.dk

PFA PENSION
Sundkrogsgade 4, DK-2100 København Ø, T: 39 17 50 00, www.pfa.dk

Høringssvar

Vedr. Offentlig høring om næste generation af den nationale identifikations- og digital signaturinfrastruktur (NemID)

Afsender	Projekt UDENFOR
Dato	27. juni 2014

Kære Digitaliseringsstyrelse

Projekt UDENFOR har to punkter som vi gerne vil gøre opmærksomme på i forbindelse med genudbydelsen af NemID.

1. Dette punkt formoder jeg hører under brugervenlighed og anvendelse. Der har været tilfælde hvor vi har hjulpet en hjemløs borger med aktivering af NemID og hvor det ikke har været muligt at benytte sig af sit cpr-nr. som bruger-ID, fordi det allerede er koblet på et andet NemID, som ligger i systemet og "spærrer" – også selvom der er tale om et NemID, som borgeren aldrig har modtaget eller aktiveret.

   En begrundelse vi har fået fra Borgerservice er, at bankerne på et tidligt tidspunkt sendte NemID af sted og ud i systemet og disse er knyttet til borgernes cpr-nr. - også selvom de ikke er blevet modtaget og aktiveret. Når borgerne så på et senere tidspunkt går ned på Borgerservicecentrerne for at skaffe NemID, kan de ikke gøre brug af deres cpr-nr. som bruger-ID.

   For mange af de hjemløse mennesker vi arbejder med (og sikkert også mange andre borgergrupper) er det en udforing at skulle huske koder og derfor gør det, det kun sværere for borgerne at skulle benytte NemID, når de pludselig skal huske to koder, hvis de ikke kan benytte deres cpr-nr., som for mange sidder på rygraden.

2. Dette punkt hører under brugervenlighed og bestilling. Kravene til at få udstedt NemID bør genovervejes i forhold til kravene om gyldig billedlegitimation – hvilket er nødvendigt, når du som hjemløs ikke har en folkeregisteradresse. Gyldige billedlegitimation som pas og kørekort er begge meget dyre og det er ingen garanti at de hjemløse nogle sinde har haft nogle af delene.

   Det ender derfor med for mange hjemløse at blive en stor økonomisk omkostning at anskaffe sig NemID og det kan for mange også være en meget forvirrende proces at finde rundt i, hvilket bliver årsagen til at NemID vælges fra.

Hvis jeg i overstående ikke forklare mig tydeligt nok og I har brug for afklaring, er I velkommen til at ringe eller skrive.

Venlig hilsen

Tabita Nyberg Petersen, pædagog tilknyttet IT-projektet

Ravnsborggade 2-4, 3. sal

2200 København

Mobil: +45 40 91 45 82

www.udenfor.dk

Fonden projekt UDENFOR kombinerer gadeplansarbejde med forskning i hjemløshed og udstødelse.

Husk du kan støtte vores arbejde via sms. Send "UDENFOR" til 1231, så giver du 100 kr. + alm. SMS-takst til vores hjælpearbejde.

Høringssvar

Vedr. Offentlig høring om næste generation af den nationale identifikations- og digital signaturinfrastruktur (NemID)

Afsender	Region Syddanmark
Dato	27. juni 2014

Ang. Offentlig høring om næste generation af den nationale identifikations- og digital signaturinfrastruktur (NemID)

1. Fremtidige forretningsmæssige behov

Jeg vil gerne citere Hans Henrik Bøttger (RegionMidt) da jeg mener at dette punkt er helt fundamentalt:

"Der skal ske en adskillelse rettighedsstyring og administration af signatur. Rettighedsstyring er ikke en del af OCES konceptet og signaturpolitikken. Der skal ikke tildeles rettighedsattributter til certifikaterne i MOCES-administrationsløsningen. Rettighedsstyring ligger hos det modtagende system og brugeres rettighedsattributter skal styres der.
Der skal ikke nedarves rettigheder fra certifikatet til systemer (som der sker hos SKAT), men rettighederne i det tilgående system administreres lokalt som det sker i f.eks. SEI.
Det er vigtigt at certifikatpolitikkerne overholdes præcist og tages alvorligt."

Og jeg erklærer mig tillige enig i at det er nødvendigt at sikre 24-7 tilgængelighed af certifikaterne. Desuden skal man kunne bruge certifikaterne uden en tidsmæssig belastning.

2. Funktionalitet og anvendelse

Der ønskes en løsning for udstedelse af MOCES som går hurtigt og ikke er administrativt og auditmæssigt omstændeligt. Det kunne eksempelvis være straksudstedelse med identifikation af medarbejderen via POCES.

Det samme gælder for genudstedelse og fornyelse.

Gode søgemuligheder i alle OCES varianter. CPR søgning* på MOCES er vigtigst, men også søgning på mailadresser, delvise søgninger osv.

Mulighed for administratordefinerede udtræk af OCES.

Da læger i regionerne kan arbejde på flere forskellige sygehuse, ønskes en arkitektur, hvor det er muligt at en medarbejder kun har ét certifikat, som unikt identificere denne medarbejder på tværs af regionen.

*) CPR søgning var muligt i OCES I, men er ikke mulig i OCES II og det står øverst på administratorernes ønskeliste.

3. Behov for brugervenlighed

Det skal være let for en bruger at bruge sit OCES certifikat, det er en selvfølge.

Der skal ydermere være fokus på brugervenlighed for administratorer af OCES, og der skal være en vejledning af brugen og administrationen til administratorer.

I OCES II er det en langsommelig proces med mange klik og lange ventetider for hvert klik at udføre administration. Det skal være muligt at opsætte brugsparametre for den enkelte virksomhed, så administrationen kan tilpasses virksomhedens størrelse og dermed understøtte brugervenlighed for både små og store virksomheder.

Eksempler på modstridende ønsker til brugervenlighed kunne være:

	Lille virksomhed	**Stor virksomhed**
Fremsøgning af MOCES	Automatisk visning af alle MOCES certifikater tilknyttet virksomheden	Direkte til ”Avanceret søgning” hvor man kan søge på f.eks. CPR og kun fremsøge et udsnit af MOCES tilknyttet virksomheden
Sletning af OCES	En ad gangen	Mulighed for masse slet
Oprettelse af OCES	En ad gangen	Mulighed for masse opret
Ændring af OCES	En ad gangen	Mulighed for masse ændring
Administratorrettigheder	Kun brug for standard administratorroller (Superadministrator og evt. administrator)	Brug for flere grupper af administratorer med rettigheder der tilpasses den enkelte virksomhed af Superadministrator.

4. Teknik og infrastruktur

Det skal være muligt at integrere op mod den centrale løsning, så man administrativt kun behøver at administrere certifikater ét sted. Men det skal også være muligt at administrere det direkte på den centrale løsning gennem en browser.

5. Samspil med interessenter

Det skal være nemt og overskueligt at sammenholde modtagne services i forbindelse med OCES, og med den fakturering der sker af brugen af OCES.

Det skal være nemt for TU (tjenesteudbyder) at holde sig opdateret med evt nye versioner, og kompleksitet i drift og vedligehold hos TU skal holdes på et minimum.

6. Fremtidig forretningsmodel

Der ønskes mulighed for at kunne skifte leverandør af OCES, hvis den valgte ikke lever op til de behov de opstår i regionerne.

Der kunne også være en opdeling så VOCES og FOCES var leveret af en leverandør og MOCES og POCES af en anden – de to sidste kunne endda være splittet op.

Det skal være muligt at følge de sager man har indrapporteret til leverandøren. Der skal være vidende og hurtig support.

7. Andre bemærkninger

Venlig hilsen

Mette Thøgersen
Product Manager
Integration og Planlægning

Regional IT - ***IT med værdi***

E-mail: Mette.Thogersen@rsyd.dk

Direkte:

Mobil: 21599069

Region Syddanmark

Damhaven 12, 7100 Vejle

Hovednummer:

www.regionsyddanmark.dk

Justitsministeriet
Budget- og Planlægningskontoret

Sagsbehandler: JGP.
J.nr. 2014-005-134

24. juni 2014

RIGSPOLITICHEFEN

Direktionssekretariatet
Polititorvet 14
1780 København V.

Telefon: 3314 8888
Direkte: 4515 2001

E-mail: politi@politi.dk

Ved e-mail af 11. juni 2014 har Justitsministeriet anmodet Rigspolitiet om en udtalelse i anledning af Digitaliseringsstyrelsens høring af 28. maj 2014 om næste generation af den nationale identifikations- og digital signaturinfrastruktur (NemID).

I den anledning skal Rigspolitiet indledningsvis bemærke, at det er Rigspolitiet bekendt, at der i den kommende tid vil blive taget initiativ til at stille yderligere krav om anvendelse af NemID ved køb af varer og tjenesteydelser over internettet. Dette vil efter Rigspolitiets vurdering væsentligt nedbringe risikoen for identitetsmisbrug.

I forlængelse heraf skal Rigspolitiet anbefale, at NemID fremover i større omfang integreres i brugen af alle systemer, der er offentlig adgang til, herunder særligt systemer med personhenførbare oplysninger eller systemer med brudstykker af personhenførbare oplysninger, der sammen med andre oplysninger kan samles til personhenførbare oplysninger. Eksempelvis kan man flere steder på internettet finde en persons fødselsdata, som efter behandling i en såkaldt cpr-generator på internettet kan give en oversigt over mulige personnumre, der dernæst kan afprøves på eksempelvis den offentlige portal www.tinglysningsretten.dk. Et hit vil herefter medføre viden om en persons personnummer. Adgang via NemId vil i betydeligt omfang begrænse et sådant misbrug og styrke efterforskningsmulighederne, hvis misbruget har fundet sted.

Endvidere skal Rigspolitiet anbefale, at det såkaldte nøglekort udgår og erstattes med f.eks. en hardwarelås (USB-dongle) til sikker netbanking, idet et nøglekort kan kopieres og misbruges. Det kan i den forbindelse oplyses, at i en nylig sag er flere hundrede nøglekort på baggrund af en phishing-mail kopieret og videresendt til bagmænd.

Med venlig hilsen

Pernille Breinholdt Mikkelsen
sekretariatschef

Til
Digitaliseringsstyrelsen

27. juni 2014

Vedr. Offentlig høring om næste generation af den nationale identifikations- og digital signaturinfrastruktur (NemID)

RfDS påskønner den åbenhed, digitaliseringsstyrelsen udviser ved at iværksætte denne høring om næste generation af den nationale identifikations- og digital signaturinfrastruktur (NemID). Det er en vigtig del af den offentlige infrastruktur, at vi har en troværdig digital identitet, således at borgere og virksomheder kan være trygge ved anvendelsen af digitale løsninger i det offentlige, samt at vi får en løsning som understøtter behovet for en sikkerhedsmæssig robust anvendelse af digital kommunikation af fortrolig information.

Det er derfor positivt, at Digitaliseringsstyrelsen afholder en høring tidligt i forløbet. RfDS vil gerne opfordre til, at resten af processen også bliver en åben proces, og at afklaringsprocessen frem mod design og krav til næste generation af digital ID inddrager aktører bredt. RfDS anser næste generation af national digital id-løsning for en vigtig forudsætning for sikkerhed og tryghed ved digitale løsninger og digital kommunikation, og vi indgår derfor gerne i en sådan proces.

RfDS' kommentarer nedenfor under punkt 1-7 bygger på følgende principper:

- **Integritet:** Borgerens digitale identitet bør tilhøre borgeren på samme måde som et pas til traditionel identifikation. Brugeren bør derfor kunne autentificere sig over for tredjepart og eventuelt få etableret afledte identiteter uden at dette bliver registreret hos udstederen.

- **Autentifikation**: Styrken og troværdigheden af en digital identitet bør ikke udelukkende være bundet til den anvendte teknologi, fx den *token*, der repræsenterer den digitale identitet; den er i højere grad bundet til sikker autentifikation af den person, som en bestemt identitets *token* er udstedt til.

- **Fortrolighed**: Opbevaringen af den fortrolige del af identiteten er afgørende for at hindre misbrug og identitetstyveri, ligesom de tjenester som identiteten anvendes mod, skal stille en sikker infrastruktur til rådighed, som hindrer kompromittering og er robuste mod falsknerier og andet misbrug som fx phishing. Det er således ikke udelukkende en digital identitet, der skal efterspørges, men i lige så høj grad tjenester, der effektivt kan sikre *fortrolighed*.

- **Privatlivsbeskyttelse:** eID bør generelt afløse brug af CPR nr. som gennemgående ID i den offentlige sektor og private sektor. *Privacy enhancing technologies* (PET) der sikrer 'skjult identitet' i databaser, og kun åbner for identifikation, når det er nødvendigt, bør indtænkes i den nye NemID-løsning.

Rådet for Digital Sikkerhed, Toldbodgade 12, 1253 København K, Danmark - CVR-nr.: 34757488
Web: www.digitalsikkerhed.dk Mail: info@digitalsikkerhed.dk

- **Åbenhed:** den kommende løsning bør understøtte flere forskellige identitetsudbydere. Dette kan skabe et egentligt marked for identitetsudbydere og vil reducere afhængigheden af enenkelt løsning i tilfælde af nedbrud. Derudover vil det sikre et system, der er kompatibelt med andre europæiske eID-systemer.

Med udgangspunkt i ovenstående principper har RfDS følgende mere specifikke kommentarer:

1. Fremtidige forretningsmæssige behov, for henholdsvis virksomheder, offentlige sektor og borgere i Danmark og udlandet samt eventuelle juridiske forhold.
RfDS mener, at en ny NemID-løsning skal kunne tilbydes af flere forskellige udbydere. Teknologi, som muliggør dette, er tilgængelig, og der er brug for valgfrihed for både private brugere og virksomheder. Der er derfor behov for, at designet af den nye løsning tager afsæt i en åben platform, som giver adgang for flere leverandører af eID.

Hermed imødekommes også et behov for levering af eID, der bygger på differentierede kontekstafhænge identiteter der matcher behovene ift. forskellige serviceudbydere.

RfDS anser den offentlige digitale identitet som én af mange digitale identiteter, som den enkelte fremover kan anvende afhængigt af den aktuelle kontekst. Der bør ske en differentiering af digitale identiteter som den enkelte kan og bør anvende. Kommunikationen mellem borger og det offentlige består af både stærkt fortrolige og mindre følsomme oplysninger. Den offentlige digitale identitet skal derfor både bestå af en identitet på almindeligt sikkerhedsniveau og en identitet, der har tilstrækkelig styrke til at borger og virksomheder trygt kan kommunikere med det offentlige selv med de mest følsomme informationer. Den stærke identitet skal være forbeholdt den bindende og stærkt fortrolige kommunikation samt til brugeren generering af afledte identiteter.

Den offentlige digitale identitet bør sammen med andre digitale identiteter kunne benyttes valgfrit af brugeren i kontakten til virksomheder og handlende.

RfDS anbefaler derfor et konkurrencepræget flerleverandør marked med repræsentation af flere (markedsdrevne) forretningsmodeller, der kan imødekomme forskellige behov for digital identifikation i både offentlig sektor og privat sektor og tilvælges af den enkelte bruger.

2. Funktionalitet og anvendelse, herunder eksempelvis niveaudelt sikkerhed, lokal administration af autorisation, single sign-on m.v.
RfDS finder det afgørende af hensyn til såvel sikkerhed som fortrolighed, integritet, autentifikation og fortrolighed, at den nye NemID løsning bygger på følgende krav til funktionalitet og anvendelse:

Standarder
Ved brug af forskellige leverandører til forskellige opgaver, vil der være behov for forskellige sikkerhedsniveauer: password, to-faktor med en-gangs password, biometri m.v. RfDS finder det afgørende, at disse sikkerhedsniveauer er defineret i standarder, der bl.a. stiller krav til minimumssikkerhed.

Sådanne standarder vil kunne bidrage til at minimere tjenesteudbydernes tekniske merarbejde for de forskellige NemID-udbydere, de ønsker at understøtte. En løsning kan tage afsæt i eksempelvis Open Card arkitekturen eller lignende. En serviceudbyder kan selv afgøre hvilke(n) eID virksomheden vil

Rådet for Digital Sikkerhed, Toldbodgade 12, 1253 København K, Danmark - CVR-nr.: 34757488
Web: www.digitalsikkerhed.dk Mail: info@digitalsikkerhed.dk

acceptere inden for minimumskravene til sikkerhed. Det afgørende er, at kravene til sikkerhed er medtænkt i udviklingen af de mest brugervenlige løsninger.

Akkreditering af tredjepart
En digital identitet skal kunne anvendes mod det offentlige i de tjenester der udbydes, men også mod de underleverandører af halvoffentlige tjenester, som akkrediteres til at kunne autentificere identiteten. Der vil dog være tredjeparts identitets-tokens, som kan have tilstrækkelig troværdighed til at offentlige tjenester skal kunne acceptere dem til ikke personfølsomme udvekslinger.

Digital signatur
eID skal kunne anvendes til en autentificerbar identifikation over for offentlige myndigheder, og til signering af ansøgninger, indberetninger og aftaler. Ligeledes skal den kunne anvendes til at underskrive aftaler med retsvirkning. Dette kræver ikke blot, at man beslutter at den digitale signatur har retsvirkning, men også at identiteten og den omgivende sikkerhedsinfrastruktur er tilstrækkelig robust til, at man efterfølgende har optimale vilkår for at eftervise, at den digitale signatur ikke er forfalsket.

Single sign-on
Single sign-on løsninger skal kunne håndtere tjenesteudbydernes forskellige krav til sikkerhed og understøtte "step-up" autentifikation (med samme løsning) eller om nødvendigt henvisning til anden autentifikationsløsning. F.eks. vil bestilling af en lægetid ikke skulle kræve den højeste troværdighed af identiteten, men ved viderestilling til egen patientjournal skal der sikres autentifikation af brugeren til det højere sikkerhedsniveau.

Autorisation og fuldmagt
Der bør udvikles en fuldmagt til fx læger, revisorer og advokater med specifikke rettigheder til de informationer, de skal kunne tilgå. Dette skal være tværgående inden for alle myndigheder, således at et sagsforløb kan gennemføres med den rette fuldmagt, men samtidigt således at borgeren reelt er i fuld kontrol med hvilke data om personen, som den enkelte fuldmagtshaver kan opnå adgang til.

Ved virksomhedsidentiteter skal det være muligt at virksomhederne selv definerer, hvad de enkelte medarbejdere, der har en virksomheds digitale identitet, kan få adgang til at se og ændre. Dette kan implementeres gennem den token, der anvendes ved login (fx SAML2), eller via en webservice, så virksomhedernes interne autorisationssystemer kan administrerer disse rettigheder.

Det bør gøres muligt for virksomheder at bruge den nye NemID-løsning til at underskrive Oauth Access Grants og lignende digitale fuldmagter, således at der kan anvendes serviceleverandører eller tilbydes serviceydelser.

Tilsvarende løsninger bør udvikles til borgerne, så de selvvalgt kan delegere brug af deres eID til begrænsede formål. Det vil være relevant fx for IT-svage personer, der ved brug af den nuværende NemID-løsning i praksis blot udleverer deres NemID credentials til familiemedlemmer eller andre, hvilket er meget uhensigtsmæssigt.

Analogt supplement
Det er ikke alle borgere og virksomheder, der er parate til eller har mulighed for udelukkende at benytte digital kommunikation. Rådet for Digital Sikkerhed foreslår derfor, at der i forbindelse med den nye nemID-løsning indtænkes en mulighed for at behandle en henvendelse analogt, fx via indskannede dokumenter, hvor den analoge underskrift udgør den digitale autentifikation. Udover at imødekomme et behov hos borgere og virksomheder, vil et analogt supplement også

Rådet for Digital Sikkerhed, Toldbodgade 12, 1253 København K, Danmark - CVR-nr.: 34757488
Web: www.digitalsikkerhed.dk Mail: info@digitalsikkerhed.dk

muliggøre samarbejde med andre EU-myndigheder, som ikke er i stand til at levere fuld eID-funktionalitet.

3. Behov for brugervenlighed, herunder forskellige brugeres aktiviteter fra bestilling til anvendelse og eventuel spærring m.v.
RfDS finder det afgørende at en ny NemID-løsning sikrer, at brugervenlighed og tilgængelighed kombineres med krav om troværdig udstedelse og anvendelse samt gennemskuelige sikkerhedsløsninger, der kan anvendes af alle.

Tilgængelige sikkerhedsløsninger
RfDS anbefaler, at der indarbejdes sikkerhedsløsninger, der skaber effektiv sikkerhed og let tilgængelighed for alle brugere. Det kan opnås ved at:

- Erstatte den nuværende udlevering af samme tekniske identifikator for en bruger (PID eller RID) til alle tjenesteudbydere med udlevering af unikke identifikatorer til hver tjenesteudbyder, svarende til systemerne hos fx Facebook og Google.

- Skabe adgang til nøglehåndtering på tværs af teknologiske platforme som fx Java, .net og Linux.

- Gøre det muligt at benytte eID på tværs af hardwareenheder som fx PC, slates, tablets og smartphones.

- Basere det Offentlige Danmarks NemID løsning på to-faktor sikkerhed med en-gangs nøgler. I tilfælde hvor der gives adgang til personfølsomme data eller væsentlige transaktioner, bør der efter Rådets mening kobles en tredje sikkerhedsfaktor på, som fx biometri.

- at åÅbne for to-faktor sikkerhed, der er understøttet af et udvalg af de elektroniske to-faktor autentifikationsteknologier, som er på markedet i dag og i vid udstrækning bruges globalt.

- Sikre kompatabilitet med udbredte ID-systemer som fx Facebook, hvor dette sikkerhedsniveau vurderes at være tilstrækkeligt.

- Skabe adgang til andre to-faktor mekanismer baseret på åbne standarder, som fx OTP-kortet og tredjepartsløsninger der bygger på åbne standarder som RFC 6238 (både Google Authenticator og Microsoft Authenticator benytter denne standard og kan derfor kryds-authenticate)[1].

Kryptering
RfDS anbefaler, at næste NemID løsning tilbyder en bedre løsning til kryptering af mails og på den måde medvirker til at fremme sikker mail kommunikation. Det kan ske fx ved at tilbyde X.500 certifikater, som giver mulighed for kryptering og signering af e-mail. Det bør i den sammenhæng gøres enklere at oprette og modtage certifikat til eget mailprogram, herunder sådanne der kan anvendes til webmail. Der bør fortsat være mulighed for virksomhedscertifikater som en løsning for signering og kryptering. Det kan ikke forventes, at alle almindelige anvendte mail-providers vil

1 Se fx RFC 6238: http://tools.ietf.org/html/rfc6238

Rådet for Digital Sikkerhed, Toldbodgade 12, 1253 København K, Danmark - CVR-nr.: 34757488
Web: www.digitalsikkerhed.dk Mail: info@digitalsikkerhed.dk

understøtte en sådan infrastruktur. Det bør derfor overvejes, om det offentlige selv skal stille en sikker dialogbaseret kommunikation til rådighed, når der er behov for dette.

4. Teknik og infrastruktur, herunder eksempelvis adskillelse af eID og eSignering, single sign-on, sammenhængende IT-arkitektur, sikkerhed m.v.
RfDS anbefaler, at det i forberedelsen af næste generation af digital ID medtænkes, at CPR-nr. afvikles som gennemgående ID i offentlige registre m.v. Der må tænkes i ny former for ID, der mindsker risiko for identitetstyveri og øger privatlivsbeskyttelsen ved at undgå ens identifikation generelt i den offentlige og store dele af den private sektor.

Der bør samtidig medtænkes muligheder for udbrede privatlivsfremmende teknikker, som giver 'skjult identitet' i databaser, der først kan meddeles, når der er behov (f.eks. efter indehaverens samtykke) eller slet ikke kan meddeles, når der ikke er behov herfor i den digitale løsning.

Et centralt greb til at skabe både effektiv sikkerhed og privatlivsbeskyttelse er efter RfDS' opfattelse brug af pseudonymisering.

Fra et integreret it-sikkerheds og privatlivsbeskyttelsesperspektiv, er det derfor efter RfDS opfattelse centralt for en ny NemID-løsning, at den:

- Kan implementere flere forskellige sikkerhedsniveauer, afhængigt af dataklassifikation, risikoprofil etc. og dermed give mulighed for bredere anvendelse.
- Understøtte teknologier som helt eller delvis fjerner behovet for indtastning af brugernavn og adgangskoder som fx FIDO Alliance U2F og UAF (biometrisk).
- Ikke kræver brug af samme brugernavn og adgangskoder til flere identitets- og/eller tjenesteudbydere eller kræver indtastning af disse oplysninger, hvor modtagerens identitet ikke på simpel vis kan verificeres af en almindelig bruger.
- Understøtter krypteringsteknologier som fx IBMs IdentityMixer og Microsofts U-Prove ved brug af attributter og pseudonymer.
- Introducerer et sikret hardware modul, som kan vise den transaktion, man er ved at godkende/signere som fx det tyske ChipTAN system. Det vil vanskeliggøre man-in-the-middle angreb, som har vist sig at være den største udfordring ved det eksisterende system.
- Gør det enkelt at tilbyde eID til børn og unge samt til tjenester og aktiviteter, hvor man i dag ikke benytter NemID, men i stedet af anvender mindre sikre identitetsløsninger.

5. Samspil med interessenter, herunder tjenesteudbydere, administrative procedurer, sikkerhedsprocedurer m.v.
RfDS opfordrer til, at afklaringsprocessen frem mod design og krav til næste generation af eID afdækker følgende emner ved inddragelse af en bred kreds af såvel danske som udenlandske interessenter:

Rådet for Digital Sikkerhed, Toldbodgade 12, 1253 København K, Danmark - CVR-nr.: 34757488
Web: www.digitalsikkerhed.dk Mail: info@digitalsikkerhed.dk

- Deltagelse i udviklingen af åbne , internationale og veldefinerede standarder for sikkerhedsniveau og privatlivsbeskyttelse.

- Nødvendige trust-relationer med internationale eID-løsninger, der kan sikre friest mulig international interaktion og bevægelighed.

- Muligheder for samarbejde i nærområdet i Norden, hvor mange krydser grænserne både i forbindelse med job og bosættelse.

- Undersøgelse af erfaringerne fra eID-samarbejdet mellem Finland og Estland i forhold til mulighederne for at etablere en større fælles eID-løsning.

6. Fremtidig forretningsmodel, herunder leverandørstyring, support, betalingsstruktur, en model med flere leverandører m.v.
Den hidtidigt anvendte model med en licensieret og økonomisk støttet leverandør er en akilleshæl for den digitale infrastruktur. Det skal sikres, at det er attraktivt for flere leverandører at levere et eller flere niveauer af digitale identiteter.

RfDS anbefaler derfor, at den nye NemID løsning udformes, så den medvirker til at skabe et egentligt marked for identitetsudbydere. På den måde kan afhængigheden af enkelt løsning i reduceres, hvilket har særlig betydning i forbindelse med nedbrud. Derudover vil det bidrage til udvikling af et system, der er kompatibelt med andre europæiske eID-systemer.

Med venlig hilsen

Formand
Birgitte Kofod Olsen

Næstformand
Rasmus Theede

Rådet for Digital Sikkerhed, Toldbodgade 12, 1253 København K, Danmark - CVR-nr.: 34757488
Web: www.digitalsikkerhed.dk Mail: info@digitalsikkerhed.dk

Digitaliseringsstyrelsen
kis@digst.dk

RÅDET FOR SOCIALT UDSATTE

Dato 27. juni 2014

Vedr. høring om næste generation af identifikations- og digital signaturinfrastruktur

Rådet for Socialt Udsatte takker for muligheden for at komme med bemærkninger i forbindelse med et genudbud af NemID.

Rådet er talerør for socialt udsatte borgere, der er kendetegnet ved at have komplekse og sammensatte problemer som misbrug, sindslidelse, hjemløshed mv. For mange socialt udsatte er der store udfordringer forbundet med den stigende brug af digital kommunikation. Rådet er selvfølgelig af den grundholdning, at retssikkerheden skal være i top. Under hensyn til dette er det fra Rådets perspektiv vigtigt at sikre så enkle og brugervenlige løsninger som muligt. Det er fx løsninger hvor man ikke skal læse så meget tekst, hvor man ikke skal huske mange kodeord osv. Det er også en udfordring for mange hjemløse at opbevare deres nøglekort til NemID og det kan for mange være en stor udfordring at få et NemID nøglekort via borgerservice, fordi det kræver billedlegitimation. Processen og prisen for at få et sådant fremstår ofte uoverskuelig. Identifikationsprocessen bør derfor forenkles så meget som overhovedet muligt.

For mange udsatte er det vigtigt at kunne tale med en person, som kan guide og hjælpe når der er brug for det. Det bør som udgangspunkt ske på borgerservice eller i det evt. værested som borgeren benytter. Som et supplement bør der som minimum være et gratis hotline nummer, hvor borgeren ikke oplever at blive vist videre og hvor de kan få en nærværende hjælp ved akut behov.

En anden udfordring som der bør overvejes er de juridiske aspekter i forbindelse med at få assistance til at håndtere digital kommunikation. Rådet har fx kendskab til værestedspersonale, som oplever nogle dilemmaer når de assisterer og 'oversætter' den digitale kommunikation.

Med venlig hilsen

Jann Sjursen

Høringssvar

Vedr. Offentlig høring om næste generation af den nationale identifikations- og digital signaturinfrastruktur (NemID)

Afsender	SAND – De hjemløses landsorganisation
Dato	27. juni 2014

SAND – De hjemløses landsorganisation vil indledningsvis takke for høringsskrivelsen.

Desværre har vi ikke mange løsningsforslag. Vi har flere opmærksomhedspunkter, der kræver kreative løsninger.

Ad. 1. Fremtidige behov

Implicit i den nuværende løsning ligger der en antagelse om at alle borgere har adgang til dels en computer, dels et sikkert sted man kan opbevare sit nøglekort. Min påstand er at mange hjemløse ikke har disse to muligheder. De er afskåret fra at komme på bibliotekerne. Enten fordi de er påvirkede eller fordi de er usoignerede. Andre har angst for andre mennesker og ønsker ikke at være indendørs. Vi ved at Borgerservice/Socialforvaltninger i stigende grad udelukker folk fra at henvende sig fysisk og at selvsamme kontorer indskrænker åbningstider i digitaliseringens og spareiverens hellige navn.

En baglomme i de bukser man har på 24 – 7 er ikke et sikkert sted. Især ikke hvis man sover på sovesal med mange andre eller er meget kaotisk. Begge del noget vi i stigende grad ser. De hjælpeinstanser der findes for hjemløse, bliver udsultet, hvorfor hjemløse har sværere og sværere ved at finde personer, der kan hjælpe dem med det tekniske elementer i en NEM ID løsning eller med at få adgang til en computer.

Jeg vil anbefale at man vier speciel meget opmærksomhed på denne gruppe borgere, hvis man vil lave en løsning, der kan inkludere dem.

Der må være parralle problemstillinger med demente og psykisk syge og måske løsningsmodeller man kan lade sig inspirere af.

Til sidst en opfordring til et eksperiment I kan udføre (til personalefesten om ikke andet): I er Robinson Crusoe på den øde ø. Han skal bruge NEM ID og det eneste der skyller op på land er den ene dunk brændevin efter den anden. I skal finde en løsning.

God fornøjelse med det videre arbejde. SAND vil meget gerne bistå jer med at udvikle og afprøve fremtidige løsningsmuligheder.

Med venlig hilsen
Ask Svejstrup, sekretariatsleder

SAND - De hjemløses landsorganisation
Sundholmsvej 34, st.
2300 København S
Tel. 89 93 70 60/20 98 79 21
Mail: ask@sandudvalg.dk

Digitaliseringsstyrelsen

Notat

Offentlig høring om næste generation af den nationale identifikations- og digital signaturinfrastruktur (NemID)

Overordnet finder SKAT, at der i forhold til den fremtidige NemID skal lægges stor vægt på at etablere en løsning med høj grad af brugervenlighed, herunder at den fremtidige NemID i højere grad møder såvel små som store virksomheders behov for en løsning, der er let at anskaffe, administrere og anvende.

SKAT ønsker, at muligheder og udfordringer ved en niveaudelt sikkerhedsløsning analyseres i forbindelse med den udbudsforberedende analyse.

Herudover lægger SKAT vægt på, at der findes en løsning, der kan håndtere alle potentielle brugergrupper, sådan at myndighedsspecifikke løsninger kan udfases, og at den fremtidige NemID så vidt muligt samtænkes med de igangværende EU-initiativer i forhold til gensidig anerkendelse og accept af elektronisk identifikationsløsninger.

I forhold til de konkrete høringstemaer:

1. Fremtidige forretningsmæssige behov,

for henholdsvis virksomheder, offentlige sektor og borgere i Danmark og udlandet samt eventuelle juridiske forhold.

- Den fremtidige løsning skal anvende åbne standarder (internationale, EU og DK standarder).
- Den fremtidige løsning skal kunne anvendes i myndigheder og private virksomheders forretningssystemer (herunder Netbanker)
- Den fremtidige løsning skal bl.a. understøtte elektronisk identifikation, kryptering, signering og sikker e-mail.
- Den fremtidige løsning skal håndtere alle virksomheds- og borgergrupper, også dem, der ikke er i besiddelse af cpr- eller cvr-nummer

2. Funktionalitet og anvendelse,

herunder eksempelvis niveaudelt sikkerhed, lokal administration af autorisation, single sign-on mv.

- Infrastrukturen skal understøtte digital forvaltning.

- I analysen af den fremtidige løsning bør det undersøges, hvordan NemLog-in kan integreres direkte på en side hos den enkelte tjenesteudbyder, frem for at findes på en særskilt mellemside. Uden at sikkerheden kompromitteres.
- Den fremtidige løsning skal etableres i flere funktionelt adskilte niveauer eller særskilte enkeltløsninger.
- Den fremtidige løsning skal kunne anvendes med sikkerhedscertifikater på SmartPhones / PDA
- Der bør ikke anvendes "slanke" identifikationsløsninger, da det fremtidige trusselsbillede ændres markant.

3. Behov for brugervenlighed,

herunder forskellige brugeres aktiviteter fra bestilling til anvendelse og eventuel spærring mv.

- Den fremtidige løsning skal anvende flere multimedie midler, som letter anvendelsen for alle interessenter, herunder brugere (film, billeder etc.).
- Der skal etableres registreringsløsninger, der sikrer en let og enkel adgang til bestilling og administration af digital signatur, herunder især registreringsløsninger, der muliggør bestilling og udstedelse af signatur online.
    - Muligheden for at understøtte SCEP eller lignende til enrollment af (medarbejder-)certifikater på grundlag af brugercredentials fra netværkslogon kan overvejes.
    - Adgang til overblik over virksomhedens/myndighedens certifikater og udløbstidspunkt i sammenhæng med notificering ved om udløb af certifikater ønskes.

4. Teknik og infrastruktur,

herunder eksempelvis adskillelse af eID og eSignering, single sign-on, sammenhængende IT-arkitektur, sikkerhed mv.

- Løsningen skal overholde besluttede certifikatpolitikker, herunder OCES og andre
- Den fremtidige løsning skal integreres med EU e-ID, sådan at der er flere mulige løsninger og leverandørvalg. Evt. ét fælles EU rod-certifikat med henblik på at etablere et ensartet identifikationsmønster.
- Den fremtidige løsning skal tilbyde alternative mulige anvendelser af digitale signaturer fra andre leverandører
- Der skal etableres en bedre proaktiv beskyttelse mod Cyberangreb m.m.
- Klientsignaturløsningen skal understøtte en høj grad af platformuafhængighed.
- Bedre driftsgarantier i forhold OSCP responderen
- Gerne supplerende service til udveksling af den offentlige del af certifikater fx mhp. Web Services Security kryptering
- Bedre understøttelse af teknisk overvågning og test.

5. Samspil med interessenter,

herunder tjenesteudbydere, administrative procedurer, sikkerhedsprocedurer mv.

- Styrkelse af kommunikation mellem de implicerede interessenter - eksempelvis i forbindelse med større ændringer så som opgradering fra OCES1 og OCES2

6. Fremtidig forretningsmodel,

herunder leverandørstyring, support, betalingsstruktur, en model med flere leverandører mv.

- Der skal etableres en løsning, som sikrer/garanterer forsyningssikkerhed og kontrol med den kommende NemID løsning.
- Der bør etableres / tilbydes flere alternative leverandørers løsninger (=> brugere får frie valg og større forsyningssikkerhed).

7. Andre bemærkninger

- Gerne et samlet udbud (ikke opdelt på fx borger- og virksomhedsområdet).

Høringssvar

Vedr. Offentlig høring om næste generation af den nationale identifikations- og digital signaturinfrastruktur (NemID)

Afsender	Sorø Kommune
Dato	27. juni 2014

Hermed høringssvar på Offentlig høring om næste generation af den nationale identifikations- og digital signaturinfrastruktur (NemID)

1. Fremtidige forretningsmæssige behov offentlige sektor og borgere i Danmark samt evt. juridiske forhold:
    a. Det skal indtænkes, at forskellige organisationer repræsenteres forskelligt. Fx har både Mærsk og Sorø Roklub CVR-numre, men der er gigantisk forskel på de to organisationer både med hensyn til tegning, kontinuitet, professionalisme, intern/egen juridisk rådgivning og støtte, økonomiske interesse og afhængighed af det offentlige osv.
    b. Må ikke forudsætte proprietære teknologier som fx Java.

2. Funktionalitet og anvendelse, herunder eksempelvis niveaudelt sikkerhed, lokal administration af autorisation, single sign-on mv.
    a. Det skal indtænkes, at forskellige organisationer repræsenteres forskelligt. Fx har både Mærsk og Sorø Roklub CVR-numre, men der er gigantisk forskel på de to organisationer både med hensyn til tegning, kontinuitet, professionalisme, intern/egen juridisk rådgivning og støtte, økonomiske interesse og afhængighed af det offentlige osv.
    b. Må ikke forudsætte proprietære teknologier som fx Java.

3. Behov for brugervenlighed, herunder forskellige brugeres aktiviteter fra bestilling til anvendelse og eventuel spærring mv.
    a. Brugergrænsefladen skal som minimum overholde http://htmlguide.borger.dk/ med tilpasninger til virk.dk. Da der er tale om et meget begrænset flow, bør der indgå omfattende test for hver visning/grænseflade, hvor der inddrages brugere i alle aldersgrupper, log-in platforme på alle styresystemer og i adskillige af mest udbredte versioner af disse (fx top 5), som igen skal testes hver især på et omfattende antal forskellig hardware – forskellige modeller, forskellige leverandører osv.
    b. Må ikke forudsætte proprietære teknologier som fx Java.

4. Teknik og infrastruktur, herunder eksempelvis adskillelse af eID og eSignering, single sign-on, sammenhængende IT-arkitektur, sikkerhed mv.
    a. Den resulterende oplevede hastighed opfatter vi som en del af brugervenlighed og tilgængelighed, da backend er uinteressant for brugere.

   b. Må ikke forudsætte proprietære teknologier som fx Java.

5. Samspil med interessenter, herunder tjenesteudbydere, administrative procedurer, sikkerhedsprocedurer mv.
   a. Må ikke forudsætte proprietære teknologier som fx Java.

6. Fremtidig forretningsmodel, herunder leverandørstyring, support, betalingsstruktur, en model med flere leverandører mv.
   a. På grund af den omfattende digitalisering bør der kun opereres med modeller, der koster gratis for slutbrugerne uanset omfang af behov for antal brugere, antal log-ins o.lign.

7. Andre bemærkninger

Tak fordi I lytter.

Venlig hilsen

Martin Sigaard

Projektleder, obligatorisk digital selvbetjening

Hovednr.: 57876000
Direkte: 57876303
E-mail: msig@soroe.dk

Sorø Kommune
Teknisk Service og Rengøring
Rådhusvej 8
4180 Sorø
www.soroe.dk

Høringssvar

Vedr. Offentlig høring om næste generation af den nationale identifikations- og digital signaturinfrastruktur (NemID)

Afsender	Theis F. Hinz
Dato	1. juni 2014

Bemærkninger vedrørende Høring om NemId

Mine bemærkninger angår ønske om at øge den folkelig tiltro til NemId's sikkerhed.

Dette kan gøres ved at brugerne selv kan vælge de CA (Certificate Authorities) som de har tiltro til. Dette kunne være udfra et udvalg som Digitaliseringsstyrelsen har godkendt. Ved mulighed kan der foreslås muligheden for at passcodes (nemid nøgler) kan generes af brugeren selv, og fremsendes til CA.

Dette ville give skeptikere af Nets (efter eks. Se & Hør skandalen) mulighed for alternativer de har tiltro til.

Ydemere vil jeg foreslå at gøre den tekniske dokumentation af NemId åben for borgere. Samtidig vil jeg foreslå at lade 3. parter gennemgå koden. Dette vil forhåbentlig forbedre befolkningens tiltro til at systemet ikke indholder bagdøre.

Mvh Theis F. Hinz

Edvard Thomsens Vej 14
2300 København S
Telefon 4178 0239
Fax 7262 6790
mei@trafikstyrelsen.dk
www.trafikstyrelsen.dk

Notat
Journalnr. TS00307-00056
Dato 27. juni 2014

Trafikstyrelsens svar på høring om næste generation af den nationale identifikations- og digital signaturinfrastruktur (NemID)

1. Fremtidige forretningsmæssige behov, for henholdsvis virksomheder, offentlige sektor og borgere i Danmark og udlandet samt eventuelle juridiske forhold.

Henvendelser fra borgere uden dansk CPR-nr. og tilsvarende virksomheder uden dansk CVR-nr. er i dag et problem. For Trafikstyrelsens vedkommende er antallet på luftfartsområdet – ikke helt lille, men der er sikkert nogle andre og større virksomheder, der har tilsvarende problemer og måske også løsninger. Der er derfor behov for følgende:

- Udenlandske selskaber skal kunne identificere sig entydig med en NemID-lignende løsning, så der kan etableres løsninger, der også henvender sig til udenlandske selskaber uden CVR-nr.
- Udenlandske statsborgere (f.eks. kabinepersonale) skal kunne identificere sig entydig med en NemID-lignende løsning, så der kan etableres løsninger, der også henvender sig til udenlandske statsborgere uden CPR-nr.
- Hvis der benyttes "single signon", skal der være en løsning, så de to ovennævnte kan udelukkes fra "single signon", såfremt man ikke ønsker adgang til sin løsning fra udenlandske selskaber/statsborgere.

2. Funktionalitet og anvendelse, herunder eksempelvis niveaudelt sikkerhed, lokal administration af autorisation, single sign-on mv.

- Medarbejderen med et medarbejder-NemID skal identificeres via CPR-nr. - ikke alene via RID. Ofte er det afgørende umiddelbart at kunne identificere medarbejderen. Alternativt skal man via en service kunne få CPR-nr. via RID – måske kan man det allerede?

- I fremtidige it-løsninger vil der være behov for at borgere og virksomheder bruger NemID til både at identificere sig og til at underskrive med – det stiller krav om, at man kan identificere på personniveau med de rette rettigheder, og det hele skal være i samme signatur.
- Det vil formentlig være nyttigt at kunne skelne mellem læse- og skriveadgang.

3. Behov for brugervenlighed, herunder forskellige brugeres aktiviteter fra bestilling til anvendelse og eventuel spærring mv.

- Trafikstyrelsen vil på sigt have et øget behov for rettighedsadministration, og der vil derfor være behov for forbedringer af den nuværende administratorsides brugergrænseflade.

4. Teknik og infrastruktur, herunder eksempelvis adskillelse af eID og eSignering, single sign-on, sammenhængende IT-arkitektur, sikkerhed mv.

- Da det ikke kan forventes, at fremtidens brugere benytter en pc – skal den fremtidige løsning være platformsuafhængig. Der skal ikke foretages yderligere udvikling og benyttes ekstra pinkoder eller lignende for at signaturen kan bruges på andet udstyr – det vil øge brugervenligheden betydeligt.
- I forbindelse med udviklingen af en applikation, som benytter sig af NemID til systemlogin, har Trafikstyrelsen haft problemer med, at sessionen med NemID timer ud i utide. I den nye version af NemID er der måske brug for en forbedring af mekanismen, som holder sessionen aktiv.

5. Samspil med interessenter, herunder tjenesteudbydere, administrative procedurer, sikkerhedsprocedurer mv.

- Det skal sikres, at store virksomheder, som DSB eller SAS, på en nem og sikker måde kan styre hvilke medarbejdere, der må hvad på en anden virksomheds måske 10-12 selvbetjeningsløsninger.
- I og med at den ene virksomhed udstiller en liste over roller, som den anden virksomheds administrator kan tildele til kollegaer afhængigt af deres arbejdsopgaver, bliver det meget vigtigt, at det kommunikeres tydeligt, hvad tildelingen indebærer.

  Hvorledes skal det f.eks. varsles til alle virksomheder, der alle-

rede har tildelt medarbejdere en rolle, hvis rettighederne på rollen udvides?

- Det kunne være relevant at hægte de forskellige handlinger op på paragraffer i lovgivningen, sådan at rettigheden f.eks. beskrives som:

  "Ret til at se, oprette og redigere virksomhedens data vedr. helbredsmæssig godkendelse af jernbanepersonale, Bekendtgørelse nr. xxx af yy-yy-yyyy"

6. Fremtidig forretningsmodel, herunder leverandørstyring, support, betalingsstruktur, en model med flere leverandører mv.

- Ift. den fremtidige forretningsmodel, skal NemID-udbyderne være opmærksomme på, at i takt med at der udvikles flere læsninger og brugen bliver mere udbredt, vil der blive øget behov for support. Derfor skal der arbejdes med opdelingen i, hvad virksomheden selv kan administrere som LRA, og hvad en udbyder/leverandør skal administrere.

7. Andre bemærkninger

Høringssvar

Vedr. Offentlig høring om næste generation af den nationale identifikations- og digital signaturinfrastruktur (NemID)

Afsender	Uddannelses- og Forskningsministeriet
Dato	2. juni 2014

Uddannelses- og Forskningsministeriet har ingen bemærkninger til vedhæftede.

f. Kia Moos

Med venlig hilsen

Joan Andersen
Sekretær
Politisk Afdeling
Direkte telefon.: +45 7231 8051
E-mail: jsp@ufm.dk

Uddannelses- og Forskningsministeriet

Departementet
Postboks 2135
DK-1015 København K
Telefon: +45 3332 9700
Fax: +45 3332 3501
E-mail: ufm@ufm.dk
www.ufm.dk

Besøgsadresse:
Slotsholmsgade 10
DK-1216 København K

Staben for Ledelse og Lean

UDLÆNDINGESTYRELSEN

Justitsministeriet
Att: Budget og Planlægningskontoret
Slotsholmen 10
1216 København K

Dato:	27. juni 2014
Sagsnummer:	14/079862
PersonID:	
Sagsbehandler:	ljn

Justitsministeriet har den 11. juni 2014 anmodet om Udlændingestyrelsens bemærkninger til en høring fra Digitaliseringsstyrelsen om næste generation af den nationale identifikations- og digital signaturinfrastruktur (NemID).
Udlændingestyrelsen har følgende bemærkninger vedrørende temaerne 1. Fremtidige forretningsmæssige behov samt 2. Funktionalitet og anvendelse.

1. Fremtidige forretningsmæssige behov
En stor andel af Udlændingestyrelsens brugere har ikke et dansk CPR-nr. og dermed heller ikke mulighed for at få et dansk NemID. En af styrelsens udfordringer i forbindelse med brugervendt digitalisering er således at kunne tilbyde pålidelige og sikre digitale services til udlændinge uden mulighed for at få dansk NemID. På den baggrund ser styrelsen et behov for digitalt at kunne identificere brugere uden NemID i forbindelse med modtagelse af oplysninger (digitale ansøgninger) eller udlevering af oplysninger via fx Min Side (adgang med NemID til personlig side med oplysninger om egne sager hos Udlændingestyrelsen og Styrelsen for Arbejdsmarked og Rekruttering) eller Digital Post.

2. Funktionalitet og anvendelse
NemID Light
En mulig løsning, som vil kunne adressere ovennævnte behov, kunne være at give udvalgte danske myndigheder mulighed for at udstede en digital identitet med begrænset gyldighed og rettighedsniveau ("NemId Light") til udlændinge uden CPR-nr eller eventuelt udlændinge, der har fået tildelt et administrativt CPR-nr. NemID light vil således kunne udstedes samtidig med identitetskontrol ved personligt fremmøde på fx en dansk repræsentation i forbindelse med ansøgning om visum eller opholdstilladelse.

Efterfølgende ved udstedelse af en opholdstilladelse i Danmark kan NemID light automatisk konverteres til et almindeligt dansk NemID.

Digital fuldmagt
En anden mulig løsning, som ligeledes vil kunne adressere det skitserede forretningsmæssige behov, kunne være en mulighed for at en person uden NemID kan give fuldmagt til en anden person eller virksomhed med NemID.

Venlig hilsen

Lars Aarud Krogh

Udlændingestyrelsen
Ryesgade 53
2100 København Ø

Telefon: *+45 35 36 66 00*
Mandag: *8.00 – 15.00*
Tirs-ons: *10.00 – 15.00*
Torsdag: *12.00 – 17.00*
Fredag: *10.00 – 13.00*
E-mail: *Se www.nyidanmark.dk*

Personlig henvendelse:
Man-ons: *8.30 – 12.00*
Torsdag: *11.30 – 17.30*
Fredag: *10.00 – 13.00*
Information på internettet: *www.nyidanmark.dk*

UNDERVISNINGS MINISTERIET
UNI•C – STYRELSEN FOR IT OG LÆRING

Notat

UNI•C København
Vester Voldgade 123
1552 København V
Tlf.nr.: 35 87 88 89
E-mail: uni-c@uni-c.dk
www.uni-c.dk
CVR-nr.: 13223459

Vedrørende: Høringssvar vedr. næste generation af den nationale identifikations- og digital signaturinfrastruktur (NemID)
Skrevet af: UNI•C – Styrelsen for It og Læring
Version:
Fordeling:

27.06.2014

Høringssvar om næste generation af den nationale identifikations- og digital signaturinfrastruktur (NemID)

I forbindelse med tilvejebringelsen af næste generation af den nationale identifikations- og digital signaturinfrastruktur (NemID) har Undervisningsministeriets styrelse for It og Læring med dette høringssvar et forretningsmæssigt fokus på elevers og medarbejderes digitale identitet i relation til primært flg. tre af høringens temaer.

- **Funktionalitet og anvendelse**, herunder eksempelvis niveaudelt sikkerhed, lokal administration af autorisation, single sign-on mv.
- **Behov for brugervenlighed**, herunder forskellige brugeres aktiviteter fra bestilling til anvendelse og eventuel spærring mv.
- **Samspil med interessenter**, herunder tjenesteudbydere, administrative procedurer, sikkerhedsprocedurer mv.

I dag løses skolernes adgangsstyring til digitale ressourcer i vidt omfang af bruger-/rolle-/rettigheds-systemet UNI•Login. Der er ikke taget stilling til om næste generation af den nationale identifikations- og digital signaturinfrastruktur (NemID) skal understøtte dele af skolernes behov for adgangsstyring. Hvis næste generation af den nationale identifikations- og digital signaturinfrastruktur (NemID) ønsker at understøtte Undervisningsministeriets område, bør løsningen, inden for den nuværende økonomi på skolerne, tilgodese særligt fire områder:

1 *Brugeradministration* - (decentralt på institutionerne via dataoverførsler fra de studieadministrative systemer)

2 *Information* (udstilling af brugernes roller: fx 'lærer', 'pædagog', 'skoleleder' eller 'elev', samt udstilling af brugernes relationer: eksempelvis relationen mellem elev og klasse, forældre og barn og lærer og skole).
3 *Licenser* (udstilling af brugernes rettigheder i og adgang til en meget bred vifte af digitale ressourcer i skolen).
4 *Autentifikation* - (brugernavn/password eller NemID for brugere over 15 år)

Særligt komponent 2 og 3 udgør i dag en del af kerneinfrastrukturen på Undervisningsministeriets område. Den nuværende infrastruktur sikrer et stort og veletableret domænekendskab om alle institutionernes brugere, som institutioner og offentlige og private tjenesteudbydere har gavn af når de enten aftager eller udvikler digitale tjenester. Der pågår pt. overvejelser på undervisningsområdet om, hvordan komponent 1, 2 og 3 kan udbygges som centrale komponenter i sektorens infrastruktur.

For så vidt angår autentifikationsdelen kan en kommende national e-identitets- og digital signatur-infrastruktur (NemID) supplere eller evt. erstatte eksisterende løsninger på Undervisningsministeriets område, hvis en kommende løsning kan tilgodese en række væsentlige forretningsmål, som knytter sig til områdets forskellige bruger- og aldersgrupper, samt de generelle rammebetingelser for uddannelsessektorens it- og datainfrastruktur:

1. Børn fra (0)6-15 år
    a. Smidig adgang, også for små børn, til digitale ressourcer via brugernavn / password (etfaktorlogin). Eksempelvis digitale læremidler, nationale test, digitale afgangsprøver, elevplaner, skolens intranet etc.
    b. Mulighed for at læreren, eller en anden ressourceperson på skolens område, inden for få minutter kan nulstille et glemt password.

2. Børn fra 15-18 år
    a. Smidig adgang til digitale ressourcer via brugernavn / password (etfaktorlogin). Eksempelvis digitale læremidler, nationale test, digitale afgangsprøver, elevplaner, skolens intranet etc.
    b. En højere grad af sikkerhed (tofaktorlogin) eksempelvis i forbindelse med afgangsprøver og andre digitale eksaminer.
    c. Mulighed for at læreren, eller en anden ressourceperson på skolens område, inden for få minutter kan nulstille et glemt password.

3. Ansatte
    a. Smidig adgang til digitale ressourcer via brugernavn / password (etfaktorlogin) til tjenester som ikke kræver høj grad af sikkerhed. Eksempelvis digitale læremidler, nationale test, digitale afgangsprøver, elevplaner, skolens intranet etc.

   b. En højere grad af sikkerhed (tofaktorlogin) til eksempelvis elevplaner og testresultater.

4. Forældre
   a. Smidig adgang til digitale ressourcer via brugernavn / password (etfaktorlogin) til tjenester som ikke kræver høj grad af sikkerhed. Eksempelvis oversigt over barnets lektier, skema og ugeplan. På forældreområdet er der eksempler på, at tvungen tofaktorlogin til alle skole/hjem-rettede tjenester er en barriere for det digitale samarbejde mellem skole og hjem.
   b. En højere grad af sikkerhed (tofaktorlogin) til eksempelvis skole/hjem-kommunikation, elevplan og test og prøveresultater.

Generelle rammebetingelser for uddannelsessektorens it- og datainfrastruktur

   a. Smidig hel eller delvis tilkobling af evt. ny nationale autentifikation til UNI•Logins registrering af uddannelsessektorens brugeradministration, rolleregistrering og licensregistrering.
   b. Sikring af fortsat single sign-on for grundskolens brugere for de løsninger, de skal anvende.
   c. En evt. udvidelse med national autentifikation må ikke medføre fordyrelser for skoler og leverandører af it-løsninger til skolerne samt medføre merudgifter for Undervisningsministeriets drifts- og vedligeholdelses-, udviklings- og supportomkostninger til UNI•Login.

Det bemærkes, at kommunale institutioner og selvejende uddannelsesinstitutioner i dag afholder udgiften til lokalt beredskab for password-administration.

Ældre Sagen

lis@digst.dk

25. juni 2014
BH/ISL

Høring om næste generation af den nationale identifikations- og digital signaturinfrastruktur(NemID)

Ældre Sagen har følgende bemærkninger til den ovennævnte høring;

Vi oplever lige nu en stor forandring af kontakten mellem borgere og det offentlige. Blandt ældre er der rigtig mange, der først de seneste år har stiftet bekendtskab med computer, internet og dertil hørende nye termer/sprog og sikkerhedsspørgsmål. Det er derfor vigtigt, at brugervenlighed og tilgængelighed er højt prioriteret i næste generation af den nationale identifikations- og digital signaturinfrastruktur.

Ved den nuværende NemID har vi fået henvendelser fra ældre, der har vanskeligt ved at læse nøglerne, fordi de er skrevet med gråt på nøglekortet (også i den store A4 udgave) eller vanskeligt ved at taste koden ind i selve log-in feltet, der som det eneste i løsningen ikke kan forstørres på skærmen. Tilgængelighed skal således tænkes ind i alle løsninger til brug for logon, her tænkes særligt på kontrast, tekststørrelse og brug af ord, som ikke er almindelig kendt. Det er ligeledes vigtigt, at det sikres, at særligt tilpassede it-programmer til personer med funktionsnedsættelse kan anvendes i samspil med den nye løsning, så tilgængeligheden sikres. Ældre Sagen foreslår, at der udføres brugertest i udviklingen af den nye løsning, hvor forskellige grupper af befolkningen med forskellige behov deltager. Ældre Sagen hjælper gerne med at finde deltagere til en sådan brugertest.

Det er selvfølgelig også meget vigtigt, at der i udviklingen af en brugervenlig og tilgængelig løsning medtænkes et højt sikkerhedsniveau fx ved at beholde et system med to-faktor sikkerhed.

Vi har ventet meget længe på, at NemID bliver anvendelig på mobile enheder, da det bliver mere og mere udbredt at anvende tablet eller smartphone til at komme i kontakt med myndigheder. Det er derfor vigtigt, at den nye løsning fremtidssikres, således at den kan anvendes uanset teknologisk platform som fx Java eller enheder som fx PC eller tablets.

Endelig mener Ældre Sagen, at der skal udvikles et demo-miljø til demonstration og træning i brug af den nye løsning. Der er over 2.000 it-undervisere rundt om i Ældre Sagens lokalafdelinger, der hjælper ældre med at lære at bruge computer og internet. Derfor foreslår vi også, at der udarbejdes et vejledningsmateriale til brug for undervisning i brug af den nye løsning. Derved sikres den bedst mulige undervisning i de lokalafdelinger, der ønsker at undervise i brugen af den nye løsning.

Venlig hilsen

Bjarne Hastrup
Adm. direktør
Ældre Sagen